

ADVANCED TECHNIQUES IN MULTIMEDIA WATERMARKING

Image, Video and Audio Applications



Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications

Ali Mohammad Al-Haj
Princess Sumaya University for Technology, Jordan

Information Science
REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey • New York

Director of Editorial Content: Kristin Klinger
Director of Book Publications: Julia Mosemann
Acquisitions Editor: Lindsay Johnston
Development Editor: Joel Gamon
Publishing Assistant: Tom Foley
Typesetter: Michael Brehm
Production Editor: Jamie Snavely
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by

Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: <http://www.igi-global.com/reference>

Copyright © 2010 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher.

Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Advanced techniques in multimedia watermarking : image, video, and audio applications / Ali Mohammad Al-Haj, editor.

p. cm.

Includes bibliographical references and index.

Summary: "This book introduces readers to state-of-art research in multimedia watermarking in the different disciplines of watermarking, addressing the different aspects of advanced watermarking research; modeling and theoretical analysis, advanced embedding and extraction techniques, software and hardware implementations, and performance evaluations of watermarking systems"--Provided by publisher.

ISBN 978-1-61520-903-3 (hardcover) -- ISBN 978-1-61520-904-0 (ebook) 1. Multimedia systems--Security measures. 2. Digital watermarking. 3. Intellectual property infringement--Prevention--Technological innovations. I. Al-Haj, Ali Mohammad. QA76.575.A38 2010 006.6--dc22

2009046731

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

Editorial Advisory Board

Ala'a Sheta, *Al-Balqa Applied University, Jordan*
Majed Taee, *University of Jordan, Jordan*
Rachid Sammouda, *University of Sharjah, UAE*
Bassam Kahhaleh, *Princess Sumaya University for Technology, Jordan*
Mansour Abbadi, *Jordan University of Science and Technology, Jordan*
Samir Shaltaf, *Princess Sumaya University for Technology, Jordan*
Ashraf Odeh, *Royal Scientific Society, Jordan*

Table of Contents

Foreword	xv
Preface	xvi

Section 1 Digital Image Watermarking

Chapter 1

Two Spatial Watermarking Techniques for Digital Images	1
<i>Dumitru Dan Burdescu, University of Craiova, Romania</i>	
<i>Liana Stănescu, University of Craiova, Romania</i>	
<i>Marian Cristian Mihăescu, University of Craiova, Romania</i>	

Chapter 2

Data Secrecy: An FFT Approach	21
<i>Tamer Rabie, UAE University, UAE</i>	

Chapter 3

Color in Image Watermarking.....	36
<i>Gaël Chareyron, École Supérieure d'Ingénieurs Léonard de Vinci, France</i>	
<i>Jérôme Da Rugna, École Supérieure d'Ingénieurs Léonard de Vinci, France</i>	
<i>Alain Tréneau, Laboratoire Hubert Curien, Université Jean Monnet, France</i>	

Chapter 4

Geometric Distortions-Invariant Digital Watermarking Using Scale-Invariant Feature Transform and Discrete Orthogonal Image Moments	57
<i>Shiraz Ahmad, Pakistan Atomic Energy Commission, Pakistan</i>	
<i>Zhe-Ming Lu, Zhejiang University, P. R. China</i>	

Section 2

Video, Audio, Text, and 3D Mesh Watermarking

Chapter 5

- From Watermarking to In-Band Enrichment: Theoretical and Applicative Trends 111
Mihai Mitrea, Institut TELECOM, France
Françoise Prêteux, Institut TELECOM, France

Chapter 6

- Audio Watermarking: State-of-the-Art 127
Dejan Dražić, Ericsson d.o.o., Serbia
Nedeljko Čvejić, University of Cambridge, UK

Chapter 7

- Watermarking Audio Signals for Copyright Protection Using ICA 144
B. R. Matam, NCRG, Aston University, UK
David Lowe, NCRG, Aston University, UK

Chapter 8

- Deterring Text Document Piracy with Text Watermarking 158
Rakesh Kumar Mishra, Feroze Gandhi Institute of Engineering and Technology, India

Chapter 9

- Blind Watermarking of Three-Dimensional Meshes: Review, Recent Advances and Future Opportunities 200
Kai Wang, Université de Lyon, CNRS, INSA-Lyon, France
Guillaume Lavoué, Université de Lyon, CNRS, INSA-Lyon, France
Florence Denis, Université de Lyon, CNRS, Université Lyon, France
Atilla Baskurt, Université de Lyon, CNRS, INSA-Lyon, France

Section 3

Multimedia Watermarking

Chapter 10

- A Unified Approach Towards Multimedia Watermarking 228
Ali Al-Haj, Princess Sumaya University for Technology, Jordan
Ahmad Mohammad, Princess Sumaya University for Technology, Jordan
Samir Abou El-Seoud, Princess Sumaya University for Technology, Jordan
Tuqa Manasrah, The University of Jordan, Jordan
Lama Rajab, The University of Jordan, Jordan
Tahani Al-Khatib, The University of Jordan, Jordan

Chapter 11	
Data Hiding Schemes Based on Singular Value Decomposition.....	254
<i>Victor Pomponiu, University of Torino, Italy</i>	
<i>Davide Cavagnino, University of Torino, Italy</i>	
<i>Alessandro Basso, University of Torino, Italy</i>	
<i>Annamaria Vernone, University of Torino, Italy</i>	
Chapter 12	
Feature Based Watermarking	289
<i>Hedley Morris, Claremont Graduate University, USA</i>	
<i>Mohammad Eyadat, California State University, USA</i>	
<i>Imad Muhi, New York Institute of Technology, Jordan</i>	
Chapter 13	
Techniques for Multiple Watermarking	324
<i>Abdellatif Zaidi, Université Catholique de Louvain, Belgium</i>	
Chapter 14	
Copyright Protection in the Distribution of Multimedia Digital Objects in Internet.....	344
<i>Mariví Higuero, University of the Basque Country, Spain</i>	
<i>Purificación Saiz, University of the Basque Country, Spain</i>	
<i>Marina Aguado, University of the Basque Country, Spain</i>	
Section 4	
Optimization and Hardware Implementation of Watermarking Algorithms	
Chapter 15	
Optimization in Digital Watermarking Techniques	369
<i>Santi P. Maity, Bengal Engineering and Science University, India</i>	
<i>Claude Delpha, Laboratoire des Signaux et Systèmes (L2S), France &</i>	
<i>Université Paris-SUD XI, France</i>	
Chapter 16	
Application of Error Control Coding for Multimedia Watermarking Technologies.....	407
<i>Mehul S. Raval, DA-IICT, India</i>	
Chapter 17	
Hardware Implementations of Image/Video Watermarking Algorithms	425
<i>Fayez M. Idris, German-Jordanian University, Jordan</i>	

Chapter 18

Spread Spectrum Watermarking: Implementation in FPGA..... 455
Santi P. Maity, Bengal Engineering and Science University, India

Compilation of References 486

About the Contributors 528

Index 536

Detailed Table of Contents

Foreword	xv
Preface	xvi

Section 1 Digital Image Watermarking

Chapter 1

Two Spatial Watermarking Techniques for Digital Images	1
<i>Dumitru Dan Burdescu, University of Craiova, Romania</i>	
<i>Liana Stănescu, University of Craiova, Romania</i>	
<i>Marian Cristian Mihăescu, University of Craiova, Romania</i>	

This chapter presents two original spatial authentication techniques for digital images. The two techniques are based on the utilization of virtual (2D or 3D) graphs embedded into the digital images. The colors of some vertices of the virtual graph are slightly modified for obtaining the watermark. Pixels or voxels of the object are modified by a spatial watermark insertion scheme. The watermark may be inserted in the most perceptually significant sub-image or in entire image, thus eliminating chances of being subjected to severe digital attacks, which will reduce the value of the protection. Both techniques require less computation than traditional techniques, both are secure since watermark application remains in the virtual graph nodes, and both can be used for colored as well black and white digital images.

Chapter 2

Data Secrecy: An FFT Approach	21
<i>Tamer Rabie, UAE University, UAE</i>	

This chapter describes a framework for image hiding in the frequency domain. that exploits spectral properties of the Fourier magnitude and phase of natural images. The theory is that as long as the Fourier phase of an image is maintained intact, the overall appearance of an image remains specious if the Fourier magnitude of the image is slightly modified. This hypothesis leads to a data hiding technique that promises high fidelity, capacity, security, and robustness to tampering. Experimental results are presented throughout the chapter to demonstrate the effectiveness of the proposed approach.

Chapter 3

Color in Image Watermarking.....	36
----------------------------------	----

Gaël Chareyron, École Supérieure d'Ingénieurs Léonard de Vinci, France

Jérôme Da Rugna, École Supérieure d'Ingénieurs Léonard de Vinci, France

Alain Tréneau, Laboratoire Hubert Curien, Université Jean Monnet, France

This chapter summarizes the state-of-the-art color techniques used in the field of image watermarking. It describes the major difficulties associated with the treatment of color images, and presents a panorama of both classical and new directions taken in the field of color images watermarking. Color techniques summarized in the chapter are classified into three categories. The first category, color watermarking through color histograms and quantization embeds the watermark within the image color representation. The second category, color watermarking through the spatial domain, includes all the methods that modify the pixel value by using its spatial position or its neighborhood. The third category, color watermarking through a transform domain generates a watermark with a help of a domain transform like DCT, DFT or DWT.

Chapter 4

Geometric Distortions-Invariant Digital Watermarking Using Scale-Invariant Feature Transform and Discrete Orthogonal Image Moments	57
--	----

Shiraz Ahmad, Pakistan Atomic Energy Commission, Pakistan

Zhe-Ming Lu, Zhejiang University, P. R. China

This chapter presents two geometric-invariant digital image watermarking techniques which apply the source-independent watermark signals to the original images. These techniques exploit the invariant properties of images for the watermarking purposes. The first technique utilizes the scale-invariant features and discrete moment invariants of the images to establish a non-blind watermarking system. The second technique utilizes only the discrete moment invariant features of the images, and the whole image is used for embedding the watermark information. Implementations of the proposed techniques are supported with a thorough discussion, and experimental results are presented to demonstrate the effectiveness of the techniques against several kinds of geometric attacks.

Section 2

Video, Audio, Text, and 3D Mesh Watermarking

Chapter 5

From Watermarking to In-Band Enrichment: Theoretical and Applicative Trends	111
---	-----

Mihai Mitrea, Institut TELECOM, France

Françoise Prêteux, Institut TELECOM, France

This chapter deals with enriched media, which refers to all possible associations established between some original data (video, audio, 3D, ...) and some metadata (textual, audio, video, executable codes, ...). Such a new content may be further exploited for various applications, like interactive HDTV, computer games, or data mining, for instance. The chapter is meant to bring into evidence the role wa-

termarking techniques may play in this new applicative field. Following the watermarking philosophy, the in-band enrichment supposed that the enrichment data are inserted into the very data to be enriched. Thus, three main advantages are ensured: backward compatibility, format coherence, and virtually no network overhead. The discussion is structured on both theoretical aspects and developed applications.

Chapter 6

Audio Watermarking: State-of-the-Art 127

Dejan Drajic, Ericsson d.o.o., Serbia

Nedeljko Cvejic, University of Cambridge, UK

This chapter recapitulates the background and the state-of-the-art of digital audio watermarking, including descriptions of audio watermarking algorithms and malicious attacks against these algorithms. It gives a literature survey of audio watermarking algorithms that form the mainstream research, and outlines the areas in which audio watermarking has been implemented, along with possible future applications. The three requirements in audio watermarking; robustness, watermark bit rate and perceptual transparency, are described as well. The chapter finally provides a comprehensive list of attacks used by adversaries to interfere with the embedded watermark and to prevent its detection.

Chapter 7

Watermarking Audio Signals for Copyright Protection Using ICA..... 144

B. R. Matam, NCRG, Aston University, UK

David Lowe, NCRG, Aston University, UK

In this chapter, a discussion of information hiding in the context of copyright protection of audio signals is presented. Independent component analysis (ICA) based watermarking methods are used to embed copyright information. The integrity of a hidden message will be investigated when the cover text, in which it is hidden, is attacked by applying signal processing techniques to the signal. The results of the application of the ICA based method are compared with the results of the application of the discrete wavelet transform (DWT) based approach. The chapter reveals the advantages of using a data dependent transform (for example ICA) based watermarking method for copyright applications when compared with static transform domain (having fixed coefficients, for example DWT) based methods.

Chapter 8

Deterring Text Document Piracy with Text Watermarking..... 158

Rakesh Kumar Mishra, Feroze Gandhi Institute of Engineering and Technology, India

Unlike audio and video, text piracy is not complemented by IT solutions except for certain proprietary initiatives. Therefore, this chapter deals with text watermarking. The chapter embarks on review of technological advancements for text copyright protection along with issues and challenges for their implementation. Appraisal comprises of watermark embedding algorithms and distribution infrastructure. A brief discussion over the document structure, watermark composition and type, classification of algorithms and future direction is also given. To make approach holistic, couple of systems are also studied.

Chapter 9

Blind Watermarking of Three-Dimensional Meshes: Review, Recent Advances and Future Opportunities	200
--	-----

Kai Wang, Université de Lyon, CNRS, INSA-Lyon, France

Guillaume Lavoué, Université de Lyon, CNRS, INSA-Lyon, France

Florence Denis, Université de Lyon, CNRS, Université Lyon, France

Atilla Baskurt, Université de Lyon, CNRS, INSA-Lyon, France

This chapter deals with digital watermarking of three-dimensional (3-D) meshes. This relatively new area of digital watermarking has numerous potential applications which already received attention from both academic researchers and industrial practitioners. The chapter focuses on the study of blind mesh watermarking techniques, which do not need the original cover mesh for watermark extraction and thus have a much larger application range than the non-blind techniques. In this chapter, the authors review the existing methods proposed so far, by classifying them into three groups: fragile schemes, high-capacity schemes and robust schemes. Then, they present their recent work on quantization-based blind watermarking of semi-regular meshes. Finally, the authors suggest some future working directions.

Section 3**Multimedia Watermarking****Chapter 10**

A Unified Approach Towards Multimedia Watermarking	228
--	-----

Ali Al-Haj, Princess Sumaya University for Technology, Jordan

Ahmad Mohammad, Princess Sumaya University for Technology, Jordan

Samir Abou El-Seoud, Princess Sumaya University for Technology, Jordan

Tuqa Manasrah, The University of Jordan, Jordan

Lama Rajab, The University of Jordan, Jordan

Tahani Al-Khatib, The University of Jordan, Jordan

This chapter describes imperceptible and robust watermarking algorithms for three different types of multimedia objects (image, video, audio). Proposed algorithms are based on cascading two powerful mathematical transforms; the Discrete Wavelet Transform (DWT), and the Singular Value Decomposition (SVD). The two transforms are different, and thus provide complementary levels of robustness against the same attack. In the proposed dual-transform algorithms, the watermark bits are not embedded directly into the wavelet coefficients, but rather on the elements of singular values of the DWT sub-bands of the media object. Effectiveness of the proposed algorithms is demonstrated through extensive experimentation.

Chapter 11

Data Hiding Schemes Based on Singular Value Decomposition.....	254
--	-----

Victor Pomponiu, University of Torino, Italy

Davide Cavagnino, University of Torino, Italy

Alessandro Basso, University of Torino, Italy

Annamaria Vernone, University of Torino, Italy

Several schemes have been devised in the fields of steganography and digital watermarking, exploiting the properties of different transform domains. This chapter focuses on the Singular Value Decomposition (SVD) transform, with the aim of providing an exhaustive overview on those steganography and watermarking techniques leveraging on the important properties of such a transform. The large number of algorithms operating in the image, video and audio context is first classified by means of a general approach, then analyzed, to highlight the advantages and disadvantages of each method. The chapter also gives a detailed discussion about the applicability of each reviewed and compared data hiding scheme, in order to identify the most appropriate candidates for practical applications.

Chapter 12

Feature Based Watermarking 289

Hedley Morris, Claremont Graduate University, USA

Mohammad Eyadat, California State University, USA

Imad Muhi, New York Institute of Technology, Jordan

Geometric attacks of an image can make it difficult, or impossible, for the legitimate owner of a watermarked digital image to recover the watermark. This chapter presents a new paradigm for rendering any watermarking scheme resistant to geometric attacks. This is done by means of a new image transform to a Rotation, Scaling, and Translation (RST) invariant domain based on ideas from shape theory. The chapter also proposes extensions of this technique to video watermarking. Finally, an example is provided of how these ‘shape based’ concepts can be extended to more general relational databases.

Chapter 13

Techniques for Multiple Watermarking 324

Abdellatif Zaidi, Université Catholique de Louvain, Belgium

The watermarking problem is relatively well understood in the single watermark case, but it lacks theoretical foundation in the multiple watermarks case. The goal of this chapter is to provide important technical insights, as well as intuitive and well developed discussions, onto how multiple watermarks can be embedded efficiently into the same host signal. The chapter adopts communication and information theoretic inclinations, and argues that this problem has tight relationship to conventional multi-user information theory. Then, its shown that by virtue of this tight relationship, that design and optimization of algorithms for multiple watermarking applications can greatly benefit from recent advances in multi-user information theory.

Chapter 14

Copyright Protection in the Distribution of Multimedia Digital Objects in Internet 344

Mariví Higuero, University of the Basque Country, Spain

Purificacion Saiz, University of the Basque Country, Spain

Marina Aguado, University of the Basque Country, Spain

This chapter presents the most significant approaches developed so far, for the distribution of digital contents with copyright protection, highlighting their most interesting features. These approaches are classified into two categories: on the one hand systems that try to prevent unauthorized uses of the

contents, and on the other hand systems whose purpose is to detect unauthorized uses of the contents and to identify involved offenders. The chapter is focused on the systems that fit in the second of these strategies, where most of which are based on the use of watermarking techniques.

Section 4

Optimization and Hardware Implementation of Watermarking Algorithms

Chapter 15

Optimization in Digital Watermarking Techniques	369
<i>Santi P. Maity, Bengal Engineering and Science University, India</i>	
<i>Claude Delpha, Laboratoire des Signaux et Systèmes (L2S), France &</i>	
<i>Université Paris-SUD XI, France</i>	

Digital watermarking is a multidisciplinary research area involving theory of communications, signal processing, multimedia coding, information theory, cryptography, computer science and game theory etc. This chapter looks at digital watermarking as an optimization problem from different combination of these areas. The goal is to resolve the conflicting requirements of different parameters and properties of digital watermarking. The chapter also presents a review of recent advances in the state-of-the-art algorithms for optimized watermarking techniques. Optimized watermarking methods are then discussed from the rigorous mathematical analysis to theoretical derivations of algorithms with the aid of soft computing techniques. The design and implementation of optimized watermarking methods for the image, video and sound signals are discussed in the context of various diverse applications. Finally, the scope of future research in this area is highlighted.

Chapter 16

Application of Error Control Coding for Multimedia Watermarking Technologies.....	407
<i>Mehul S. Raval, DA-IICT, India</i>	

The performance of watermarking schemes can be improved if channel codes are used for encoding the hidden message. This chapter targets applications of Error Control Coding (ECC) to watermarking namely; copyright protection, authentication, forensics and stego watermarking techniques including active steganography. The chapter aims at studying various properties of watermarking systems, looking into their specific requirements, and then try to search for suitable error control code. This will boost the over all performance of watermarking techniques. This chapter also intends to discuss the state-of-the-art research in this direction, and then presents a watermarking method based on facts covered in the chapter.

Chapter 17

Hardware Implementations of Image/Video Watermarking Algorithms	425
<i>Fayez M. Idris, German-Jordanian University, Jordan</i>	

The use of watermarking in consumer products and real-time applications dictates the development of hardware architectures. This chapter presents a survey of existing implementations of image and video watermarking. It first discusses the design issues and implementation challenges in image and video

watermarking with emphasis on computational complexity aspects. This is followed by a classification and detailed survey of the different reported hardware implementations and identifying the exploited techniques to improve efficiency. Future perspectives to address the challenges of hardware architecture design for image and video watermarking are then discussed.

Chapter 18

Spread Spectrum Watermarking: Implementation in FPGA.....	455
<i>Santi P. Maity, Bengal Engineering and Science University, India</i>	

This chapter first presents a brief review on hardware implementation of digital watermarking algorithms, followed by development of hardware architecture for spatial domain and fast Walsh transform (FWT) domain Spread spectrum (SS) watermark system design using field programmable gate array (FPGA). Few challenges for hardware design of watermarking algorithms are then described with an objective to give an idea how to develop watermarking algorithms so that it can be implemented on hardware. The chapter ends with few open research problems on hardware architecture as scope of future research work.

Compilation of References	486
About the Contributors	528
Index.....	536

Foreword

Digital watermarking technology is strongly advocated as a solution to prevent illegal and malicious copying and distribution of digital media. In fact, many multimedia watermarking algorithms have been proposed in the last decade to protect the copyright of multimedia objects such as digital images, audio and video clips. However, as the amount of digital multimedia production increases exponentially, the need for better and more advanced techniques for watermarking multimedia digital objects increases as well. I am therefore delighted to have this book edited by Dr. Ali Mohammad Al-Haj. Together with authors from all over the world he managed to publish and discuss fundamentals, applications and experiences in the field of multimedia watermarking. Indeed, this book comes to introduce readers to state-of-the-art research in multimedia watermarking in order to enable high quality research in the different disciplines of watermarking.

I would like to congratulate the editor and the authors to this really succeeded book. I can recommend it to all researchers, students and practitioners, who are working in the field of watermarking and close-by subjects as well as to people who only would like to inform themselves about this newsworthy and prospective technology. With all my heart I wish this publication a large audience.

Michael E. Auer

*School of Systems Engineering
Carinthia University of Applied Sciences
Villach, Austria*

Michael E. Auer received his Ing. degree in 1971, and his Ph.D. degree in 1975, from the Dresden University of Technology. From 1974 to 1991 he was an assistant professor at the faculties Electrical Engineering and Informatics of Dresden University. From 1991-95 he was with F+O Electronic Systems GmbH, Heidelberg (Head of software department). In 1995 Michael Auer was appointed Professor of Electrical Engineering of the School of Electronics at Carinthia Tech Institute, Villach, Austria and has also a teaching position at the University of Klagenfurt. Furthermore works as a visiting professor at the Universities of Amman (Jordan), Brasov (Romania) and Patras (Greece). Michael Auer has experience in leading of several national and international projects in the fields of remote engineering and technology supported learning. Under his guidance international teams developed a Joint European Master Study Program "Remote Engineering" (EU project MARE) and a Joint European Bachelor Study Program "Information Technology" (EU project BIT2010). In June 2006 Michael Auer was elected as President and CEO of the "International Association of Online Engineering" (IAOE), a non-governmental organization that promotes the vision of new engineering working environments worldwide. He had been included in the 2006 & 2007 edition of Who's Who in Science and Engineering.

Preface

In recent years, the tremendous advancement of digital technology has increased the ease with which digital multimedia files (image, video, and audio) are stored, transmitted, and reproduced. Consequently, content providers and owners are faced with the problem of protecting against copyright violation and other forms of abuse of their digital property. The nature of digital multimedia content makes traditional copyright methods unsuitable for establishing ownership. Therefore, digital watermarking was proposed, and strongly advocated, as a solution to prevent illegal and malicious copying and distribution of digital media. Many multimedia watermarking algorithms have been proposed in the last decade, however as the amount of digital multimedia production increases exponentially, the need for better and more advanced techniques for watermarking multimedia digital objects increases as well.

The primary objective of the book is to introduce readers to state-of-the-art research in multimedia watermarking in order to enable high quality research in the different disciplines of watermarking. Therefore, this book is considered useful as a reference for professionals and researchers working in areas such as image and document watermarking, audio and video watermarking, multimedia fingerprinting, information hiding, secured e-commerce, copyright protection, authentication, information management, and hardware implementation of real-time multimedia watermarking. The book consists of four sections, and eighteen chapters, covering a wide spectrum of multimedia watermarking topics. Section 1 compromises four chapters covering new advancements in digital image watermarking. Watermarking of other multimedia objects such as video, audio, text and 3D meshes are covered in Section 2. Techniques for files containing different multimedia objects are covered in Section 3. Optimization and hardware implementation of digital watermarking techniques are covered in section 4.

In section 1, four chapters have been chosen to address new advancements in different image watermarking areas; spatial domain watermarking, frequency domain watermarking, color in watermarking, and geometric-invariant image watermarking. Chapter 1 presents two original spatial authentication techniques for digital images. The two techniques are based on the utilization of virtual (2D or 3D) graphs embedded into the digital images, where the colors of some vertices of the virtual graph are slightly modified for obtaining the watermark. The watermark is inserted in the most perceptually significant sub-image or in entire image, thus eliminating chances of being subjected to severe digital attacks. Both techniques require less computation than traditional techniques, both are secure since watermark application remains in the virtual graph nodes, and both can be used for colored as well black and white digital images.

Chapter 2 deals with advancements in image watermarking in the frequency domain. It describes a framework for image hiding that exploits spectral properties of the Fourier magnitude and phase of natural images. The theory is that as long as the Fourier phase of an image is maintained intact, the overall appearance of an image remains specious if the Fourier magnitude of the image is slightly modified. This hypothesis leads to a data hiding technique that promises high fidelity, capacity, security, and

robustness to tampering. Experimental results are presented throughout the chapter to demonstrate the effectiveness of the proposed approach.

Color is still an unresolved issue in digital watermarking. Chapter 3 summarizes the state-of-the-art color techniques used in image watermarking. The chapter first describes the major difficulties associated with the treatment of color images, and then presents a panorama of both classical and new directions taken in the field of color images watermarking. Color techniques summarized in the chapter are classified into three categories; color watermarking through color histograms and quantization, color watermarking through the spatial domain, and color watermarking through a transform domain.

The last chapter in this section, chapter 4 presents two geometric-invariant digital image watermarking techniques, which apply the source-independent watermark signals to the original images. These techniques exploit the invariant properties of images for the watermarking purposes. The first technique utilizes the scale-invariant features and discrete moment invariants of the images to establish a non-blind watermarking system. The second technique utilizes only the discrete moment invariant features of the images and the whole image is used for embedding the watermark information. Implementations of the two techniques are supported with a thorough discussion, and experimental results are presented to demonstrate the effectiveness of the proposed techniques against several kinds of geometric attacks.

Research in video, audio and text watermarking received less attention than image watermarking due to the inherent difficulties in these media types, such as larger amount of data, unique attacks, and sensitivity of the human visual and auditory systems. In section 2, five chapters have been chosen to address advancements in different areas in video watermarking, audio watermarking, text watermarking, and 3D mesh watermarking. Chapter 5 deals with video watermarking and in-band enrichment, chapters 6 and 7 describe current status advancements in audio watermarking, chapter 8 describes text watermarking, and the last chapter introduces watermarking of 3D meshes and outlines its importance.

Chapter 5 brings into evidence the role watermarking techniques may play in the new applicative field of video *in-band enrichment*. Following the watermarking philosophy, the *in-band enrichment* supposed that the enrichment video is inserted into the video to be enriched. Thus, three main advantages are ensured: backward compatibility, format coherence, and virtually no network overhead. The discussion is structured on both theoretical aspects and on developed applications.

Chapter 6 recapitulates the state-of-the-art of digital audio watermarking, including descriptions of audio watermarking algorithms and malicious attacks against these algorithms. The chapter gives a literature survey of audio watermarking algorithms that form the mainstream research, and outlines the areas in which audio watermarking has been implemented along with possible future applications. The chapter also provides a comprehensive list of attacks used by adversaries to interfere with the embedded watermark and to prevent its detection.

In chapter 7, Independent Component Analysis (ICA) based watermarking methods are used to embed copyright information in audio signals. The integrity of a hidden message when the cover text in which it is hidden, is attacked by applying signal processing techniques such as filtering and addition of noise to the signal will be investigated. The results of the application of the ICA based method are compared with the results of the application of the discrete wavelet transform (DWT) based approach. The chapter reveals the advantages of using a data dependent transform (for example ICA) based watermarking method for copyright applications when compared with static transform domain (having fixed coefficients, for example DWT) based methods.

Literature piracy, though not being given much attention, constitutes a major bulk. Therefore, chapter 8 deals with text watermarking, which is a very important technology to solve the literature piracy problem. The chapter embarks on review of technological advancements for text copyright protection along with issues and challenges for their implementation. Appraisal comprises of watermark embedding

algorithms and distribution infrastructure. A brief discussion over the document structure, watermark composition and type, classification of algorithms and future direction is also given. To make approach holistic, a couple of systems are also studied.

Chapter 9 deals with digital watermarking of three-dimensional (3-D) meshes. This relatively new area of digital watermarking has numerous potential applications which already received attention from both academic researchers and industrial practitioners. The authors, first, review the existing methods proposed so far by classifying them into three groups: fragile schemes, high-capacity schemes and robust schemes. Then, they present their recent work on quantization-based blind watermarking of semi-regular meshes. Finally, the authors suggest some future working directions in watermarking of three-dimensional meshes.

The number of digital files with multimedia objects (images, audio, video, and text) is increasing across the Internet. In section 3, five chapters are introduced to present new advancements in multimedia watermarking. Chapter 10 describes a unified dual-transform approach for watermarking multimedia objects, while chapter 11 gives a survey on the use of the SVD (Singular Value Decomposition) transform in multimedia watermarking. Chapters 12 proposes feature-based watermarking for copyright protection of images and video documents. Chapter 8 furnishes the theoretical foundation for embedding multiple watermarks in multimedia objects. Finally, chapter 14 describes copyright protection in the distribution of multimedia digital objects across the Internet.

Chapter 10 describes imperceptible and robust watermarking algorithms for three different types of multimedia objects (image, video, audio). Proposed algorithms are based on cascading two powerful mathematical transforms; the Discrete Wavelet Transform (DWT), and the Singular Value Decomposition (SVD). The two transforms are different, and thus provide complementary levels of robustness against the same attack. In the proposed dual-transform algorithms, the watermark bits are not embedded directly into the wavelet coefficients, but rather on the elements of singular values of the DWT sub-bands of the media object. Effectiveness of the proposed algorithms is demonstrated through extensive experimentation.

Chapter focuses 11 on the Singular Value Decomposition (SVD) transform, with the aim of providing an exhaustive overview on those steganography and watermarking techniques leveraging on the important properties of such a transform. The large number of algorithms operating in the image, video and audio context is first classified by means of a general approach, and then analyzed to highlight the advantages and disadvantages of each method. The chapter also gives a detailed discussion about the applicability of each reviewed and compared data hiding scheme, in order to identify the most appropriate candidates for practical applications.

Chapter 12 presents a new paradigm for rendering any watermarking scheme resistant to geometric attacks such as rotation, scale change or cropping. This is done by means of a new image transform to a Rotation, Scaling, and Translation (RST) invariant domain based on ideas from shape theory. The chapter also proposes extensions of this technique to video watermarking. An example is provided of how these ‘shape based’ concepts can be extended to more general relational databases, provided that an abstract notion of shape is employed.

The goal of chapter 13 is to provide important technical insights, as well as intuitive and well developed discussions, onto how multiple watermarks can be embedded efficiently into the same host signal. The chapter adopts communication and information theoretic inclinations, and argues that this problem has tight relationship to conventional multi-user information theory. By virtue of this tight relationship, the author shows that design and optimization of algorithms for multiple watermarking applications can greatly benefit from recent advances and new findings in multi-user information theory.

The last chapter in this section, chapter 14, presents the most significant approaches developed so far for the distribution of multimedia digital contents with copyright protection, highlighting their most

interesting features. The approaches may be classified into two categories: systems that try to prevent unauthorized uses of the contents, and systems whose purpose is to detect unauthorized uses of the contents and to identify involved offenders. The chapter is focused on systems that fit in the second of these strategies; most of which are based on the use of multimedia watermarking techniques.

The last section of this book presents four chapters that deal with performance improvement of digital watermarking through optimization and hardware implementation. Chapter 15 suggests improving performance by treating watermarking as an optimization problem, and chapter 16 by using error correction codes. On the hand, chapter 17 gives a survey on how hardware implementations of image and video watermarking algorithms can accelerate watermarking speed and makes real-time watermarking feasible. The last chapter takes spread spectrum watermarking as a special case, and gives a detailed FPGA architecture for an actual watermarking system.

Chapter 15 looks at digital watermarking as an optimization problem to resolve the conflicting requirements of different parameters and properties of digital watermarking. The chapter presents a review of recent advances in the state-of-the-art algorithms for optimized watermarking techniques. Optimized watermarking methods are discussed from the rigorous mathematical analysis to theoretical derivations of algorithms with the aid of soft computing techniques. The design and implementation of optimized watermarking methods for the image, video and sound signals are discussed in the context of various diverse applications.

Chapter 16 describes how application of Error Control Coding (ECC) improves performance of watermarking schemes. The authors study various properties of watermarking systems, looking into their specific requirements, and then try to search for suitable error control code in order to boost the over all performance of watermarking techniques. The chapter also discusses the state-of-the-art research in this direction, and presents a watermarking method based on facts covered in the chapter.

The use of watermarking in real-time applications and consumer products, such as digital cameras and camcorders, dictates the development of hardware architectures. Chapter 17 presents a survey of existing hardware implementations of image and video watermarking. It first discusses the design issues and implementation challenges in image and video watermarking with emphasis on computational complexity aspects. This is followed by a classification and detailed survey of the different hardware implementations reported in the literature. Future perspectives to address the challenges of hardware architecture design for image and video watermarking are then discussed.

The last chapter, chapter 18, describes a special hardware implementation of a spread spectrum (SS) watermark system. It first presents a brief review on the hardware implementation of digital watermarking algorithms, followed by the development of a hardware architecture for a spatial domain and fast Walsh transform (FWT) domain Spread spectrum (SS) watermark system design using field programmable gate array (FPGA) techniques. Few challenges for hardware design of watermarking algorithms are then described with an objective to give an idea how to develop watermarking algorithms so that it can be implemented in hardware.

Section 1

Digital Image Watermarking

Chapter 1

Two Spatial Watermarking Techniques for Digital Images

Dumitru Dan Burdescu

University of Craiova, Romania

Liana Stănescu

University of Craiova, Romania

Marian Cristian Mihăescu

University of Craiova, Romania

ABSTRACT

The rapid growth of digital multimedia technologies brings tremendous attention to the field of digital authentication. Digital watermarking has become widely recognized as an effective measure for copyright protection of multimedia data. The owner or the distributor of the digital images can insert a unique watermark into copies for different customers or receivers, which will be helpful to identify the source of illegal copies. In this chapter the authors present two original spatial authentication techniques for digital images. These new algorithms yield an invisible watermark that is robust to various kinds of attacks. The main principle is the utilization of a virtual (2D or 3D) graph embedded into the digital images. Then, the colors of some vertices of the virtual graph are slightly modified for obtaining the watermark. The proposed techniques modify pixels or voxels of the object by a spatial watermark insertion scheme. These techniques can be used for all kinds of digital images, color or black and white, and the new algorithms produce an invisible robust watermark. The techniques lower the computational complexity that normally rises with the traditional watermarking algorithms. This approach reduces computation and implementation complexity of the algorithms. These techniques seem to replace advantages of the transform domain techniques with those of the spatial domain techniques.

INTRODUCTION

Multimedia content is vulnerable to large scale copying and redistribution through easily accessible

networks. Unauthorized digital copying is a major concern for multimedia content providers.

In many contexts it is essential to be able to tell if a message is authentic or if it has been modified by an adversary. This applies for instance to forensic photography, where someone may want to forge

DOI: 10.4018/978-1-61520-903-3.ch001

or disable evidence, by doctoring an image. The most well-established solutions are cryptographic techniques such as digital signatures or message authentication codes (MAC). These solutions are mature and widely trusted. The signature or the MAC is transmitted together with the message, and the receiver can verify that the message fits the MAC or signature. While an adversary can modify the message, it is computationally infeasible to generate a matching MAC or signature. Unfortunately after decrypting, this method fails to any type of duplication or image retransmission.

Alternative solutions have been proposed in digital watermarking. This new emerging technology, digital watermarking, provides a promising way to protect a digital image from illicit copying and manipulating.

Digital watermarking is a method to hide some information that is integrated with a multimedia object (Sequeira and Kundur 2001). The object may be any form of multimedia, such as image, audio, video, or text. A digital watermark is an invisible signal that is embedded directly in the digital media (images, audio, video, 3D objects, etc.) so that it is inseparable from the digital media.

Digital watermarking, in general, allows us to embed a message (watermark) within another data file (such as an image) called the host. The embedding is done by imperceptible changes to the host, so that the watermarked host can replace the original for all practical purposes. A basic application of watermarking is to extend a legacy data structure. There are (Cox et al. 2007) presented two advantages of digital watermarking for authentication. Firstly, the authentication information is hidden as an inherent part of the message (host). Therefore it can be incorporated in a legacy data structure. Thus it avoids the appended signature of cryptology. The other advantage is more subtle. Because the watermark is hidden in the data, it will undergo the same transformations as the data. By observing the transformed watermark, it may be possible to determine the exact transformation the message has undergone, and possibly undo it.

The two most common methods used for digital image watermarking are spatial and spectral domain methods (Bassali et al. 2000, Mukherjee et al. 2004). Spectral domain methods have several advantages over the spatial domain methods. First, they are more robust, since the watermark is inserted in the perceptually significant parts of the image, which corresponds to the mid-frequency range. Second, they are well-suited to resist the compression attacks. Third, some transform domain algorithms are robust against specific geometric transformations such as Discrete Fourier Transform (DFT) which is robust to most affine transformations. Although transform domain algorithms have more advantages in providing robustness, sometimes it is difficult to satisfy imperceptibility constraints in the spatial domain simultaneously with the spectral domain constraints.

In order to take full advantage of both the spatial and the spectral domains, researchers started looking at the joint time-frequency representation of the image, which gives a more comprehensive representation of the image compared to looking at each domain individually (Barkat et al. 2003). This approach also provides flexibility in the amount of data that can be hidden inside an image (Zheng et al. 2007).

Watermarking of 3D meshes has received a limited attention due to the difficulties encountered in extending the algorithms developed for 1D (audio) and 2D (images and video) signals to topological complex objects such as meshes. Other difficulties arise from the wide variety of attacks and manipulations 3D watermarks should be robust to. For this reason, most of the 3D watermarking algorithms proposed so far adopt a non-blind detection (Ohbuchi et al. 2004).

There is a wide range of applications of digital watermarking including copyright protection, authentication, finger-print, copy control and broadcast monitoring etc. For different kinds of applications digital watermarking should show different properties (Cox et al. 2000). Many

watermarking algorithms have been proposed by researchers to maintain the originality and integrity of networked digital multimedia contents. Invisible-robust watermarking of digital images is one of the leading research areas.

Here we mainly discuss the copyright protection problem for digital images. For this kind of application, digital watermarking should have properties such as robustness, high detection reliability, imperceptibility for detection, redundancy in distribution and resistant to picture's distortions.

Many image watermarking algorithms for copyright protection have been proposed. They can be generally classified onto two categories: spatial domain watermarking schemes and spectrum domain watermarking schemes. Algorithms belong to the first category embedded directly a watermark by modifying the pixel value of an image. Recent research focuses on spectrum domain watermarking schemes, which embed a watermark by modifying the spectrum coefficients after an image has been transformed to the spectrum domain such as, Discrete Cosine Transform (DCT) domain (Lu et al. 2000), Discrete Fourier Transform (DFT) domain (Lin et al. 1999), Discrete Wavelet Discrete (DWT) domain (Cheng 2001) and fractal domain (Puate et al. 1996, Mohanty et al. 2006). To achieve efficient trade-offs between robustness and invisibility some authors (Voloshynovskiy et al. 2000) propose to adjust the watermark strength according to properties of the Human Vision System (HVS) so that the distortion introduced by the watermark is below the Just Noticeable Difference (JND). One problem with the current watermarking algorithms is that most of them only have one key. The same key is used for both watermarking embedding and detection. Anyone who holds the key and can pass the watermark verification is supposed to be the owner. But what happens if two or more people create an image collaboratively. With the current watermarking schemes each of them is assigned the same key. The proposed schemes here solve

this problem by offering the possibility of embedding multiple keys.

RELATED WORK

In this section, we discuss selected important contributions from the existing literature.

Electronic watermarking was invented in 1954 by Emil Hembrooke of the Muzac Corporation (Cox and Miller 2002). Experts from computer science, cryptography, signal processing, and communications have worked together to develop watermarks suitable for various applications. Digital watermarking provides value-added protection on top of data encryption and scrambling for content protection and effective digital rights management. Digital watermarking raises a number of questions (Cox and Miller 2002), and still need to be addressed. This will allow the development of fool proof commercial watermarking systems (DWA 2008, <http://www.digitalwatermarkingalliance.org/>).

Watermarking has many different applications (Bender et al. 2000; Cox and Miller 2002), such as ownership evidence, fingerprinting, authentication and integrity verification, content labeling and protection, and usage control. Watermarking schemes do not work effectively for all types of media and universally for various diverse applications. Depending on the target application and type, each watermark must satisfy certain characteristics (Mintzer et al. 1997). The success of any watermarking scheme is determined by its performance against intentional and unintentional attacks (Petitcolas et al. 1999; Voloshynovskiy et al. 2001). The requirements for fulfilling desired characteristics and for succeeding against attacks are mutually conflicting (Heileman et al. 1999; Servette et al. 1998). Several benchmark suites for testing performance robustness that combine many possible attacks into a unified framework are available (Voloshynovskiy et al. 2001; Guitart et al. 2006; Khan and Mirza 2007).

A watermarking scheme consists of three parts: the watermark algorithm, the encoder, and the decoder and comparator (Memon and Wong 1998). The watermarking algorithm incorporates the watermark into the multimedia object, whereas the verification algorithm authenticates the object by determining the presence of the watermark and its actual data bits. Available techniques use different transform domains to embed the watermark inspired by information coding and image compression. Based on human perception, digital watermarks can be either visible or invisible. A visible watermark is a secondary translucent mark overlaid on the primary image and is visible to a viewer on careful inspection. The invisible watermark (may be either robust or fragile) is embedded in such away that modifications made to the pixel value are perceptually unnoticeable and can be recovered only with an appropriate decoding mechanism (Mohanty and Bhargava 2008). In multiple watermarking, two or three watermarks are embedded for copyright protection, content authentication, or captioning (Hua et al. 2001). Since starting with IBM's Vatican Library project (Mintzer et al. 1996), visible watermarking technology progressed significantly (Topkara et al. 2005). Invisible-robust watermarking was initiated by the research team of Cox (Cox et al. 1997), Craver (Craver et al. 1998), and others. This chapter is for invisible-robust watermarking.

The problem of 3D image watermarking is a relatively new area as compared to 2D image watermarking. Watermarking techniques (Cox et al. 2001, Petitcolas 1999) developed for other kinds of multimedia such as audio, video, and 2D images data are not generalized enough to be applicable to 3D images. The problem of watermarking 3D images might be solved by using solutions related to other representations of 3D objects. Even if 3D objects can be represented in several different ways (e.g. NURBS, voxels, implicit surface, polygonal meshes) most of the existing 3D watermarking algorithms work on polygonal meshes since this representation is the

lowest common denominator of the other ones (i.e. it is easy to convert the other representations to meshes). For example the watermark may be inserted by altering mesh attributes such as vertex coordinates or vertex connectivity.

The spatial description of a 3D mesh includes both geometry and connectivity information. Spatial techniques modify the spatial description to embed information. 3D meshes are one such form, where data set is represented as a graph by geometry (vertices or points) and topological (connectivity) information. A lot of watermarking techniques have been proposed for 3D meshes. These techniques are based on spatial information or some kind of transform. Spatial techniques (Alface et al. 2005, Bors 2006, Harte et al. 2002, Zafeiriou et al. 2005) operate on the data, whereas transform techniques (Petitcolas 1999, Ohbuch et al. 2004) apply mathematical techniques to derive information from the original data. Some of the blind techniques for 3D meshes operate on the geometry (vertex or point) and topological (edges) information of the 3D mesh model. Mesh-based blind watermarking techniques are relatively vulnerable to connectivity attacks, such as re-meshing or mesh simplification (Praun et al. 1999). Different methods have been developed for watermarking point-sampled surfaces (Agarwal and Prabhakaran 2007). Some of the blind methods such as (Zafeiriou et al. 2005) try to find the center of gravity and use principal component analysis for watermarking. However, such methods are vulnerable to cropping as the center of gravity shifts and the watermarks are lost. Alface et al. (2007) also localizes watermarks in features (e.g. head of the Stanford bunny model) of 3D models. The basic idea is to identify features of 3D models, and try to achieve robustness and imperceptibility per feature watermark. However, these techniques are comparatively less robust to global attacks as compared to local attacks.

Invisible watermarking has the greatest need for standardization (Mintzer et al. 1998). For an invisible watermarking technique, the robust-

ness property alone is not sufficient to guarantee content protection (Craver et al. 1998). Application specific watermarking techniques need to be developed with standard encoder-decoder systems incorporated in multimedia devices. The legal framework provided for the applicability of digital watermarking is through the Digital Millennium Copyright Act, which protects against deliberate removal of, or attacks on, the watermark (Eskicioglu and Delp 2001). Recently, the use of watermarking is being explored for digital video broadcasting by the DWA (2008). With respect to strategies that break watermarking schemes, the work of Holliman and Memon (2000) describes a class of attacks on certain block-based oblivious watermarking schemes.

One spatial domain watermarking technique which is invisible, robust to geometric attacks and based on affine transformations is presented by Wu et al. (2001). Pixels in a neighborhood in a real image are usually highly correlated, and this assumption forms the basis of many techniques such as predictive coding for deciding watermark locations (Dugelay and Roche 2000). Several techniques first apply a transform (e.g., discrete Fourier, discrete cosine, Mellin-Fourier, wavelet) to the image, insert the watermark in the transformed space, and then invert the transform. The noise introduced by the watermarking signal is thus spread over the whole image. A direct application of these techniques to a relation will introduce errors in all of the attribute values, which might not be acceptable. Furthermore, such a watermark might not survive even minor updates to the relation. All these methods fail because they are easily detected. For example, the STIRMARK open source software tool can detect any spectral change of the digital image. The open source software STIRMARK available on the Web generates many of attacks as in the spectrum domain it can be filtering, or compression or adding another watermark over the first one. The STIRMARK software generates random rotations and distortions on blocks of the image

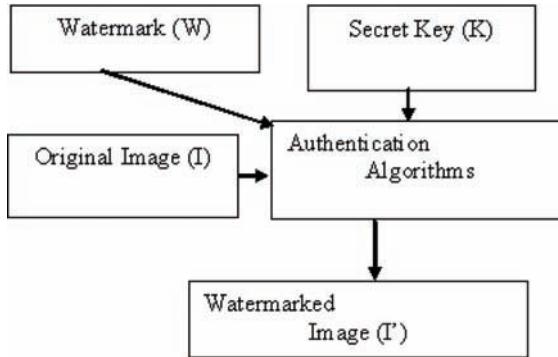
and scaling and cropping of images. The result is very slight alterations on image, but watermarks are usually heavily damaged.

Because watermarking is used for copyright protection, researchers investigate the design of high performance, low-power hardware-based watermarking systems for real-time applications. Despite significant advances, research still needs to address many challenges related to attack resilience and robustness. Much of the current research attempts to embed a pseudorandom sequence as a watermark; however, a source-based watermark like a unique identifiable color logo is more appealing for easy identification of ownership, authentication, and acceptance as legal evidence. Thus, we address the issue of strategically creating and implanting a watermark with the dual purpose of attack prevention and detection.

WATERMARKING TECHNIQUE FOR 2D IMAGES

Several image watermark schemes have been developed in the past few years, both spatial and frequency domains are used for watermark embedding. Spatial watermarks are constructed in the image spatial domain, and embedded directly into an image's pixel data (Burdescu, 2004). Since the meaning of multimedia data is based on its content, it is necessary to modify the multimedia bit-stream to embed some codes, i. e. watermarks, without changing the meaning of the content. The embedded watermark may represent either a specific digital producer identification label, or some content-based codes generated by applying a specific rule. Because the watermarks are embedded in the data content, once the data is manipulated, these watermarks will also be modified such that the authenticator can examine them to verify the integrity of the data. All watermarking methods share the same building blocks – an embedding system and the watermark extraction or recovery system.

Figure 1. Block diagram of a watermark embedding system



A generic embedding system (Figure 1) should have as inputs: a cover data/image (I), a watermark symbol (W) and a key (K) to enforce security. The output of the embedding process is always the watermarked data/image (I').

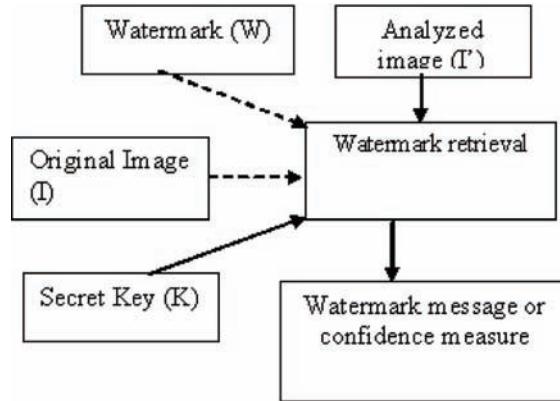
The generic watermark recovery process (Figure 2) needs the watermarked data (I'), the secret key (K) and depending on the method, the original data (I) and/or the original watermark (W) as input while the output is the recovered watermark with some kind of confidence measure for the given watermark symbol or an indication about the presence of watermark in the cover image under inspection.

The authentication technique presented in this paper applies principles not used so far. In proposed technique, each image is marked by altering some pixels with a coefficient obtained with a given algorithm. The image pixels are altered according with the formula:

$$D(i,j) = C(i,j) + a \cdot M \cdot W \quad (1)$$

Where: $C(i,j)$ is the original value of the pixel at position (i,j) ; $D(i,j)$ is the value of authentication symbol of the same pixel; “ a ” is a scaling factor (which may be a constant or a variable according with user’s specification); M represents the block number where the key is introduced; W is an au-

Figure 2. Generic watermark recovery scheme



thentication coefficient which may have take the values +1 or -1 (but there is possibility to change the value according with user’s specification).

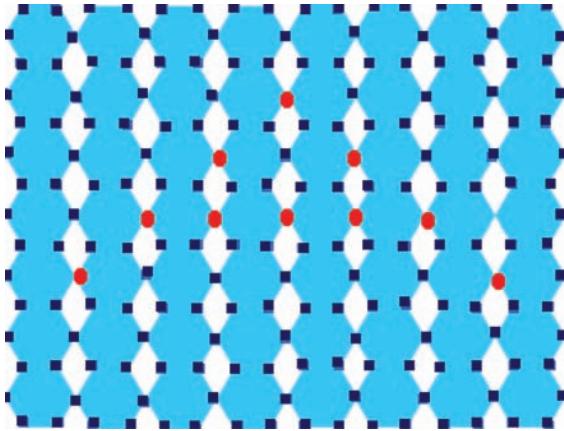
The main idea of presented technique is to build a virtual graph which has in its original nodes the pixels from original image.

The graph may have cells with the shape as hexagons in which the length of edges represents the number of pixels (e.g. 3, 4, 5 or more pixels). For preserving flexibility there may be considered any virtual graph which has the nodes placed as regular geometric shapes and the number of pixels that are considered as edge length is left at user’s discretion. In this way, the original image is seen as a virtual graph in whose nodes are inserted the authentication symbol along with the used defined key.

The image of the virtual graph, in which the cells are hexagons, is presented in Figure 3 in which the authentication symbol is designed in red (it has been chosen a random high contrast color different than the one obtained by the technique). In this figure, the letter “A” was drawn as key into the nodes of the virtual graph.

Thus the image is viewed as a graph not as a pixel matrix. The vertices represent the pixels and the edges represent neighborhood between pixels. The algorithm for this operation is as following:

Figure 3. Virtual graph and key



```

PROCEDURE Construct_Graph(Image
I,edge)
BEGIN
    for * i->0,width/edge - 3*edge
        for * j->0;height/3
            if (i modulo 3==0)
                then
                    * if (jmodulo 2 ==0)
                        then bmap[i]
                            [j]=bmp.bmap[edge*i]
                            [edge*j+edge-1];
                        end if;
                    * if(jmodulo 2==1)
                        then bmap[i]
                            [j]=bmp.bmap[edge*i]
                            [edge*j+edge+2];
                        end if;
                end if;
            if (i modulo 3==1)
                then
                    * if (jmodulo 2 ==0)
                        then bmap[i]
                            [j]=bmp.bmap[edge*i-1]
                            [edge*j-edge];
                        end if;
                    * if (jmodulo 2 ==1)
                        then bmap[i][j]=bmp.
                            bmap[edge*i-1][edge*j+edge*2];
                end if;
            end if;
        end for j;
    end for * i;
END

```

```

        end if;
    end if;
    if (i modulo 3==2)
        then
            * if(j modulo 2==0)
                then bmap[i]
                    [j]=bmp.bmap[edge*i-2]
                    [edge*j+edge-1];
                end if;
            * if(j modulo
2==1)
                then
                    bmap[i][j]=bmp.bmap[edge*i-2]
                    [edge*j+edge+2];
                end if;
            end if;
        end for j;
    *output the graph g
end for * i;
END

```

Proposition 1

The total running time of a call of the procedure Construct_Graph (Image I, edge) is $O(n*m)$, where “n” is the width and “m” is the height of the digital image.

Proof

It can be observed that the first FOR loop of the algorithm is executed at most once for a pixel of the width of image. Hence, the total time spent in this loop is $O(n)$. The second FOR loop processes the pixels on the height. Hence, the total time spent in this loop is $O(m)$. So, the total time spent in these loops is $O(n*m)$, because are processed all pixels of the image at most once. From previous statements is inferred that the total running time of this procedure is $O(n*m)$.

For introducing the authentication symbol a block is chosen (an entire image or a part of it represents a block) from the image(i.e. from virtual graph). Hence the block may be represented by

entire graph or a part of it. A node (i,j) of virtual subgraph is chosen from the block and from this one it will start entering the key (K). This key may be a digit, or a letter, or any graphical sign that will be “drawn” using the nodes of the virtual graph. In the nodes of the virtual graph that are chosen to determine the “drawing” of the key, the color of the pixel will change according with formula (1).

For example, in color images the color of the three color channels (RGB format) will change by addition or subtraction of W coefficient computed as a function of the color channel of a neighbour pixel. In our case, it is taken as basis the down pixel of the node that is taken into consideration. The computation of W coefficient for each channel may be more flexible. For example, it may be considered the average of colour coefficients for the channels of neighbour pixels, around the graph’s node. The entire process starts from a node of coordinates (m0, n0) and continues within all image nodes (virtual graph) such that the key spreads in all original image (not only in some areas of the image as in other methods that use spatial key).

The algorithm for marking the image graph is shown below:

```

PROCEDURE mark_graph (Graph
bmap)
BEGIN
  *choose 2 nodes in the graph
  (m0, n0) and (m1, n1)
  for * i->m0, n0
    for * j ->m1, n1
      change_color(i, j, const)
      end for j;
    end for i;
END

```

Proposition 2

The total running time of a call of the procedure Mark_Graph (Graph bmap) is O(n²), where “n”

is the number of nodes of graph attached to the image.

Proof

It can be observed that the first FOR loop of the algorithm is executed at most once for each node of the graph. Hence, the total time spent in this loop is O(n). The second FOR loop processes the pixels of node which has the same color of its neighbor. Thus the inner FOR loop processes the nodes of unvisited neighbor. So, the total time spent in these loops is O(n²), because are processed all nodes of the graph at most once. From previous statements is inferred that the total running time of this procedure is O(n²).

For detecting the key and the authentication symbol of an authenticated image I’ it is considered the original virtual graph in which the elements of the embedded key are searched. If a certain number of marked nodes is found (a certain threshold may be imposed) according to the presented algorithm (i.e. with what has been marked in initial virtual graph) it means that the image belongs to an unknown owner (each owner has its own key).

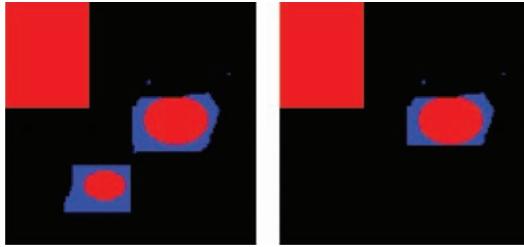
The algorithm for obtaining the key is the following (untransformed watermarked image):

```

PROCEDURE detect_untransformed
(Image I,int edge,int w,int h,
int percent)
BEGIN
  *construct_graph
  (I,edge);
  count=0;
  for * i->m0, n0
    for * j->m1, n1
      if (color(bmap[i][j]) ==
      color(bmap[i+1][j])) -1)
        count = count +1;
      end if;
    end for j;
  end for i;

```

Figure 4. Experiment with cropped image



```
*output percent of similitude
between the original marked im-
age and the image verified;
END
```

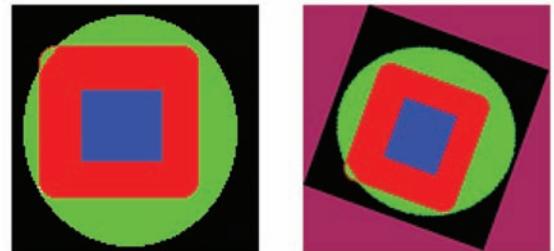
There is a variety of modern and possible sophisticated attacks which the technological advancement has posed in the current age. The general transformations (attacks) that can be done on images (Fei et al. 2004) are: rotation, redimension, compression (transforming the image to JPEG) and cropping. Because it is not known what transformation (attack) the user did, all these transformations are verified one by one and the percentage of similitude between the original image and the verified one is returned.

The previous algorithm of untransformed image may be applied if the image is cropped. In this case it may be possible to lose some marked pixels depending on the position where the image was cropped.

In Figure 4, the first image is the image marked and the second one is the image marked and cropped. The detection algorithm detects this cropped image in percent of 88.88% (Burdescu et al. 2006).

In the case of image rotation (angle of 90, 180 and arbitrary) all the image nodes are verified because the nodes' position is changed. We search the nodes for which all of the three color channels have the values like the color's channels of the bottom pixel minus one (or a certain constant). Before verifying these nodes, the image

Figure 5. Experiment with rotated image



is dimensioned again to the initial dimensions at which the image is marked.

In the Figure 5, the first image is the marked image and the second is the image marked and rotated by 30 degree.

The algorithm for detecting the drawn key in the case of rotating the image is the following:

```
PROCEDURE detect_rotated (Im-
age I,int edge,int w,int h, int
percent,int constant)
BEGIN
    *redimension(I,w,h);
    *construct_graph (I,edge);
    count=0;
    for * i->0,w
        for * j->0,h
            if (color(bmap[i+1][j])-
constant<=color(bmap[i][j]) <=
color(bmap[i+1][j]) +constant)
                then
                    count=count+1;
                end if;
            end for j;
        end for i;
    *output percent of simili-
tude between the original marked
image and the image verified;
END
```

The experiments showed that in the case of a rotation by 90 and 180 degree, the constant is zero,

Table 1. Results for experiment with rotated image

Rotation Angle	Similitude Percent
30	33.33%
60	33.33%
90	100%
180	100%

but in the case of a rotation by arbitrary angle the constant is very big (100).

The experiment uses the marked image which was rotated with different angles. From experiments resulted the following percentage of similitude between the marked image and the marked rotated image, as shown in the Table 1.

The implemented authentication algorithm entirely detects an image that was transformed to JPEG, only if the image is compressed with a quality of 100% and 80%. For image processes (compression, decompression), was used ADOBE PHOTOSHOP. The variable m_0, n_0, m_1, n_1, h, w are known, being the same variables that are used in the process of image marking. The color of pixels arranged into nodes selected by us for marking the image is changed because of transformations supported by the image. Then the color of these pixels is searched within a certain interval.

The algorithm for detecting the drawn key in the case of compressing the image is the following:

```

PROCEDURE detect_jpg (Image
I,int percent, int constant)
BEGIN
*decompressed(I);
*construct_graph (I, edge);
count=0;
for * i->m0,n0
    for * j->m1,n1
        if (color(bmap[i+1]
[j]) -constant <=color(bmap[i]
[j]) <= color(bmap[i+1][j])
+constant)
            then count = count
+1;
    end if;
end for j;
end for i;

```

```

*output percent of similitude
between the original marked im-
age and the image verified;
END

```

The experiments prove that a good value for this constant is 30 (Burdescu et al. 2006).

In the case when we want to detect an image that was enlarged the results are weaker.

The algorithm for detecting the drawn key in the case of enlarging the image is the following:

```

PROCEDURE detect_larged (Im-
age I, int edge,int w,int h, int
percent,int constant)
BEGIN
*redimension(I,w,h);
*construct_graph (I,edge);
count=0;
for * i->0,m
    for * j->0,n
        if (color(bmap[i+1][j])
-constant <=color(bmap[i][j]) <=
color(bmap[i+1][j]) +constant)
            then count = count
+1;
        end if;
    end for j;
end for i;
*output percent of similitude
between the original marked im-
age and the image verified;
END

```

The experiments show that a good value for this constant is 70 (Burdescu et al. 2006).

WATERMARKING TECHNIQUE FOR 3D IMAGES

There are many formats for 3D model representations of real objects. Depending on the information needed for that object, the structure can store position information (the x, y, z coordinates of a point), color information (the color of a point in the desired format – i.e. RGB), drawing primitive information. The input file of model will also include the number of used primitives of each type. Every object is represented using elementary structures called primitives. There are three types of primitives: contour primitive – points and lines, 2D empty (not filled) objects, surface primitive – 2D filled objects (i.e. filled triangles), volume primitive – 3D filled objects. The primitive information consists of primitive type, color, sometimes texture (a pattern applied to the primitive) or orientation (described by a primitive normal – i.e. the plane normal for surface primitives).

The algorithms described here are suitable for any type of primitives or model, but, for this application, the scene is scaled such that they are bounded in a cube with 500 voxels edges. The cube is defined by the points (0, 0, 0) and (500, 500, 500). Different values can be chosen for the dimension of the cube or for its vertices, or the enclosing volume can be a rectangular prism. These values were chosen only for presented purposes. The cube “contains” slices. Every slice will be a 500 x 500 image. The voxels that are not part of the model will be considered as having a white color.

The decomposition of 3D digital images using basis functions (that are localized in spatial position, orientation and scale) has proved to be extremely useful in a series of applications (such as image compression, image coding, noise removal and texture synthesis). Such decomposition reveals various statistical regularities that can be exploited to develop techniques for a number of applications. One of the constraints that are imposed to

the model file is that it can be bounded by the chosen cube (in our case, the cube defined by the points (0, 0, 0) and (500, 500, 500)). When a model is read from the file, the program computes its lengths on each axis (denoted lx_old, ly_old, lz_old) and scales the model to (lx, ly, lz), such that all of them are less than the selected values (sel_lx, sel_ly, sel_lz) for the bounding box (in our case 500). Then, it creates a {sel_lx by sel_ly by sel_lz} matrix for the model. For each primitive in the model the procedure computes which points are included in it, and then assigns the color to the corresponding element in the matrix. The remaining pixels are colored white. The algorithm for calculating cube, bounding boxes is as follows:

```

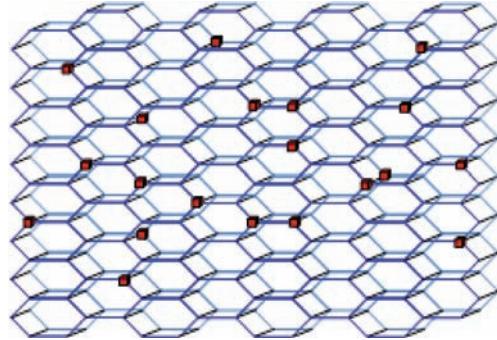
PROCEDURE read_model;
BEGIN
    compute lx_old, ly_old, lz_
old
    read cx10, cy10, cz10 //lower
    left corner of the bounding box
    read cx20, cy20, cz20 //upper
    right corner of the bounding box
    sel_lx<-cx20-cx10; sel_ly<-
    cy20-cy10; sel_lz<-cz20-cz10
    scale model to lx, ly, lz
    create sel_lx x sel_ly x
    sel_lz matrix M
    for i=0..sel_lx-1
        for j=0..sel_ly-1
            for k=0..sel_lz-1
                if (i,j,k) Model
                then M(i,j,k) =
Model(i,j,k).color
                else M(i,j,k) =
white
            end if;
        end for k;
    end for j;
end for i;
END;
```

Although this type of structure allows the retaining of 3D information, the computer's display is still 2D. In order to show some results and sustain them by proof, 2D images are needed. For that, a series of significant slices are extracted from the represented 3D model. First, the slicing plane "p" is selected. In order to select the slicing planes a virtual spatial network is used. This network is formed of a set of elementary 3D objects (cells with 12 - cube, 20, 36 or more edges). Each of these cells is formed starting from a basic 2D shape (square, hexagon, octagon) on which is created the corresponding 3D primitives. The faces of these primitives determine the slicing planes. The edge length and the type of primitive are selected considering the degree of similitude required by the query. If the desired degree of similitude is very high, then a network with cells that have a greater number of edges and a smaller edge length will be selected, thus allowing a better sampling; otherwise, the virtual network will be formed of cells with a smaller number of edges and a bigger edge length. In the presented paper the 2D primitive used is the hexagon. After slicing the object on the determined planes, a matrix M2D having the corresponding remained dimensions is initialized (if xOy is selected as plane "p", then the matrix is $lx * ly$). The elements of M2D are assigned the values from M, but with the third coordinate fixed to "p". Below is the algorithm for the slice through a cube by a plane parallel to xOy, the other cases being similar.

```
.....
for i=0 to lx-1
for j=0 to ly-1
M2D(i,j)=M(i,j,p)
    end for j;
end for i;
.....
```

The method implemented is simpler and requires less complex computations than the general method (e.g. polygonal meshes).

Figure 6. The virtual graph embedded into 3D image



The main idea of watermarking technique is the use of the 3D virtual graph that is considered embedded in the image. In our case this virtual graph is composed by the cells of a honeycomb. Then, the 3D model is considered as a sequence of slices that represent sections of the 3D model.

That means, for some nodes of virtual graph, the value of the voxel is changed according to the following formula:

$$D(i,j,k) = C(i,j,k) + a*M*W \quad (2)$$

Where: $C(i,j,k)$ is the original value of a voxel at position (i,j,k) ; $D(i,j,k)$ is the watermarked value of the same voxel; 'a' is a scalar factor (here a is chosen constant, but can be a variable of the position to improve the invisibility of the watermark and its detection);

M is the number of the block (or slice) where is embedded the key, but may be one for entire image; and W is the watermark coefficient to be embedded. In our work, W could take the values +1 or -1 (one can easily extend the implementation by modification of M).

This watermarking scheme is secure since any degree of "degradation" of the digital image is applied, the watermark remains in the virtual graph nodes. This is due to the fact that the voxels whose colors are modified are in relationship with the colors of their neighbors. So, a "degradation"

of a certain portion of the image will produce the automate modification of the nodes' color that are contained in the watermark key.

For implementation of the watermarking algorithm we took a slice-based approach to 3D objects watermarking. From the 3D objects we extract a certain number of key-slices. The number of slices and their spatial position depend on the chosen algorithm for the key insertion. For example, these slices can be chosen in the same vertices of the virtual 3D graph (or another scheme can be chosen). This way, in the 2D slices, some hexagons will be obtained representing parts of the virtual graph. The pixels of each image key-slice are arranged into hexagons like in Figure 1. Then the 2D key-slice is viewed as a virtual graph not as a pixel matrix. The vertices represent the voxels and the edges represent neighborhood between voxels. The algorithm for this operation is as follows:

```

PROCEDURE construct_graph_from_
keyslice (Slice K, edge);
BEGIN
for i=0.. width/edge - 3*edge
    for j=0.. height/3
        if i modulo 3=0
            then
                if j modulo 2=0
                    then K[i]
[j]=K[edge*i] [edge*j+edge-1];
                end if;
                if j modulo 2 =1
                    then K[i]
[j]=K[edge*i] [edge*j+edge+2];
                end if;
                end if;
                if i modulo 3=1
            then
                if j modulo 2 =0
                    then K[i]
[j]=K[edge*i-1] [edge*j-edge];
                end if;
                if j modulo 2 =1

```

```

                    then K[i]
[j]=K[edge*i-1] [edge*j+edge*2];
                end if;
            end if;
            if i modulo 3 =2
                then
                    if j modulo 2 =0
                        then K[i]
[j]=K[edge*i-2] [edge*j+edge-1];
                    end if;
                    if j modulo 2 =1
                        then K[i]
[j]=K[edge*i-2] [edge*j+edge+2];
                    end if;
                end if;
            end if;
        end for j;
    end for i;
    *output the graph
END

```

Proposition 3

The total running time of a call of the procedure `construct_graph_from_keyslice(Slice K, edge)` is $O(m*n)$, where “m” is the width and “n” is the height of image.

Proof

Recall that the number of pixels of image is $m*n$, where “m” is the width and “n” is the height of image. Observe next, that the first loop FOR of the algorithm is executed at most once for each pixel of the image. The inner loop FOR processes the pixels of an unvisited neighbor. So, the total time spent in these loops is $O(m*n)$, because are processed all pixels of image at most once. The result of the previous statements is that the total running time of this procedure is $O(m*n)$.

As presented above, the image is arranged into hexagons having different dimensions of edges. For introducing the key W, certain nodes from the 2D virtual graph (i, j) will be considered, which may be selected for representing a

letter, a number or a function. In these nodes the three color's channels of the considered pixel are changed depending on the three color channels of the bottom pixel minus one or another constant (const). We consider a started node having the coordinates (m0, n0) where the marking process started and an ended node where the process of marking ended. The algorithm for marking the image graph is shown below:

```

PROCEDURE mark_keyslice_graph
(Graph g);
BEGIN
    for *each keyframe
        *choose 2 nodes in the graph
        (m0, n0) and (m1, n1)
        for i=m0.. n0
            for j=m1.. n1
                *change_color(i, j,
                const)
            end for j;
        end for i;
    end for;
END

```

Proposition 4

The total running time of a call of the procedure `mark_keyslice_graph(Graph g)` is $O(k*p^2)$, where “k” is the number of key-slices and “p” is the number of nodes of graph attached to the image.

Proof

It can be observed that the second inner FOR loop of the algorithm is executed at most once for each node of the graph. Hence, the total time spent in this loop is $O(p)$. The third inner FOR loop processes the pixels of the node, which has the same color as its neighbor. This inner FOR loop processes the nodes of unvisited neighbor. So, the total time spent in these two loops is $O(p^2)$, because all nodes of the graph are processed at

most once. These operations are executed once for each key-slice. Hence, the total time spent in the first loop is $O(k)$. From previous statements is inferred that the total running time of this procedure is $O(k*p^2)$.

For reconstructing the marked image, only the graph's nodes corresponding to the selected key will be verified. If the marked voxel has the color in the interval [min, max] with respect to the color of the bottom pixel, then it will consider that this voxel was marked in conformity with the given algorithm. The values $\langle \text{min}, \text{max} \rangle$ resulted from a lot of experiments (Burdescu et al. 2008).

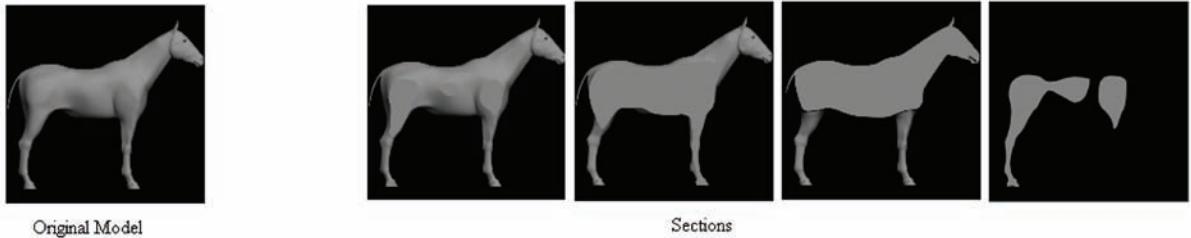
There is a variety of modern and possible sophisticated attacks which the technological advancement has posed in the current age. The transformations (attacks) that can be done on 3D models are: rotation, re-dimension, mesh optimization, tri-dimensional cropping. Because it is not known what transformation the user did, all these transformations are verified one by one and the percent of similitude between the original 3D model and the verified one is returned. The cube is centered at (0,0,0), so the corners are the coordinates (250,250,-250). The 3D model is centered in the cube, so the section plan by the center of the cube has the zero coordinates. If the 3D model is not transformed, it is applied the algorithm presented below for detection of marked 3D model:

```

PROCEDURE detect_untransformed
(3DModel 3M, int edge, int w,
int h, int percent);
BEGIN
    for *each slice K in 3M
        * construct_graph_
        from_keyslice (Slice K, edge);
    end for;
    count=0;
    for i = m0.. n0
        for j = m1.. n1
            if (color(K[i][j]) =
            color(K[i+1][j]))

```

Figure 7. The original model and the considered sections



```

        then count =
count +1;
        end if;
    end for j;
end for i;
*output percent of similitude
between the original marked im-
age and the image verified;
END

```

Observation 1

The previous and the following algorithms have the same time complexity (Proposition 4) because the operations are similar as in the previous one.

The detection algorithm detects the marked 3D model in ratio of 100% if the 3D image is untransformed.

Also this algorithm may be applied if the 3D model is cropped. In this case it may be possible to lose some marked pixels depending on the position where the slices are cropped. In Figure 7, the original model and its four slices sectioned at (-48.233, -22.429, 2.806, 43.09) are presented.

The detection algorithm detects this cropped 3D model in ratio of 91.1% (Burdescu et al. 2008).

In the case of 3D model rotation (angle of 90, 180 and arbitrary), all the considered slices nodes are verified because the nodes' position is changed. We search the nodes for which all of the three color's channels have the same values as the color's channels of the bottom pixel minus one (or a certain constant).

```

PROCEDURE detect_rotated
(3DModel 3M, int edge, int w,
int h, int percent, int con-
stant);
BEGIN
    for *each slice K in 3M
        *construct_graph
(3M,edge);
    end for;
    count=0;
    for * i=0.. w
        for * j=0.. h
            if (color(K[i+1]
[j]) -constant<=color(K[i][j])
<=color(K[i+1][j]) +constant)
                then count =
count+1;
            end if;
        end for j;
    end for i;
*output percent of similitude
between the original marked im-
age and the image verified;
END

```

The experiments showed that in the case of rotation by 90 and 180 degree, the constant is zero, but in the case of rotation by arbitrary angle the constant is very big (100). From experiments resulted the following percents of recognition between the marked 3D model and the marked rotated 3D model, as in the following Table 2.

In the case that we want to detect a 3D model, which was enlarged the results are weaker. The algorithm is:

```

PROCEDURE detect_larged (3DModel 3M, int edge,int w,int h, int
percent,int constant);
BEGIN
    for *each frame K
        *construct_graph
(K,edge);
    end for;
    count=0;
    for * i=0.. m
        for *j=0.. n
            if (color(K[i+1]
[j])-constant<=color(K[i][j]) <=
color(K[i+1][j]) +constant)
                then count =
count +1;
            end if;
        end for j;
    end for i;
    *output percent of similitude
between the original marked im-
age and the image verified;
END

```

From experiments resulted the following percents of recognition between the marked 3D model and the marked enlarged 3D model, as in the Table 3. The bigger the enlarged percents, the weaker the recognition percents will be. Experimental results show that a good value for this constant is 60. (Burdescu et al. 2008)

Since the performed transformation types are unknown all of them are verified and similarity percentage with authenticated image (it is considered a certain threshold for the number of nodes detected as being marked) is returned. For example if authentication symbol has been found in over 60% than it may be considered that the digital image has been authenticated.

Table 2. The percents of recognition obtained between the un-rotated and rotated marked 3D model, for different rotation angles

Rotation Angle	Similitude Percent
30	51.6%
45	51.6%
60	51.6%
90	100%
180	100%

Table 3. The percents of recognition obtained between the marked and enlarged marked 3D model, for different enlarged percents

Enlarged Percent	Recognition Percent
20	87.2%
40	74.5%
60	74.5%
80	71.3%
100	50.4%

DISCUSSION AND CONCLUSION

This chapter presented a novel approach for the creation of a spatial watermark that homogeneously adapts to the host image. A watermark insertion, extraction, and authentication scheme are proposed.

The significant contribution concerns three aspects: (a) two new original spatial authentication techniques for digital images, color or black and white, were presented; (b) in order to minimize the time complexity of the algorithms a virtual hexagonal grid-graph structure based on the image pixels or voxels was introduced; (c) these new techniques are sufficiently robust against a variety of modern and possible attacks as the experiments proved.

The key idea is the utilization of a virtual (2D or 3D) graph embedded into the entire digital images (color or black and white). The watermark may be

inserted in the most perceptually significant sub-image or in entire image, thus eliminating chances of its being subjected to severe digital attacks, which will reduce the value of the protection.

The experimental results presented on the quality and recognizability demonstrated the performance of the methods. It has tested the algorithms for several standard geometric attacks, such as rotation, crop, scaling. The quantitative measure of the extracted watermark shows the resilience to different tests. To increase watermarking security, it was adopted the method of invisible insertion of the watermark in the most significant region of the host image such that tampering of that portion with intention to remove or destroy the watermark will degrade the esthetic quality and value of the image.

The techniques insert a spatial protection key directly in the whole image, making the procedures for detecting it very hard. These presented techniques have the specific characteristics of imperceptibility for detection, redundancy in distribution, robustness in the extraction process and resistance for image's distortions. The presented techniques can be used on large scale in digital images authentication, with a minimum discomfort for usage and negligible costs.

As a disadvantage, based on experimental results, these methods are not sufficiently robust to attacks such as series of compression. However, the proposed watermarking schemes are secure because any degree of degradation we may apply the watermark remains in the virtual graph nodes. The advantage of the techniques is the possibility of using watermarking templates with special geometrical or special characteristics in the spatial domain. This is important for the proper recovery of the main watermark information in the frequency domain if an attack occurs. The main idea is the use of a virtual 2D or 3D graph, which is embedded into the original digital image. Spatial mask of suitable size is used to hide data with less visual impairments. From 3D objects we extracted a certain number of key-slices. It was

taken a slice-based approach to 3D watermarking. This scheme has much lower computational complexity and it also survives the cropping attacks where the transformed to the spectrum domain watermarks fail. This new algorithm produces an invisible watermark that is robust to various standard tests.

The method developed for digital watermarking for authentication of 2D and 3D images satisfies the necessary requests for the authentication technique and the series of presented transformations accounts for the fact that it resists possible attacks. The method is easy to implement and the experimentally determined robustness shows that it can be used without fear of being detected or changed. The watermarked image is not a new one because the number of the transformed pixels is very little ($n < <$ number of the image pixels, where 'n' is the number of nodes of virtual graph). In addition, the pixels of the watermarking are slightly changed thus the human eye cannot discern them. The watermark insertion process exploits average color of the homogeneity regions of the cover image. The complexity of the algorithms is proved to be $O(n^2)$, where 'n' is the nodes number of virtual graph for watermark. The developed authentication method works for all types of digital image color or black and white.

The presented algorithms provide a degree of freedom in choosing the number of graph nodes to be embedded, which makes it suitable for applications that embed flexible number of nodes.

The problem of "image collaboratively" may be easily solved by presented techniques. This way each author of an image area will use a private key that will be inserted within the image by using a virtual graph only in the block that belongs to that author.

In future works, we would like to extend the proposed watermarking techniques to enhance a still image with a watermarking scheme based on the insertion of mark in two fields: the multi-resolution and the spatial one. The resulting image may be entitled as a "double watermarked image".

The approach takes into consideration that nodes of the virtual graph will use frequency methods of modifying pixels. The main goal of this approach is to benefit from the advantages of its field in the watermarking process and to escape the drawbacks of each technique. The double watermarking scheme will use powerful error-correcting turbo codes to improve resistance against attacks.

REFERENCES

- Barkat, B., & Sattar, F. (2003). A new time-frequency based private fragile watermarking scheme for image authentication. *IEEE International Symposium on Signal Processing and Applications*, (vol. 2, pp. 363–366).
- Bender, W., Butera, W., Gruhl, D., Hwang, R., Paiz, F. J., & Pogreb, S. (2000). Applications for data hiding. *IBM Systems Journal*, 39(3-4), 547–568. doi:10.1147/sj.393.0547
- Bors, A. (2006). Watermarking Mesh-Based Representations of 3D Objects Using Local Moments. *Image Processing. IEEE Transactions on*, 15, 687–701.
- Burdescu, D.D. & Stanescu, L. (2004). A Spatial Watermarking Algorithm for Digital Images. *Control Engineering and Applied Informatics Journal*, 6(3), 57–63.
- Burdescu, D. D., & Stanescu, L. (2006). An Algorithm for Authentication of Digital Images. In *International Conference on Security and Cryptography*, Setubal, Portugal, (pp. 303-311).
- Burdescu, D. D., Stanescu, L., Ion, A., & Tanasie, R. (2008). A New 3D Watermarking Algorithm. In *3DTV Conference: The True Vision - Capture, Transmission and Display of 3D Video*, Istanbul, Tukey, (pp. 381 –384).
- Cheng, Q., & Huang, T. (2001). *An Image Watermarking Technique Using Pyramid Transform*. Proc. Of the ACM Multimedia.
- Cox, I., Miller, M., & Bloom, J. (2001). *Digital Watermarking: Principles & Practice*. San Francisco: The Morgan Kaufmann Series in Multimedia and Information Systems.
- Cox, I. J., & Miller, M. (1997). A review of watermarking and importance of perceptual modeling. *Proceedings of SPIE Human Vision and Imaging*, 3016, 92–99.
- Cox, I. J., Miller, M., & Bloom, J. (2000). Watermarking Applications and Their Properties. In *Proc. of Int. Conf. Information Technology: Coding and Computing*, (pp. 6-10).
- Cox, I. J., Miller, M., Bloom, J., Friedrich, J., & Kalker, T. (2007). *Digital Watermarking and Steganography*. San Francisco: Morgan Kaufmann.
- Cox, I. J., & Miller, M. L. (2002). Electronic watermarking: The first 50 years. *EURASIP Journal on Applied Signal Processing*, 2, 126–132. doi:10.1155/S1110865702000525
- Craver, S., Memon, N., Yeo, B. L., & Yeung, M. M. (1998). Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications. *IEEE J. Selec. Areas Comm.* 16, (4 May), 573–586.
- Dugelay, J. L., & Roche, S. (2000). A survey of current watermarking techniques. In Katzenbeisser, S., & Petitcolas, F. A. (Eds.), *Information hiding techniques for steganography and digital watermarking* (pp. 121–148). Norwood, MA: Artech House.
- DWA. (2008). Retrieved from <http://www.digitalwatermarkingalliance.org/default.asp>

- Eskicioglu, A. M., & Delp, E. J. (2001). An overview of multimedia content protection in consumer electronics devices. *Signal Processing Image Communication*, 16, 681–699. doi:10.1016/S0923-5965(00)00050-3
- Fei, C., Kundur, D., & Kwong, R. (2004). Analysis and Design of Watermarking Algorithms for Improved Resistance to Compression. *IEEE Transactions on Image Processing*, 13(2), 126–144. doi:10.1109/TIP.2004.823830
- Guitart, O., Kim, H. C., & Delp, E. J. (2006). Watermark evaluation test-bed. *J. Electr. Imag.*, 15(4).
- Harte, T., & Bors, A. (2002). Watermarking 3D models. In *Proceedings 2002 International Conference on Image Processing*, (Vol. 3, pp. 661 – 664).
- Heileman, G. L., Pizano, C. E., & Abdallah, C. T. (1999). Performance measures for image watermarking schemes. In *Proceedings of the 5th Baiona Workshop on Emerging Technologies in Telecommunications*, (pp. 149–152).
- Holliman, M., & Memon, N. (2000). Counterfeiting attack on oblivious block wise independent invisible watermarking schemes. *IEEE Transactions on Image Processing*, 9, 432–441. doi:10.1109/83.826780
- Hua, X. S., Feng, J. F., & Shi, Q. Y. (2001). Public multiple watermarking resistant to cropping. In *Proceedings of the 6th International Conference on Pattern Recognition and Information Processing*, (pp. 263–268).
- Khan, A., & Mirza, A. M. (2007). Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding. *Information Fusion*, 8(4), 354–365. doi:10.1016/j.inffus.2005.09.007
- Lin, C. Y., Wu, M., Lui, Y. M., Bloom, J. A., Miller, M. L., & Cox, I. J. (1999). Rotation, Scale and Translation Resilient Public Watermarking for Images. *IEEE Transactions on Image Processing*, 10(5), 767–782. doi:10.1109/83.918569
- Lu, C. S., Huang, S. K., Sze, C. J., & Liao, H. Y. M. (2000). Cocktail Watermarking for Digital Image Protection. *IEEE Trans. On Multimedia*, 2(4), 209–224. doi:10.1109/6046.890056
- Memon, N., & Wong, P. W. (1998). Protecting digital media content. *Communications of the ACM*, 41(7), 35–43. doi:10.1145/278476.278485
- Mintzer, F., Braudaway, G., & Yeung, M. (1997). Effective and ineffective digital watermarks. In *Proceedings of the IEEE International Conference on Image Processing*, 3, 9–12.
- Mintzer, F., Braudaway, G. W., & Bell, A. E. (1998). Opportunities for watermarking standards. *Communications of the ACM*, 41(7), 57–64. doi:10.1145/278476.278487
- Mintzer, F. C., Boyle, L. E., Cazes, A. N., Christian, B. S., Cox, S. C., & Giordano, F. P. (1996). Towards online Worldwide Access to Vatican Library Materials. *IBM Journal of Research and Development*, 40(2), 139–162. doi:10.1147/rd.402.0139
- Mohanty, S. P., & Bhargava, B. K. (2008). Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks. *ACM Trans. Multimedia Comput. Commun. Appl.*, 5(2), 12. doi:10.1145/1413862.1413865
- Mohanty, S. P., Guturu, P., Kougianos, E., & Pati, N. (2006). A novel invisible color image watermarking scheme using image adaptive watermark creation and robust insertion-extraction. In *Proceedings of the 8th IEEE International Symposium on Multimedia (ISM)*, (pp. 153–160).

- Mukherjee, D. P., Maitra, S., & Acton, S. T. (2004). Spatial domain digital watermarking of multimedia objects for buyer authentication. *IEEE Transactions on Multimedia*, 6(1), 1–15. doi:10.1109/TMM.2003.819759
- Ohbuchi, R., & Mukaiyama, A. (2004). Watermarking a 3D Shape Model Defined as a Point Set. In *Proceeding of CW* (pp. 392–399). Takahashi.
- Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—A Survey. In *Proc. IEEE* 87(7, July), 1062–1078.
- Praun, E., Hoppe, H., & Finkelstein, A. (1999). Robust mesh watermarking. In *Proceedings of SIGGRAPH*, 99, 49–56.
- Puate, J., & Jordan, F. (1996). Using Fractal Compression Scheme to Embed a digital Signature into an Image. In *Proc. of SPIE Photonics East Symposium*.
- Sequeira, A., & Kundur, D. (2001). Communications and information theory in watermarking: A survey. In *Proceedings of SPIE Multimedia Systems and Application IV*, 4518, 216–227.
- Servette, S. D., Podilchuk, C., & Ramchandran, K. (1998). Capacity issues in digital watermarking. In *Proceedings of the IEEE International Conference on Image Processing, ICIP-98*, (Vol. 1, pp. 445–449).
- Topkara, M., Kamara, A., Atallah, M., & Nitisoraru, C. (2005). ViWiD: Visible watermark based defense against phishing. [LNCS]. *Lecture Notes in Computer Science*, 470–484. doi:10.1007/11551492_36
- Voloshynovskiy, S., Deguillaume, F., & Pun, T. (2000). Content Adaptive Watermarking Based on a Stochastic Multi-resolution Image Modeling. In *Tenth European Signal Processing Conference*.
- Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J., & Su, J. (2001). Attacks on digital watermarks: Classification, estimation-based attacks and benchmarks. *IEEE Communications Magazine*, 39(9), 118–126. doi:10.1109/35.940053
- Wu, Y., Guan, X., Kankanhalli, M. S., & Huang, Z. (2001). Robust invisible watermarking of volume data using the 3D DCT. In *Proceedings of Computer Graphics International* (pp. 359–362). CGI.
- Zafeiriou, S., Tefas, A., & Pitas, I. (2005). Blind robust watermarking schemes for copyright protection of 3D mesh objects. *Visualization and Computer Graphics. IEEE Transactions on*, 11(5), 596–607.
- Zheng, D., Liu, Y., Zhao, J. & el Saddik, A. (2007). A Survey of RST Invariant Image Watermarking Algorithms. *ACM Computing Surveys*, 39(2), Article 5.

Chapter 2

Data Secrecy: An FFT Approach

Tamer Rabie
UAE University, UAE

ABSTRACT

This chapter describes a framework for image hiding that exploits spectral properties of the Fourier magnitude and phase of natural images. The theory is that as long as the Fourier phase of an image is maintained intact, the overall appearance of an image remains specious if the Fourier magnitude of the image is slightly modified. This hypothesis leads to a data hiding technique that promises high fidelity, capacity, security, and robustness to tampering. Experimental results are presented throughout the chapter that demonstrate the effectiveness of this approach.

INTRODUCTION

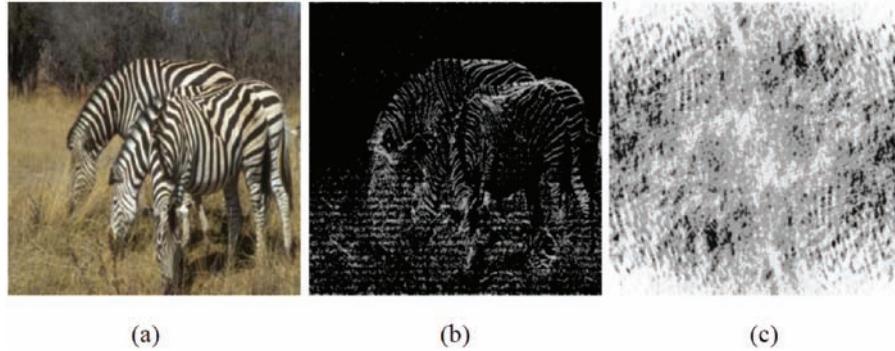
The proliferation and exchange of multimedia data over the internet and wireless networks has brought with it new prospects for covert communication. Data hiding techniques, commonly known as steganography, when dealing with hiding secret messages in a cover media (Rabie, 2007; Provos and Honeyman, 2003), or watermarking when copyright protection of multimedia data is involved (Wu and Liu, 2003), have received a great deal of attention in recent years (Chan and Cheng, 2004; Solanki

et al., 2004; Jain et al., 2002; Marvel et al., 1999; Nozaki et al., 1998).

Techniques for data hiding inside digital images have been generally confined to one popular approach, namely the manipulation of the Least Significant Bit (LSB) of an image pixel value and the rearrangement of image colours to create LSB or parity bit patterns, which correspond to the message being hidden (Curran and Bailey, 2003), with variants that try to improve three different aspects; capacity, security, and robustness (Chen and Wornell, 2001). Capacity refers to the amount of information that can be hidden in the cover medium, security refers to an eavesdropper's inability to detect hidden information, and robustness refers

DOI: 10.4018/978-1-61520-903-3.ch002

Figure 1. (a) Zebras image, (b) Inverse Fourier transform of $\exp(j.\theta(u,v))$ (the phase-only image of the Red-channel of the Zebras image). (c) Inverse Fourier transform of $|F(u,v)|$ (the magnitude-only image of the Red-channel of the Zebras image)



to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

This chapter presents a framework for data hiding which exploits spectral properties of the Fourier magnitude and phase of natural images which has allowed for a fresh new approach to image hiding in the frequency domain.

Background

The importance of Fourier magnitude and phase of the carrier image, as related to the problem of data hiding and watermarking, has been rarely discussed in the literature (Tan, 2002; Honsinger, 2000; Ramkumar et al., 1999; O’Ruanaidh et al., 1996). In the early work of Ramkumar et al. (1999) they introduce the notion of data hiding in images in which only the magnitude of the discrete Fourier transform (DFT) coefficients are altered to embed the hidden information bits. While this technique proposes a similar idea to our approach, it differs completely in the actual methodology. In Honsinger (2000), a method of data embedding based on the convolution of the hidden message data with a random phase carrier is presented with results that promise robustness to printing and scanning. The shortcomings of that technique, which bears no resemblance to

the novel approach discussed in this chapter, is the requirement of a phase carrier which must be deconvolved from the cover host image to reveal the hidden message.

SIGNIFICANCE OF MAGNITUDE AND PHASE

It is well known that for many images, the phase of the Fourier transform is more important than the magnitude (Huang et al., 1975; Oppenheim and Lim, 1981; Oppenheim et al., 1983; Ramkumar et al., 1999). Specifically if

$$F(u,v) = |F(u,v)| \cdot \exp(j.\theta(u,v)) \quad (1)$$

denotes the two-dimensional (2D) Fourier transform of an image $f(x,y)$, then the inverse Fourier transform of the phase of this 2D signal $\exp(j.\theta(u,v))$ has many recognizable features in common with the original signal, whereas the inverse Fourier transform of the magnitude $|F(u,v)|$ generally bears no resemblance to the original. This is illustrated in Figure 1 where Figure 1-(a) is an RGB color image and Figure 1-(b) is the phase-only image, i.e., the inverse Fourier transform of $\exp(j.\theta(u,v))$.

Clearly, the phase-only image retains many of the features of the original. By contrast, the magnitude-only image, i.e., the inverse Fourier transform of $|F(u,v)|$, shown in Figure 1-(c), bears no resemblance to the original image. As is evident in this example, the phase-only image often has the general appearance of a high-pass filtered version of the original with additive broadband noise.

The importance of phase also extends to one-dimensional signals. It has been shown that the intelligibility of a speech sentence is retained if the inverse transform of the Fourier phase of a long segment of the speech signal is combined with unity magnitude to obtain the phase-only equivalent speech (Oppenheim and Lim, 1981). In fact, in listening to this processed sentence, total intelligibility is retained although the speech has the general quality associated with high-pass filtering and the introduction of additive white noise. The magnitude-only speech has some structure which provides a speech like characteristic but with no speech intelligibility.

Fourier Magnitude Information Hiding

The discussion in the previous section suggests that, as long as the Fourier phase of an image is maintained intact, the overall appearance of an image remains specious if the Fourier magnitude of the image is slightly modified. This hypothesis leads to a data hiding technique that promises high fidelity, capacity, security, and robustness of hidden message embedding and extraction which allows a virtually unsuspicious stego image to be transmitted unnoticed. The word stego will be used throughout the chapter to describe the carrier image after having the hidden message embedded inside it.

The extent to which the Fourier magnitude of the carrier image can be overloaded (with the hidden message embedding) depends on the amount of degradation that one is willing to allow to the stego image. Experimental results show that a

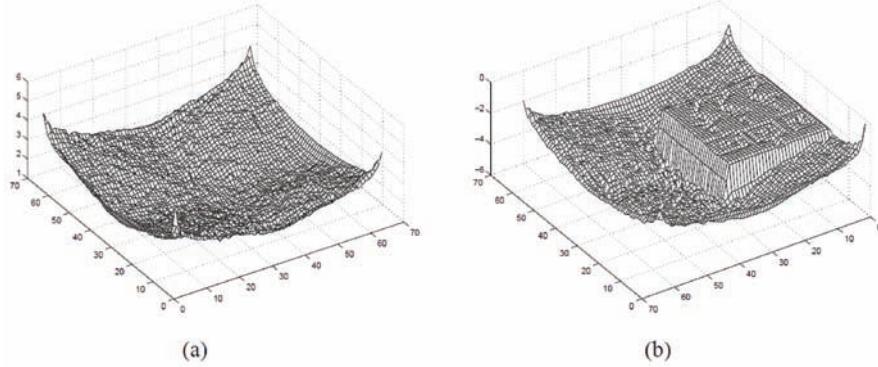
typical hidden message image may be as large as half the size of the carrier image for an unnoticeable amount of noise artifacts in the stego image.

Our choice of a carrier image is influenced by the most common image type exchanged over the internet, namely the Joint Photographic Experts Group (JPEG) image format. We thus start with a 24-bit Red, Green, Blue (RGB) color JPEG image as the carrier. One of the major concerns with typical data hiding techniques that use RGB color carrier images is the visible artifacts that may occur in the stego image due to embedding data directly in the individual (R,G,B) channels (which alter the carrier's LSB of color values in common data hiding techniques). To overcome this potential problem, which compromises the security and raise suspicion of hidden data in the image, we adopt a color/brightness (also known as chrominance/luminance) separation strategy.

There are several advantages to the separation of color from brightness information in image processing. Perceptual experimental evidence has established that the human visual system has a much higher sensitivity to changes in brightness than to color. Moreover, there seems to be general agreement that spatial resolution is markedly lower in chromatic (chrominance) channels than in the achromatic (luminance) one, hence high frequency information, i.e. fine details and edges, come mainly from the luminance channel (Watson, 1990; Forssen et al., 2002). Thus, in developing our data hiding framework we avoid altering the luminance information in the carrier image altogether. This is a stark shift from mainstream data hiding techniques used today.

We choose to separate the color carrier image using the CIE $L^*a^*b^*$ color space (Schanda, 2007; Margulis, 2006). $L^*a^*b^*$ space is a nonlinear transformation of RGB space that specifies color in terms of human perception in a way that is independent of the characteristics of any particular imaging device. The $L^*a^*b^*$ color space separates the RGB image into a luminance channel (L), and two chrominance channels (a , b). In general the

Figure 2. (a) A typical chrominance-a magnitude spectrum of the original carrier image before embedding occurs and (b) the embedded hidden image message in the high frequency region of this magnitude spectrum



luminance channel suffers less noise artifacts than the chrominance channels (Rabie, 2004). Detailed information about the CIE color spaces can be found on their website at <http://www.cie.co.at>.

These luminance/chrominance properties discussed above prompt us to embed the hidden message inside the Fourier magnitude of one of the chrominance channels (for example the chrominance-*a* channel) while preserving the luminance channel unaltered for optimal visual quality. This has an added advantage of reduced noise artifacts in the stego image with zero degradation in the original intensity brightness values. The 2D Fourier transform of the chrominance-*a* channel is first computed and the magnitude spectrum is separated from the phase spectrum. Let $Ca(u,v)$ be the Fourier transform of the chrominance-*a* channel of the carrier image which can be expressed in polar form as:

$$Ca(u,v) = Ma(u,v) \cdot \exp(j \cdot \theta a(u,v)) \quad (2)$$

The technique used to embed a hidden message image into the Fourier magnitude of the chrominance-*a* channel of the carrier image is to replace the high-frequency areas in the Fourier magnitude spectrum with the values of the hidden message's image. This type of embedding prevents aliasing of the hidden message when extracted

(which appears as a mirroring of parts of the hidden image from one side onto the opposite side and causes data loss). Figure 2 shows the ‘before’ and ‘after’ figures of the chrominance-*a* magnitude spectrum of a typical carrier image (Figure 2-(a)) when a hidden message image is embedded in the high frequency areas of this magnitude spectrum to produce a modified chrominance-*a* magnitude spectrum (Figure 2-(b)).

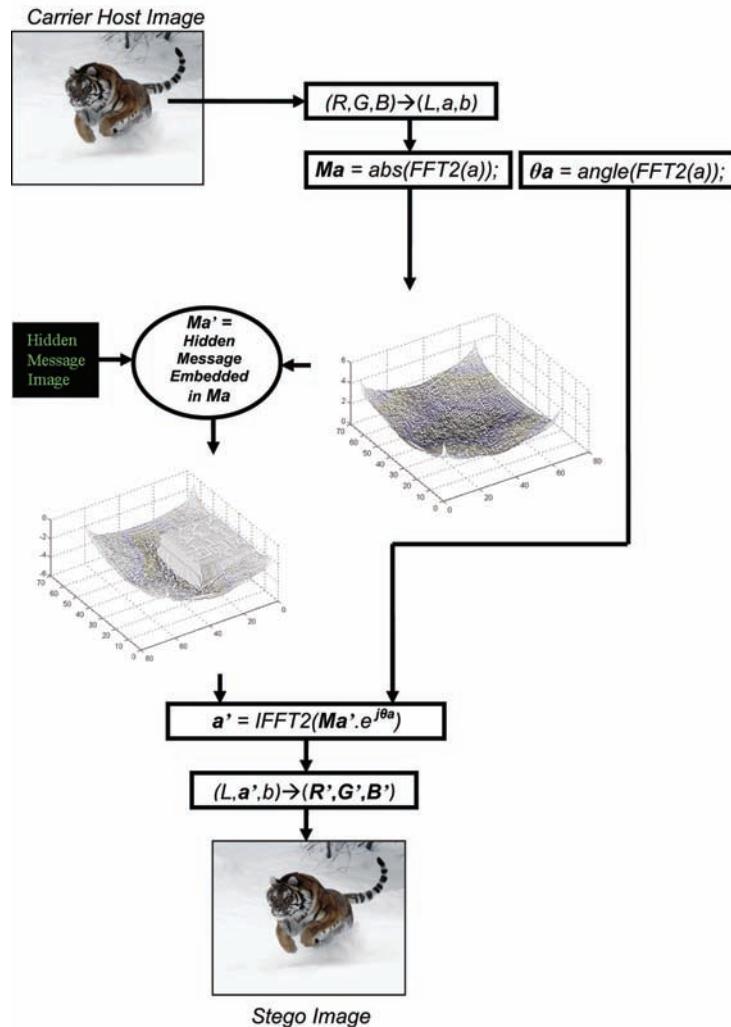
This modified chrominance-*a* Fourier magnitude $Ma'(u,v)$ is then combined with the complex Fourier phase of the original chrominance-*a* channel to produce the Fourier stego spectrum of the chrominance-*a* channel as shown in equation (3), which when transformed back to the spatial domain gives us a modified chrominance-*a* channel (a'). Combining this with the *L* and *b* channels (L, a', b) and transforming back to the (*R, G, B*) color space, will produce the space-domain stego image which contains the hidden information. This is clearly depicted in the diagram of Figure 3.

$$Ca'(u,v) = Ma'(u,v) \cdot \exp(j \cdot \theta a(u,v)) \quad (3)$$

Recovery of Hidden Information

Extraction of the hidden message image takes place in reverse order to the hiding process. Referring

Figure 3. Block diagram showing the general steganography algorithm used to hide a message image inside the Fourier magnitude spectrum of the chrominance- a channel of the carrier image after separating luminance from color information to preserving the luminance channel unaltered for optimal visual quality of the generated stego image



to Figure 3 (bottom-up), first the (R,G,B) stego image is converted to the L*a*b* color space and the chrominance- a channel is separated from the other channels. The 2D Fourier transform of this extracted chrominance- a channel is then computed and the magnitude spectrum is separated from the phase spectrum. It is this magnitude spectrum that contains the hidden secret image. This hidden image is extracted from the high-frequency

areas in the Fourier chrominance- a magnitude spectrum, making sure that the for-loop that is used to extract the hidden image is the same for-loop that was used to embed this hidden image. This embedding-extraction loop can be considered as a security key for recovering the hidden data. Without knowing the correct embedding loop, it becomes a guessing game for successfully recovering the hidden information.

To accurately compare our FFT-based data hiding techniques described in this chapter with the most common methods used for data hiding it becomes necessary to assess the data loss issues (fidelity of stego and recovered data) that are inherent in steganography algorithms. Steganographic systems that modify least-significant bits of the carrier image are often susceptible to visual attacks (Westfeld and Pfitzmann, 1999). Visual attacks mean that one can see steganographic messages on the low bit planes of an image because they overwrite visual structures, which exists to some degree in all the image's bit layers; this usually happens in BMP and GIF images. This is not true for our Fourier magnitude steganography method. The data hiding takes place in the frequency domain, and only the magnitude spectrum of the chrominance-*a* channel of the carrier image is modified, leaving the luminance channel as well as the other chrominance-*b* channel unaltered.

Suspicious visual pattern artifacts may occur when data hiding takes place in the FFT magnitude of the luminance channel instead of the other two chrominance channels (Figure 4-top). For our FFT-based technique, the implication of embedding a hidden image in the high frequency areas of the Fourier magnitude of the chrominance-*a* channel is an additive noise component in the spatial domain of the chrominance-*a* channel which appears as minor color artifacts in the stego image. The amplitude of the noise that appears in the stego image is proportionate to the variance of the hidden message image. The smaller the changes in the hidden image, the lower the noise that affects the colors of the stego image, and vice versa.

Figure 4 shows a comparison between embedding a kitten gray scale image in the high-frequency areas of the Fourier magnitude of the luminance channel (luminance stego shown in the top image set) and the same hidden kitten image embedded in the Fourier magnitude of the chrominance-*a* channel (chrominance-*a* stego image shown in the middle image set). Looking at both the luminance

and chrominance-*a* stego images it is clear that embedding the kitten gray scale image in the Fourier magnitude of the chrominance-*a* channel produces significantly less artifacts in the resulting stego image. Also when extracting the hidden kitten image from the chrominance-*a* stego image (bottom right image) has less noticeable artifacts in it than the extracted kitten image from the luminance stego image (bottom left image). Only when magnifying the chrominance-*a* stego image that one starts to see very unnoticeable color artifacts that do not affect the image and are unsuspicious, while it is clear from the magnified luminance stego image that it exhibits severe pattern noise artifacts that are much more suspicious.

Figure 5 shows the results of embedding a hidden text black and white image, shown in Figure 5-(b), into the 24-bit color carrier image of Figure 5-(a). The resulting color stego image shown in Figure 5-(c) has no suspicious degradation which is visually confirmed from the high fidelity of the color stego image. Figure 5-(d) shows the extracted hidden image from the color stego of Figure 5-(c). It is clear that the extracted hidden message is clearly legible and suffers minor degradations.

SECURITY LEVELS

The data hiding process presented in this chapter is based on manipulating spectral magnitude multiplied by spectral phase of color images (see equations (1) and (2)), which is equivalent to manipulating the convolution of the spatial-domain magnitude image with the spatial-domain phase image (such as those in Figure 1(b) and (c)). This has the effect of scattering the hidden image three times across all pixels of the carrier image; once when the embedded hidden image is transformed together with its magnitude spectrum host from the frequency domain to the space domain, and secondly, when this magnitude image is convolved with the phase image to produce the

Figure 4. (Top) Luminance stego image showing severe pattern artifacts, and (Middle) Chrominance_a stego image showing unnoticeable color artifacts, (Bottom Left) extracted kitten image from Luminance stego, (Bottom Right) extracted kitten image from Chrominance_a stego image



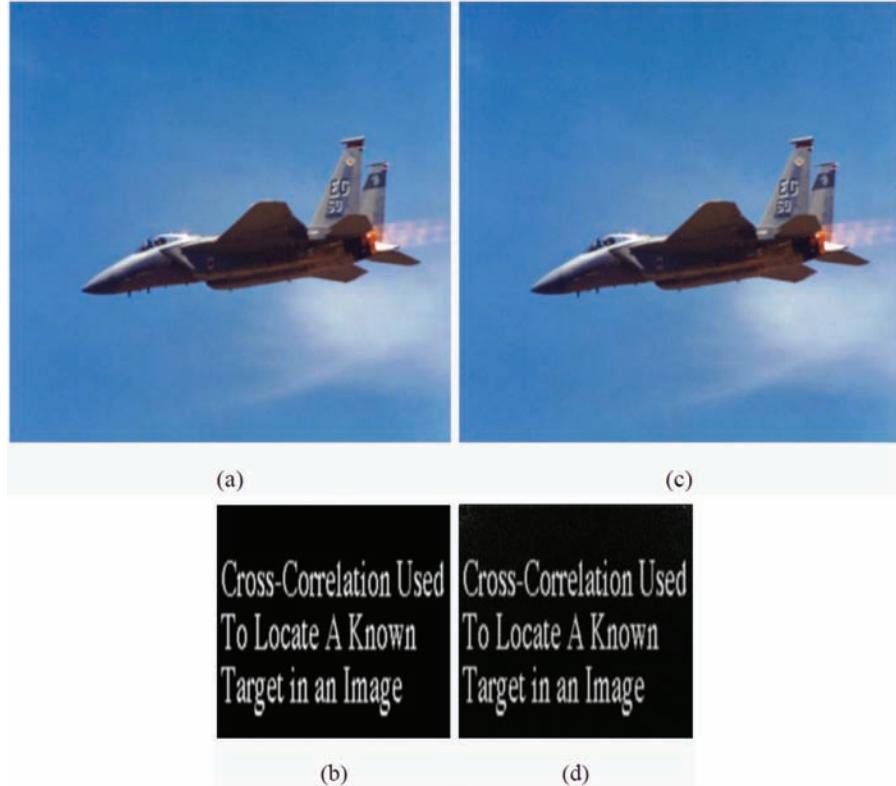
stego chrominance- a channel image, and finally when the colour stego (L,a,b)-based image is transformed to the (R,G,B) color space, effectively distributing the hidden image information in the chrominance- a channel to all (R,G,B) channels, further enhancing the security of the final stego image. This FFT-based steganography method, thus, provides a three-layer security measure that

can be exploited in secure data transmission over insecure networks.

Robustness to Stego Medium Tampering

To demonstrate the robustness of this image hiding technique to tampering degradations in the

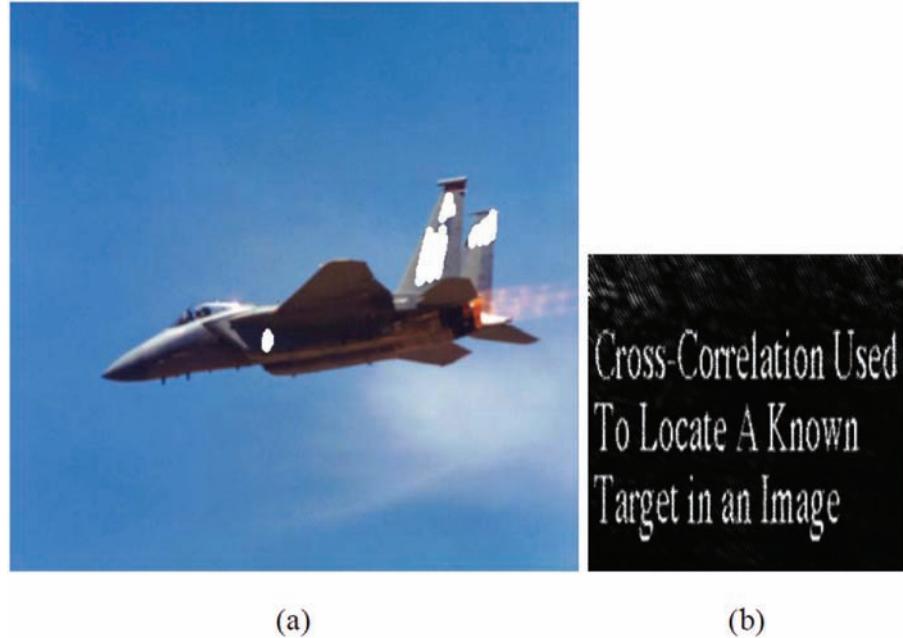
Figure 5. (a) Original color carrier image of size 512x512, (b) Original hidden text message of size 256x256, (c) Color stego image with hidden text message of (b) embedded inside its magnitude of Chrominance_a spectrum, (d) Extracted hidden message image from the stego image of (c)



stego image, we simulate different tampering effects and attempt to extract the hidden image from the tamper-degraded stego image. We start by demonstrating partial information removal tampering on the stego image of Figure 5-(c) in the form of masking out the letters on the aircraft's body and tail using a whiteout marker as shown in Figure 6-(a). The extracted hidden message image shown in Figure 6-(b) is very legible, with some minor degradations at the top of the image, corresponding to the location closest to the band-limit frequency regions of the Fourier magnitude, where the masking replaces some of these frequencies with high amplitude frequencies which appear as bright artifacts in the upper half of the extracted hidden message image.

In the remainder of this section, we present a series of tampering applied to a red rose flower stego image which was embedded with a handwritten message image. The left column of Figure 7 shows a series of Flower stego images with increasing areas of the images being removed. The right column of the figure shows the corresponding extracted hidden handwritten message images. It is clear that up to a 60% loss in the data of the stego image we will still be able to extract a relatively legible hidden message image, while at 98% data loss, the ghost of the image is still there but obviously unreadable. In these cases, a qualitative evaluation of the extracted hidden message image is more important than quantitative numbers, and clearly this image

Figure 6. (a) Tampered Color stego image, (b) Extracted hidden message image from tampered stego image showing acceptable legibility



hiding technique works for severe cases of data loss in the stego image.

Finally, in Figure 8, we show two more tampering examples on the Flower stego image and the resulting extracted hidden message image. Figures 8-(a) and (b) show the Flower stego image with repaint tampering, and the corresponding extracted hidden message images. It is clear that even though with the increase in repaint tampering in the stego images, a corresponding increase in degradation occurs in the extracted hidden message images, the extracted handwritten message images are still legible to a high degree.

Figure 8-(c) shows a tampered Flower stego image where the central area of the Flower is rotated by 90 degrees, and the corresponding extracted hidden message image. Figure 8-(d) shows an extreme case of rotation tampering where 80% of the Flower stego image is flipped vertical. The corresponding extracted hidden message image shown has been flipped horizontally after extrac-

tion from the tampered stego image to remove the mirror effect in the handwritten text due to the vertical flip of the stego image. In all these cases the extracted handwriting is still readable which demonstrates the robustness of our technique to these different types of tampering.

To understand how this image hiding technique is robust to these types of severe tamperings, we must recall that the hidden message image is not simply embedded in the individual pixels of the space-domain carrier image, but rather, in the frequency spectrum of the magnitude of the chrominance-*a* channel of the carrier image, and, as explained earlier, this is equivalent to scattering the hidden message image data over all the carrier image pixels. This explains why when 60% of the stego image data are lost or removed we can still retrieve the hidden message, albeit with some degradations. In other words, as long as 40% or more of the stego image data remains

Figure 7. A series of Flower stego images with increasing data loss tampering and their corresponding extracted hidden message images

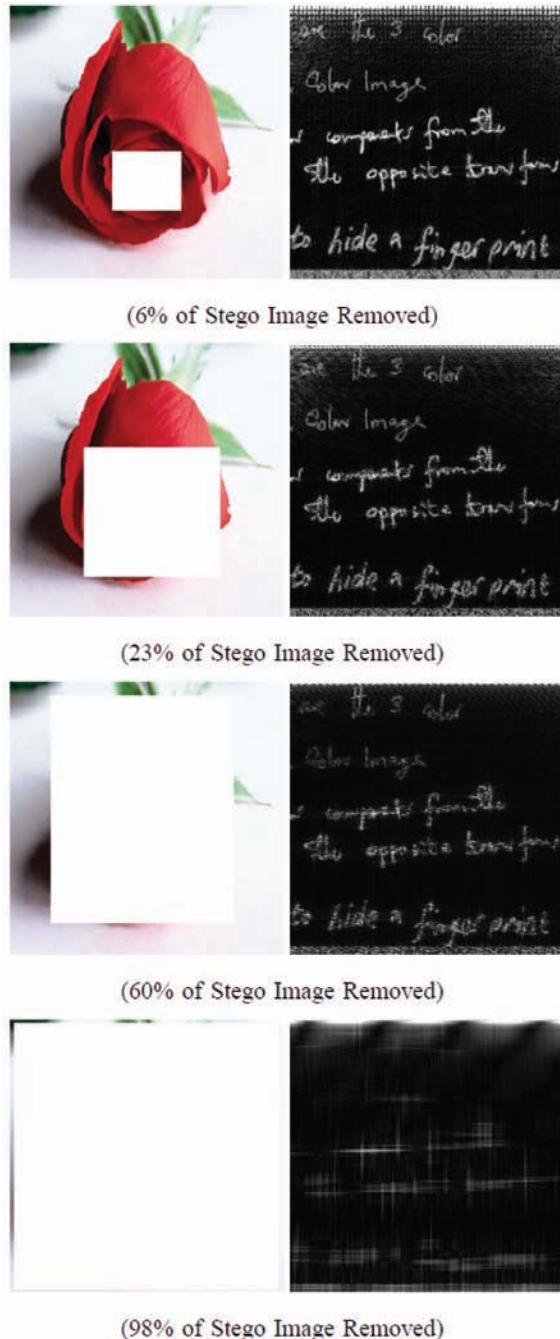
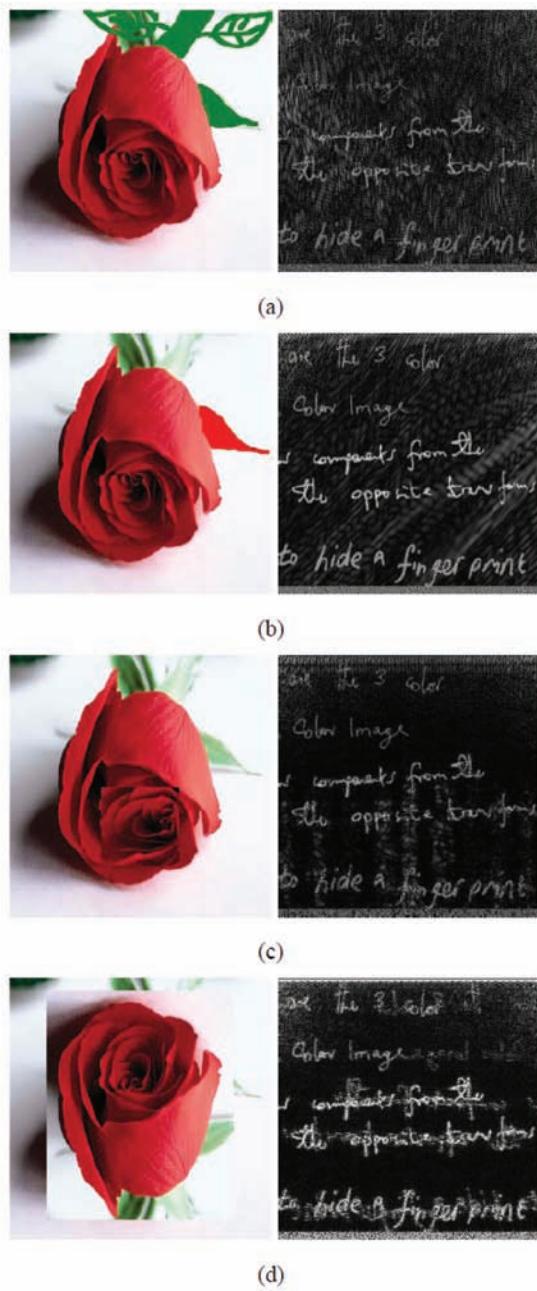


Figure 8. The Flower stego image with repainting and rotation tampering, and their corresponding extracted hidden message images



intact, we can extract the hidden message image with reasonable integrity.

FUTURE RESEARCH DIRECTIONS

The FFT-based steganography framework described in this chapter has been successfully used in speech steganography for secure sound message sharing and transmission. This speech steganography system, which was first proposed in Rabie and Guerchi (2007), and further developed (Guerchi et al., 2008; Guerchi and Rabie, 2007), exploits the advancements in speech processing to hide efficiently secret speech in narrowband cover speech. Linear predictive coding (LPC) is used to represent the secret speech with reduced number of parameters. These parameters are embedded in selective perceptually-irrelevant frequency locations in the FFT magnitude of a cover speech signal. Objective and subjective measures have shown that the resulting stego speech, which contains the secret sound message, is indistinguishable from the cover speech.

The same framework has also been exploited for the problem of super-resolution color image compression. This novel paradigm, which was introduced in Rabie (2006), combines space-domain and frequency-domain color image processing operations. In the space domain, image color-brightness separation is exploited, and in the frequency domain, spectral properties of the Fourier magnitude and phase of the digitally-acquired image are exploited. Working in both domains concurrently addresses both issues of quality and reduced storage size. Experimental results as well as empirical observations have shown that this technique is very competitive with the widely used JPEG image compression standard with the added advantage of being able to recover the original quality without any degradation common in lossy compression techniques.

This paradigm has potential for many more applications related to multimedia data hiding.

For example, techniques described in this chapter may be used in hiding fingerprint scans inside a person's own photograph for security checks. For hospital database management, this technique may be useful in reducing the storage and retrieval overhead of patient information by embedding important medical information in a patient's own magnetic resonance image or an X-ray image hidden inside a photograph of the injured part. Other applications may include hiding a simple speech annotation inside an image acquired by a digital camera programmed to use this data hiding technique, to name a few. Finally, one potentially attractive application of this technique is to hide the full sound track of a movie inside the individual frames of the movie with negligible degradation to the movie and the extracted hidden sound track. The sound segment to be embedded into the current frame would have to be resampled to reshape it into an $N \times N$ matrix which would then be hidden inside the Fourier magnitude of the current image frame of size $2N \times 2N$. The main benefit of this application is reduced sized movies since the sound track will be totally hidden inside the movie frames, thus eliminating the memory overhead taken up by the sound track.

CONCLUSION

This chapter laid out a framework for FFT-based data hiding that makes use of the Fourier magnitude of the carrier image to maintain the color composition of the stego image while allowing a relatively large sized hidden message image (to a maximum of half the size of the carrier image) to be robustly embedded and extracted with minor degradation. The advantages of this technique have been expressed throughout the chapter and can be summarized in that this paradigm leads to a data hiding technique that provides high fidelity, capacity, security, and robustness of hidden message embedding and extraction which allows

a virtually unsuspicious stego image to be transmitted unnoticed.

REFERENCES

- Castleman, K. (1996). *Digital Image Processing*. Upper Saddle River, NJ: Prentice-Hall.
- Chan, C. K., & Cheng, L. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, 37, 469–474. doi:10.1016/j.patcog.2003.08.007
- Chen, B., & Wornell, G. (2001). Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, 47(4), 1423–1443. doi:10.1109/18.923725
- Curran, K., & Bailey, K. (2003). An evaluation of image based steganography methods. *International Journal of Digital Evidence*, 2(2), 1–40.
- Forssen, P.-E., Granlund, G., & Wiklund, J. (2002). *Channel representation of colour images*. (Tech. Rep. LiTH-ISYR-2418), Computer Vision Laboratory, Department of Electrical Engineering [Linkoping, Sweden.]. Linkoping University, SE-581, 83.
- Guerchi, D., Harmain, H., Rabie, T., & Mohamed, E. (2008). Speech Secrecy: An FFT-based Approach. *International Journal of Mathematics and Computer Science*, 3(2), 1–19.
- Guerchi, D., & Rabie, T. (2007). Narrowband CELP Hiding by Wideband Speech. *The Ninth IASTED International Conference on Signal and Image Processing (SIP 2007)*, Honolulu, Hawaii, USA.
- Honsinger, C. (2000). *Data embedding using phase dispersion*. IEE Seminar on Secure Images and Image Authentication (Ref. No. 2000/039), (pp. 5/1–5/7). Rochester, NY: Eastman Kodak Co.
- Huang, T., Burnett, J., & Deczky, A. (1975). The importance of phase in image processing filters. *IEEE Trans. on ASSP*, 23(6), 529–542. doi:10.1109/TASSP.1975.1162738
- Jain, A., Uludag, U., & Hsu, R. (2002). Hiding a face in a fingerprint image. In *Proc. International Conference on Pattern Recognition (ICPR)*, Quebec City, Canada.
- Margulis, D. (2006). *Photoshop Lab Color: The Canyon Conundrum and Other Adventures in the Most Powerful Colorspace*. Berkeley, CA: Pearson Education.
- Marvel, L. M., Charles, G., Boncelet, J., & Retter, C. T. (1999). Spread spectrum image steganography. *IEEE Transactions on Image Processing*, 8(8), 1075–1083. doi:10.1109/83.777088
- Nozaki, K., Niimi, M., Eason, R. O., & Kawaguchi, E. (1998). A large capacity steganography using colour bmp images. In *ACCV '98: Proceedings of the Third Asian Conference on Computer Vision*, (Vol. I, pp.112–119). London: Springer-Verlag.
- O’Ruanaidh, J., Dowling, W., & Boland, F. (1996, September 16–19). Phase watermarking of digital images. In *Proc. IEEE International Conference on Image Processing (ICIP)*, Lausanne, Switzerland, (Vol. 3, pp. 239–242).
- Oppenheim, A., & Lim, J. (1981). The importance of phase in signals. *Proceedings of the IEEE*, 69(5), 529–541. doi:10.1109/PROC.1981.12022
- Oppenheim, A., Lim, J., & Curtis, S. (1983). Signal synthesis and reconstruction from partial Fourier-domain information. *Journal of the Optical Society of America*, 73(11), 1413–1420. doi:10.1364/JOSA.73.001413
- Provost, N., & Honeyman, P. (2003). Hide and seek: an introduction to steganography. *IEEE Security and Privacy Magazine*, IEEE. Computers & Society, 32–44.

- Rabie, T. (2004). Adaptive hybrid mean and median filtering of high-ISO long-exposure sensor noise for digital photography. *SPIE Journal of Electronic Imaging*, 13(2), 264–277. doi:10.1117/1.1668279
- Rabie, T. (2006, November 19-21). A Novel Compression Technique for Super Resolution Color Photography. In *Proceedings of the IEEE International Conference on Innovations in Information Technology (IIT2006)*, (pp. 1-5), Jumeirah Beach Hotel, Dubai, UAE.
- Rabie, T. (2007). Frequency-domain data hiding based on the Matryoshka principle. *Int. J. Advanced Media and Communication*, 1(3), 298–312. doi:10.1504/IJAMC.2007.013952
- Rabie, T., & Guerchi, D. (2007, November 24-27). Magnitude Spectrum Speech Hiding. In *IEEE International Conference on Signal Processing and Communication (ICSPC07)*, Dubai, UAE.
- Ramkumar, M., Akansu, A., & Alatan, A. (1999). A robust data hiding scheme for images using DFT. In *Proc. IEEE International Conference on Image Processing (ICIP)*, (pp.1–5).
- Schanda, J. (2007). *Colorimetry*(p. 61). New York: Wiley-Interscience. doi:10.1002/9780470175637
- Solanki, K., Jacobsen, N., Madhow, U., Manjunath, B. S., & Chandrasekaran, S. (2004). Robust image-adaptive data hiding using erasure and error correction. *IEEE Transactions on Image Processing*, 13(12), 1627–1639. doi:10.1109/TIP.2004.837557
- Tan, C. (2002). *Image Camou-Flaging using Phase Randomization*. Retrieved from <http://pachome2.paci.c.net.sg/chewkeong/ImgCamou.pdf>
- Watson, A. (1990). Perceptual-components architecture for digital video. *Journal of the Optical Society of America. A, Optics and Image Science*, 7(10), 1943–1954. doi:10.1364/JOSAA.7.001943
- Westfeld, A., & Pfitzmann, A. (1999). Attacks on steganographic systems. In *Proc. 3rd Int'l Workshop on Information Hiding*, (pp.61–76). London: Springer Verlag.
- Wu, M., & Liu, B. (2003). Data hiding in image and video: part I – fundamental issues and solutions. *IEEE Transactions on Image Processing*, 12(6), 685–695. doi:10.1109/TIP.2003.810588

ADDITIONAL READING

- Anderson, R.J. and Petitcolas, F.A.P. (1998) ‘On the limits of steganography’, *Selected Areas in Communications, IEEE Journal on*, Volume: 16, Issue: 4, Pages: 474 - 481
- Artz, D. (2001). Digital steganography: hiding data within data. *Internet Computing, IEEE*, Volume, 5(Issue: 3), 75–80. doi:10.1109/4236.935180
- Cachin, C. (2004). An information-theoretic model for steganography. *Information and Computation*, 192(Issue 1), 41–56. doi:10.1016/j.ic.2004.02.003
- Chang, C., Chen, G., & Lin, M. (2004). Information hiding based on search-order coding for VQ indices. *Pattern Recognition Letters*, 25(Issue 11), 1253–1261. doi:10.1016/j.patrec.2004.04.003
- Chang, C., & Tseng, H. (2004). A steganographic method for digital images using side match. *Pattern Recognition Letters*, 25(Issue 12), 1431–1437. doi:10.1016/j.patrec.2004.05.006
- Furuta, T., Noda, H., Niimi, M., & Kawaguchi, E. (2003) ‘Bit-plane decomposition steganography using wavelet compressed video’, *Information, Communications and Signal Processing, 2003 and the Fourth Pacific Rim Conference on Multimedia. Proceedings of the 2003 Joint Conference of the Fourth International Conference on*, Volume: 2, Pages:970 - 974 vol.2

- Hairong Qi. Snyder, W.E.; and Sander, W.A.; (2002) 'Blind consistency-based steganography for information hiding in digital media', *Multimedia and Expo, 2002. ICME '02. Proceedings. 2002 IEEE International Conference on*, Volume: 1, Pages:585 - 588 vol.1
- Jamil, T. (1999). Steganography: the art of hiding information in plain sight. *Potentials, IEEE, Volume, 18*(Issue: 1), 10–12. doi:10.1109/45.747237
- Lin, C., & Tsai, W. (2004). Secret image sharing with steganography and authentication. *Journal of Systems and Software, 73*(Issue 3), 405–414. doi:10.1016/S0164-1212(03)00239-5
- Manikopoulos, C. Yun-Qing Shi; Sui Song; Zheng Zhang; Zhicheng Ni; and Dekun Zou; (2002) 'Detection of block DCT-based steganography in gray-scale images', *Multimedia Signal Processing, 2002 IEEE Workshop on*, Pages:355 - 358
- McBride, B., Peterson, G., & Gustafson, S. (2005). (in press). A new blind method for detecting novel steganography [Corrected Proof, Available online]. *Digital Investigation*. doi:10.1016/j.diin.2005.01.003
- Moulin, P.; and O'Sullivan, J.A.; (2003) 'Information-theoretic analysis of information hiding', *Information Theory, IEEE Transactions on*, Volume: 49, Issue: 3, Pages:563 - 593
- Munirajan, V., Cole, E., & Ring, S. (2004) 'Transform Domain Steganography Detection Using Fuzzy Inference Systems', *Multimedia Software Engineering, 2004. Proceedings. IEEE Sixth International Symposium on*, Pages:286 - 291
- Niimi, M., Noda, H., Kawaguchi, E., & Eason, R. O. (2002) 'High capacity and secure digital steganography to palette-based images', *Image Processing. 2002. Proceedings. 2002 International Conference on*, Volume: 2, Pages:II-917 - II-920 vol.2
- Noda, H., Spaulding, J., Shirazi, M. N., & Kawaguchi, E. (2002). Application of bit-plane decomposition steganography to JPEG2000 encoded images. *Signal Processing Letters, IEEE, Volume, 9*(Issue: 12), 410–413. doi:10.1109/LSP.2002.806056
- Noda, H., Spaulding, J., Shirazi, M. N., Niimi, M., & Kawaguchi, E. (2002) 'Application of bit-plane decomposition steganography to wavelet encoded images', *Image Processing. 2002. Proceedings. 2002 International Conference on*, Volume: 2, Pages:II-909 - II-912 vol.2
- Pages:510 - 516
- Rising, L. S., & Calliss, F. W. (1993) 'An experiment investigating the effect of information hiding on maintainability', *Computers and Communications, 1993., Twelfth Annual International Phoenix Conference on*, 23-26 March 1993
- Srinivasan, Y., Nutter, B., Mitra, S., Phillips, B., & Ferris, D. (2004) 'Secure transmission of medical records using high capacity steganography', *Computer-Based Medical Systems, 2004. CBMS 2004. Proceedings. 17th IEEE Symposium on*, Pages:122 - 127
- Tsai, P., Hu, Y., & Chang, C. (2004). A progressive secret reveal system based on SPIHT image transmission. *Signal Processing Image Communication, 19*(Issue 3), 285–297. doi:10.1016/j.image.2003.10.005
- Vasiltsov, I. V., Karpinskyy, M. P., & Sagan, A. M. (2003) 'Development of VHDL-based core with embedded steganography function', *CAD Systems in Microelectronics, 2003. CADSM 2003. Proceedings of the 7th International Conference. The Experience of Designing and Application of*, Pages:260 - 261
- Wang, S. (2004). (in press). Steganography of capacity required using modulo operator for embedding secret image [Corrected Proof, Available online]. *Applied Mathematics and Computation*.

Wu, M., Ho, Y., & Lee, J. (2004). An iterative method of palette-based image steganography. *Pattern Recognition Letters*, 25(Issue 3), 301–309. doi:10.1016/j.patrec.2003.10.013

Wu, Z., Yang, W., & Yang, Y. (2003). ABS-based speech information hiding approach. *Electronics Letters*, Volume, 39(Issue: 22), 1617–1619. doi:10.1049/el:20030993

Xu, J., Sung, A. H., Shi, P., & Liu, Q. (2004) ‘JPEG compression immune steganography using wavelet transform’, *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, Volume: 2, Pages: 704 - 708 Vol.2

Xu, J., Sung, A. H., Shi, P., & Liu, Q. (2004) ‘JPEG compression immune steganography using wavelet transform’, *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, Volume: 2, Pages: 704 - 708 Vol.2

Yu, Y., Chang, C., & Hu, Y. (2005). Hiding secret data in images via predictive coding. *Pattern Recognition*, 38(Issue 5), 691–705. doi:10.1016/j.patcog.2004.11.006

Zhi-jun, W., Xin-Xin, N., & Yi-xian, Y. (2002) ‘Design of speech information hiding telephone’, *TENCON ‘02. Proceedings. 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering*, Volume: 1, Pages:113 - 116 vol.1

KEY TERMS AND DEFINITIONS

Stego: Is the terminology used in the steganography community to describe the carrier image after having the hidden message embedded inside it.

Visual attacks: Mean that you can see steganographic messages on the low bit planes of an image because they overwrite visual structures, which exists to some degree in all the image’s bit layers this usually happens in BMP and GIF images.

FFT: Fast Fourier Transform, used to transform a space domain signal to the frequency domain.

Steganography: Is the art and science of hiding communication; a steganographic system embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper’s suspicion.

Capacity: Refers to the amount of information that can be hidden in the cover medium.

Security: Refers to an eavesdropper’s inability to detect hidden information.

Robustness: Refers to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

Chapter 3

Color in Image Watermarking

Gaël Chareyron

École Supérieure d'Ingénieurs Léonard de Vinci, France

Jérôme Da Rugna

École Supérieure d'Ingénieurs Léonard de Vinci, France

Alain Tréneau

Laboratoire Hubert Curien, Université Jean Monnet, France

ABSTRACT

This chapter summarizes the state-of-the-art color techniques used in the emerging field of image watermarking. It is now well understood that a color approach is required when it comes to deal with security, steganography and watermarking applications of multimedia contents. Indeed, consumers and business expectations are focused on the protection of their contents, which are here color images and videos. In the past few years, several gray-level image watermarking schemes have been proposed but their application to color image is often inadequate since they usually work with the luminance or with individual color channel. Unfortunately, color cannot be considered as a simple RGB decomposition and all of its intrinsic information must be integrated in the watermarking process. Therefore, it is the chapter objective to present, first, the major difficulties associated with the treatment of color images, and second, the state-of-the-art methods used in the field of color image watermarking.

INTRODUCTION

In the last decade, we have seen a tremendous growth in color and color-based applications within the signal, image and video processing communities. Color is no longer interpreted as an extension of gray scale and is now considered as a key element for a number of image and video processing systems. In particular, color space transforms have played a

central role in coding, compression and transmission applications. Color also plays a major role in pattern recognition and digital multimedia, where color based-features and color segmentations have been proven effective in indexing and multimedia content access. Moreover, the fusion of color and edge based features has improved the performance of image retrieval applications. Furthermore, color has become more recently a major component in security, steganography, and watermarking applications of multimedia contents (Tréneau et al., 2008)

DOI: 10.4018/978-1-61520-903-3.ch003

This chapter presents the state-of-the-art watermarking techniques that are specifically designed for color images. Watermarking algorithms are generally used for content origin identification, copy protection, illegal copies tracking, finger-printing, and content access control (Elbasi & Eskicioglu, 2006; Lukac & Plataniotis, 2007). The main objective of the watermarking techniques is to embed data into a host image by introducing changes that are imperceptible to the human eye but recoverable by a computer program. The signature locations in the image are determined by a secret key that prevents possible attacks or alterations from:

- Signal processing algorithms, like compression, coding transformations, contrast enhancement, color enhancement, dithering, re-sampling.
- Geometrical transformations, such as rotation, translation, cropping, scaling.
- Watermark removal, watermark duplication or unauthorized detection.

In general, watermarking algorithms are based either on an additive process, a multiplicative or a quantization process. The watermark is extracted from the marked image either blindly or with a secret key. Most of the watermarking schemes are symmetric (i.e. the embedding and detection keys are identical). While several methods have been proposed to watermark grey level images, only a few have been designed for color images. Most of the time, these methods integrate color information and human vision system by using histogram and quantization scheme, frequency domain transform or spatial domain processing. Recently, these approaches have clearly demonstrated that, for many demanding applications (High Definition video as example), reaching an invisible and robust mark requires, at least, the integration of the color information within the watermarking process. For these reasons, this chapter is divided in two parts. The first part is

focused on the major difficulties associated with color treatment and the second part presents the state-of-the-art methods in use in the field of color image watermarking.

COLOR IN IMAGE WATERMARKING: ISSUES AND PROBLEMS

Since the traditional color Red Green Blue (RGB) triplet has been proven successful in numerous applications, it is not surprising that the color information is processed in parallel for each color component independently of each other. Reducing the color information to three components is a simple abstraction that ignores the intrinsic information contained in the color. In particular, the Human Visual System and the inter-correlation between these colors components cannot be ignored (Sharma, 2002). Since the RGB values are the only data usually available, the goal of color imaging is to produce new algorithms that take into account the color definition and the color image formation. Furthermore, the transition from scalar to vector-valued image processing is not yet addressed in the watermarking literature and therefore it becomes essential to clarify first what is behind color information and what are the concepts associated with vector-valued color image processing.

Color is represented by its red-green-blue (RGB) values, which are usually between 0 and 255. However, this RGB triplet is a biased representation of the color information. A color is correctly defined by its complete wavelength response while RGB components represent only 3 specific wavelengths (Lukac & Plataniotis, 2007). Also, a color is dependant on the viewing conditions. For example, with an acquisition system, the color will change depending on the illuminant (i.e. the lightning conditions) and the sensor type (CCD or CMOS). In a viewing system, the sensation given by a color will also depend on the illuminant, the display and subjectively,

Figure 1. Simulation of a scene under several standard illuminants: D65 Noon daylight, D75 overcast daylight, D50 Horizon light and F2 cool white fluorescent. Illuminants are defined by the CIE, International Commission on Illumination; the simulation is obtained with the help of the color software color space, <http://www.couleur.org>.



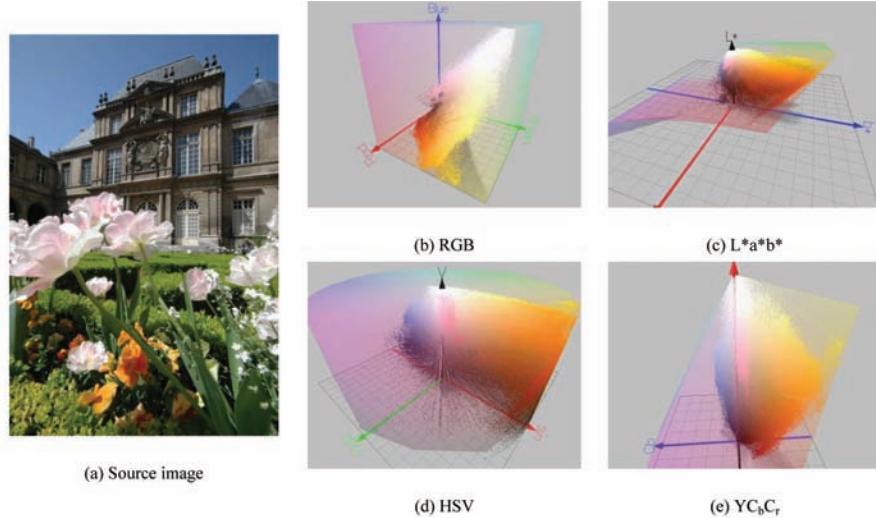
the viewer. *Figure 1* illustrates the impact of the illuminant on the acquisition system. The same scene is displayed with 4 distinct illuminants. It appears clearly that the sensations expressed by these four images are different, even if the illuminant is the only parameter modified, starting from a cold illuminant (D75) to a warm one (F2) (Schanda, 2007). The same conclusion holds with a badly calibrated monitor.

To understand precisely the concept of color information, it is worth to review the fundamental properties of the human vision system (Watson, 1993). Using its cones, it can detect light in the range of 400 nanometers (violet) to 700 nanometers (red) and can adapt to a large variation of illumination levels. The vision system perceives this range of light wavelengths as a smoothly varying rainbow of colors, which is called the visual spectrum. Also, the human visual system is nearly color constant for a large area of surfaces and lighting conditions. A yellow lemon will be perceived yellow in the early morning, at noon and in the evening. As a matter of fact, the perceived color is not the direct result of the spectral distribution of the received light but is rather an interpretation of

the received light in a particular context. Finally, the sensitivity of the human visual system is not uniform regarding color and spatial frequencies. These observations lead to the conclusion that an efficient color image processing needs an adequate color representation.

The literature is full of different color spaces which have been used to represent various color components which can be more or less independent. One of the biggest problems in color image processing is to find the appropriated colorspace for the problem being addressed. While the application context often defines the original space (such as RGB for images or Yuv for television) the insertion space has to be discussed according to the expected properties of the watermark. *Figure 2* shows the 3D representation of the RGB color space along with the representation of the three classical color spaces, HSV (Hue, Saturation, Value), YC_bC_r and $L^*a^*b^*$, used with watermarking algorithms (Lukac & Plataniotis, 2007). The RGB color space has the most correlated components while the YC_bC_r color components are the less correlated. Moreover, the forward and backward transforms between RGB and YC_bC_r color spaces

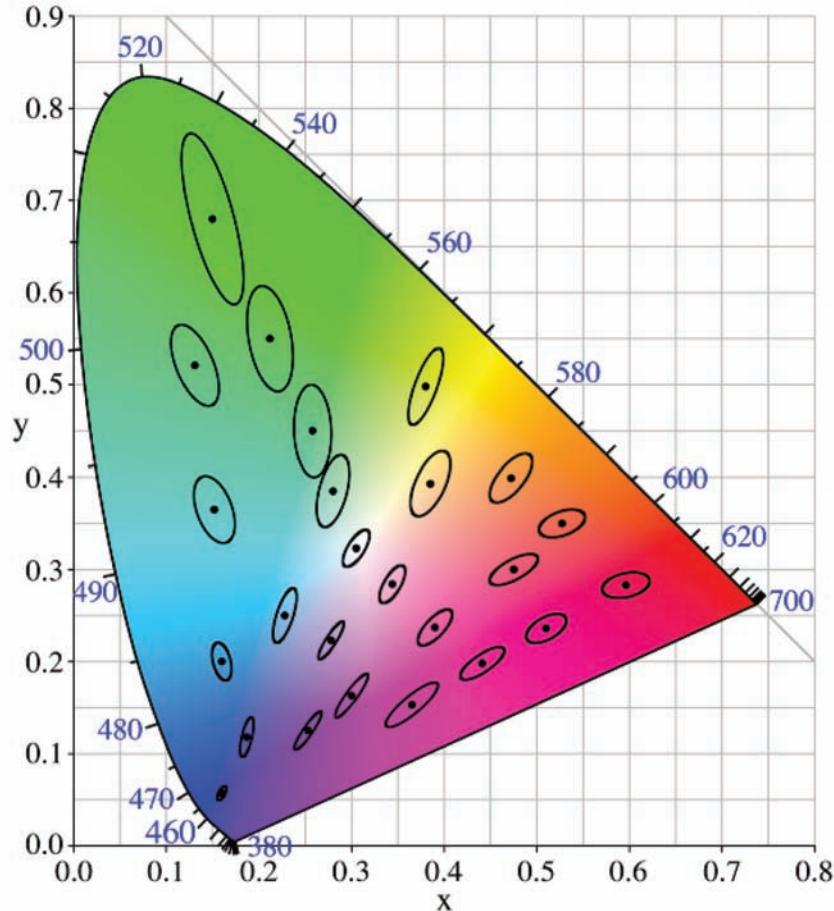
*Figure 2. Representation of a natural image with several color spaces: RGB, L*a*b*, HSV and YC_bC_r. L*a*b* is obtained using a standard D65 illuminant, which is the one found with the original photography.*



are linear. With correlated components such like RGB components, touching one component independently of the others is not necessarily the best choice since the perceived colors is dependant of the three components together. This is the reason why the RGB colorspace is called a correlated color space. On the other hand, YC_bC_r permits to extract uncorrelated components and favor the separation of the achromatic part from the chromatic part. Another way to solve the problem of the color components inter-correlation is the Karhunen-Loeve transform. A principal component analysis transform permits the computation of the X₁X₂X₃ color space with independent color components. HSV color space separates color in three components, two chromatic (Hue and Saturation) and one achromatic (Value). The forward and backward transforms between RGB and HSV are not linear and HSV is a less correlated space than RGB. L*a*b* is a color space with L as the Luminance and a,b as the color-opponent components. It is based on the nonlinearly-compressed XYZ color space, which is converted from RGB using the white point and the illuminant. Thus, instead of the previous cited color spaces, L*a*b*

is not device dependant. Also, L*a*b* color is designed to approximate the human vision system. In particular, the L component closely matches the human perception of lightness (Schanda, 2007). This implies notably, that the computing distance in L*a*b* is more efficient with respect to the human visual system. Indeed, the distance computation (commonly the Euclidean one) between two colors in the RGB color space is clearly not the best approach. For example, a distance of 5 in RGB does not represent the same visual difference with respect to the colors position in the color space. On the contrary, in L*a*b* color space, a deltaE (the Euclidean distance in L*a*b* color space) of 5 has the same overall visual difference. Furthermore, the literature considers that a deltaE less than 2 results in two indistinguishable colors. To illustrate this matter, MacAdam ellipses have been designed as a region on a chromaticity diagram with all colors which are indistinguishable to the average human eye from the color at the center of the ellipse. *Figure 3* illustrates these ellipses showing clearly the non uniformity of the human vision system.

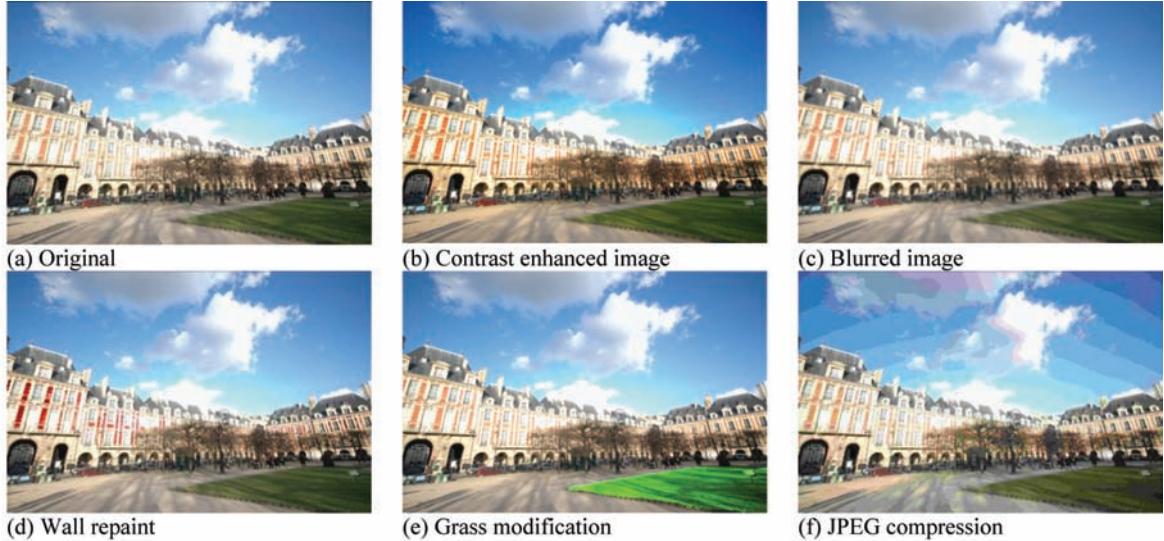
Figure 3. MacAdam ellipses plotted on the CIE 1931 xy chromaticity diagram. The ellipses are ten times their actual size, as depicted in (Macadam, 1942).



These observations suggest a new direction on how to measure the quality of a watermarked image. It is generally agreed that detecting the difference between two images is a hard problem since it refers to the human visual system, which is a subjective one. Many papers in the literature use the *famous* peak signal-to-noise ratio (PSNR) based on the mean-squared error (MSE) between two images. In the best case, the MSE measure is computed in the $L^*a^*b^*$ color space (Chareyron et al., 2006) but, most of the time, the MSE is computed from the RGB color components. Since PSNR is a component average and treats equally the errors whatever is the content of the image, it

is not enough correlated with the human perception (Lukac & Plataniotis, 2007; Thomas et al., 2007). If the watermark is precisely embedded into textured regions or edges, the PSNR is then inadequate to measure the image quality. Figure 4 illustrates this point by showing five images which have been transformed but retain the same PSNR measure (36.5 ± 0.2). With a PSNR of 36, one mark may be invisible while another may be drastically visible. This problematic use of the PSNR with watermarking algorithms is in fact similar to the color image compression problem (Lukac & Plataniotis, 2007) and several solutions have been proposed (Ebner et al., 2007; Li et al.,

Figure 4. Original image and five modified images with the same PSNR value (36.5 ± 0.2). The images were obtained by using an automatic contrast enhancement, a gaussian blurring algorithm, a manual repaint of walls and grass and, finally, a jpeg compression. The top images are visually similar. Repainting part of an image changes the perception of the image but still gives the same PSNR. Performing a JPEG compression with a constant PSNR gives a poor quality image that disturbs the viewer.



2009; Simone et al., 2008; Zhou Wang et al., 2004) to overcome the PSNR limitation. For example:

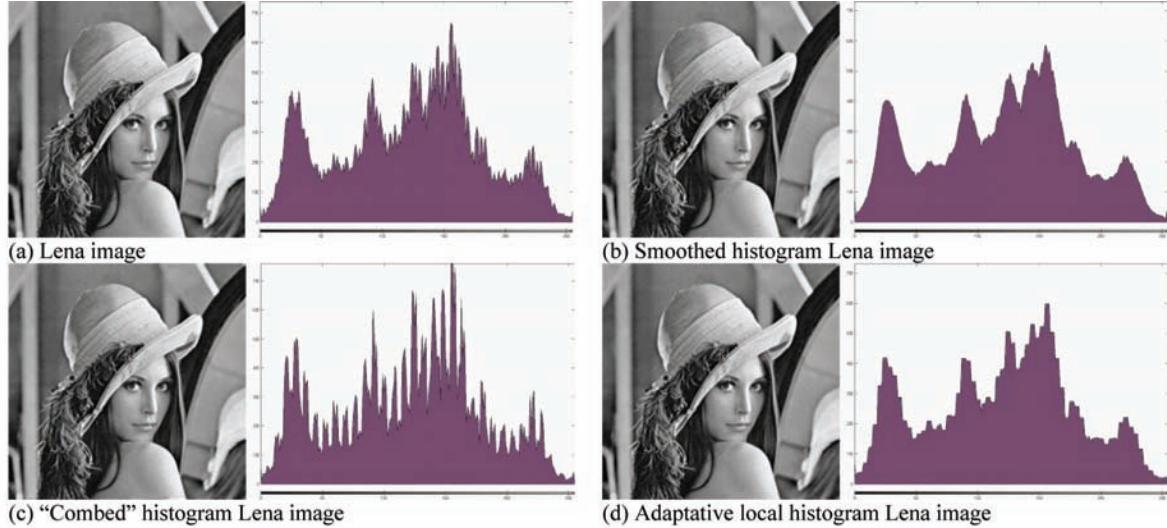
- **SSIM:** Mean Structural Similarity, built on the hypothesis than the human visual system is adapted to extract structural information from the scene.
- **VIF:** Visual Information Fidelity, a fidelity criterion that quantifies the Shannon information that is shared between the reference and the distorted image relative to the information contained in the reference image.
- **Multi-Channel Metrics:** Weighted PSNR, Weighted SSIM. The multi-channel versions of these metrics result in a single quality index which takes into account the distortion of all the color channels. As an example, the Weighted SSIM in YC_bC_r color space may be computed as the sum

$$0.8 \times \text{SSIM}(Y) + 0.1 \times \text{SSIM}(C_b) + 0.1 \times \text{SSIM}(C_r).$$

However, none of these “perceptual” measures may be considered as a standard. Most studies perform benchmarks using the PSNR and therefore propagate its intrinsic defaults. Indeed, the problem of “how to measure the difference between two images by taking into account the human visual system?” is still open.

In conclusion of this part, it appears that incorporating the color information in a watermarking process is not a trivial task. But it is a necessary one since using color is merely the most adapted way to deal with the human visual system. As noted before, the percentages of watermarking studies that are really exploiting the color information is modest but the research is very active in this domain with promising techniques as described in the next section.

Figure 5. Example of watermarked images processed with three different algorithms. A pre-determined shape is applied on the histogram, which result in no significant visual perception differences.



COLOR WATERMARKING TECHNIQUES

This section presents a panorama of both classical and new directions taken in the field of color images watermarking. It is generally agreed that the image watermarking process can be classified into three categories. The first one, *color watermarking through color histograms and quantization* embeds the watermark within the image color representation. The second one, *color watermarking through the spatial domain*, includes all the methods that modify the pixel value by using its spatial position or its neighborhood. The third one, *color watermarking through a transform domain* generates a watermark with a help of a domain transform like DCT, DFT or DWT.

Color Watermarking Through Color Histograms and Quantization

One way to watermark a color image is to use its color histogram. The main advantage of a color histogram is its robustness to rotations and other

geometric transformations. On the other hand, the main difficulty associated with color histogram is that there is a non-linear relationship between its representation and the pixel representation. The algorithm used to insert the marking is a modification of the histogram that matches a pre-determined shape. Although this is a basic process with grey level images since the grey levels are ordered, this approach is more complex with color images. Figure 5 shows the impact of three different algorithms (Bevilacqua & Azzari, 2007; Chrysochos et al., 2007) on the image histogram. It is clear that a modified histogram does not affect the perception of the image.

The problem associated with a color image is that there is one histogram per component. A naïve solution would be to watermark each histogram, but, as noted before, the color is not a simple combination of different components. As a consequence, the use of a grey level algorithm with a color image requires the ordering of the colors in one histogram. To solve this problem, (Roy & E. Chang, 2004) have proposed to use the Earth Mover Distance (EMD) which modifies an image

to reach a target histogram. Other watermarking methods based on color histogram may be noticed. (Coltuc & Bolon, 2000) proposed to use notches in the HSI color space. Number and locations of notches define the watermark, the detection is then blind and of low complexity. Similarly (C. Lin et al., 2006; P. Tsai et al., 2004) proposed also to partition and modify the feature space to insert the watermark. Another problem with color histogram is the complexity of the representation. For this reason, the embedding process proposed by (Roy & E. Chang, 2004) uses only the $C_b C_r$ color histogram extracted from the $Y C_b C_r$ color space. An even easier solution consists in using the three color histograms extracted from the HSV color space. Nevertheless, this solution is not satisfactory because it does not take into account the color inter-correlation. An alternative to the histogram approach is the modification of the three dimensional color representation of the image. In this approach, the watermark is inserted by doing a quantization (i.e. modification) of the image color distribution. This solution presents the advantage to consider the color space entirely.

Several schemes based on a quantization process have been proposed (Chao et al., 2006; Chou & Wu, 2003; T. Liu & Zheng-ding Qiu, 2002; P. Tsai et al., 2004). The purpose of the color quantization process is to represent an image with a limited number of colors which result in a minimal visual distortion (Lukac & Plataniotis, 2007). Such schemes generally involve two steps. The first step consists in choosing an appropriate color palette. The second step consists in reconstructing the image by replacing each original color with the most similar one found in the palette. Therefore, the goal of the quantization process is to build a set of colors whereas the perceived difference between the original image and the quantized one is as small as possible. Unfortunately, there is no universal criterion that characterizes the perception of image similarities. One criterion commonly used by the quantization algorithms is the distance minimization between the input

color and its representative which is somehow equivalent to the PSNR.

It has been shown that the quality of a quantized image depends on the image content and on the grey-levels of the color palette (LUT). Likewise the quality of a watermarking process will depend on these features (Chao et al., 2006). Several papers have proposed a color watermarking scheme based on a quantization process. Among them, (Soo-Chang Pei & J. Chen, 2006) have proposed an approach which embeds two watermarks in the same host image. One watermark applies on the a^*b^* chromatic plane with a fragile mark (a mark which is not supposed to resist to a transformation). Such mark is obtained by modulating the indexes of a color palette. Another watermark applies on the L^* lightness component, this time with a robust mark. The mark is obtained by the quantization of the grey-levels. This method is innovative and interesting as the fragile watermark embedded in the chromatic component does not degrade the function of the robust watermark embedded in the luminance component. (Chareyron et al., 2006) have proposed a vector watermarking scheme which embeds one watermark in the xyY color space. The mark is obtained by modulating the pixels color values previously selected by the color quantization process. This scheme is based on the minimization of color changes between the watermarked image and the host image in the $L^*a^*b^*$ color space. This scheme is also robust to geometrical transformations and, with some limits, to JPEG compression.

On the other hand, this scheme is fragile to major color histogram changes. (P. Tsai et al., 2004) have proposed a watermark scheme which performs at the same time the pixel mapping step and the watermark embedding step. This scheme is robust for images with uniform distribution palette. Other methods based on the Quantization Index Modulation (QIM) have also been proposed. By definition, the Quantization Index Modulation (QIM) method quantizes each pixel of the host image with one index which corresponds to a color

quantizer (i.e. a set of colors). These indexes are also used to carry out the watermark information. Generally speaking, the QIM schemes present several advantages. The detection of the watermark does not require a prior knowledge of the original image and it is difficult to extract the embedded watermark with the help of statistical analysis. The main disadvantage of this method is that a large mark is required to achieve a sufficiently small error probability, therefore increasing the processing complexity. According to (Chou & Wu, 2003), in most QIM schemes, the quantization and the processing schemes are not optimal because they do not take into account the properties of the human visual system.

To guarantee the transparency of the embedded watermark, the color difference between a pixel and its watermark counterpart should be uniform and must not be perceptible through the whole image. To achieve this goal, (Chou & Wu, 2003) and (Chareyron et al., 2006) propose that uniform quantization be carried out in a uniform color space and tuned to enable imperceptible color difference between any adjacent colors in the quantized color space. *Figure 6* illustrates the color quantization approaches showing the marked image and the error map. The minimization of the deltaE distance (Chareyron et al., 2006) allows the image watermarking without any visual differences. Moreover, to further enhance the imperceptibility of the watermark in the color image, (Thomas et al., 2007) have proposed to use a quantization process which preserves the color gamut of the host image.

Color Watermarking Through the Spatial Domain

Let first recall the classical LSB (Least Significant Bit scheme) method (van Schyndel et al., 1994). Its principle is to insert a mark in the pixel low order bits, by replacing the LSB of the images with a pseudo-noise (PN) sequence or by adding a PN sequence to the data LSB. It is well-known,

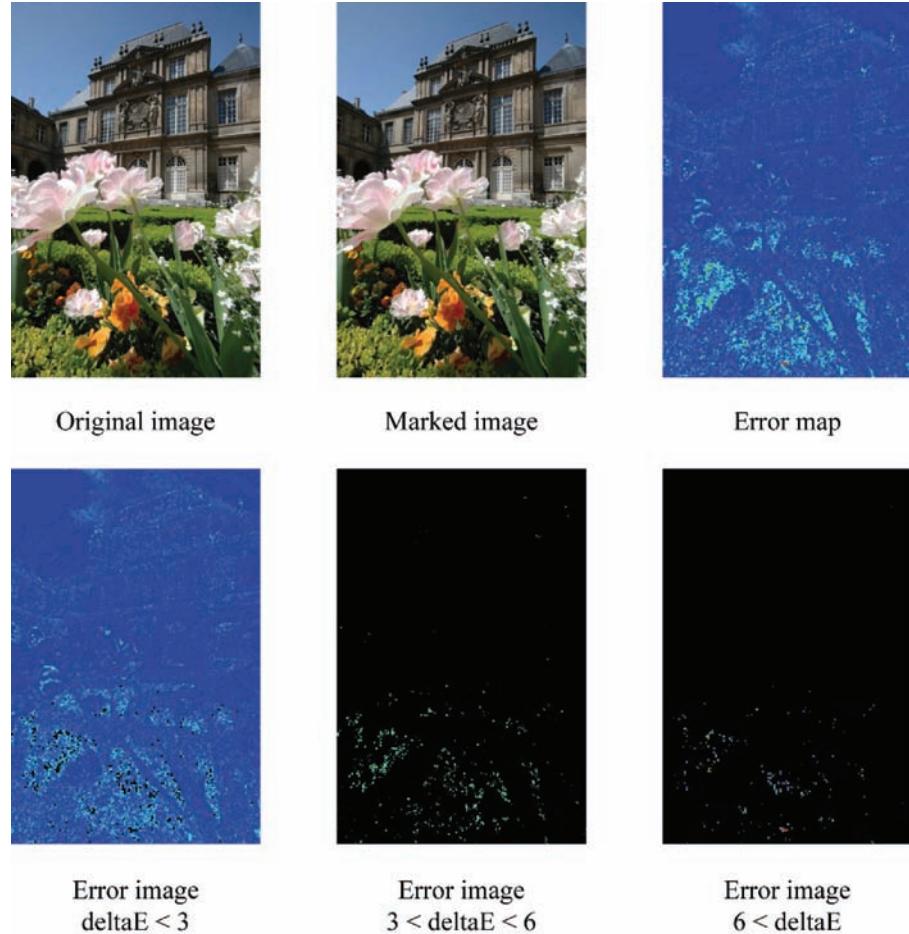
the LSB techniques provide invisible water mark but they are not robust. In particular, they are highly sensitive to noise since the watermark can be easily removed. Image manipulations, such as re-sampling, rotation, format conversion and cropping, will also, in most cases, erase the watermark. Several steganography algorithms, such as the Ez-Stego tool or the S-Tools, use the LSB insertion to produce less detectable hidden information (N. Johnson & Jajodia, 1998). The LSB scheme has been extended by (S. Pei & Cheng, 2000) who proposed a repeating LSB-insertion watermarking scheme for palette-based color images. Recently, (Xinpeng Zhang & S. Wang, 2009) have proposed a fragile watermarking scheme based on the LSB approach with a hierarchical mechanism. This scheme is then able to identify the blocks containing tampered content: the watermark data hidden in the rest blocks are used to locate the tampered pixels. In addition, using exhaustive attempts, it is possible to recover the original watermarked image.

Another classical approach based on spatial domain that takes into account the color sensitivity of the human visual system has been proposed by (Kutter et al., 1997). Taking into account human perception, this method uses only the blue channel to embed the watermark by modifying a selected set of pixel values. This method was the first approach that was explicitly designed for color images. *Figure 7* shows an example of watermark using the Kutter approach. The watermarking scheme proposed by (Kutter et al., 1997) can be described as follows (Wilkinson, 2005):

- *Watermark Generation.* The watermark is defined by a bit string of length X. The watermarking key is used as a seed for a pseudo-random generator that produces a watermark sequence of length X. An additional bit is added at the front and at the end of the sequence to form a final watermark of length X+2. These front and end ‘signature’ bits are always set to 0 and 1,

Color in Image Watermarking

*Figure 6. Illustration of the watermarking process via a color quantization (Chareyron et al., 2006). Original and marked images are shown. The error maps are computed in the L*a*b* color space with the distance deltaE. The separated error maps include only pixels with an error in the specified interval ($\text{deltaE} < 3$, $3 < \text{deltaE} < 6$, $6 < \text{deltaE}$).*

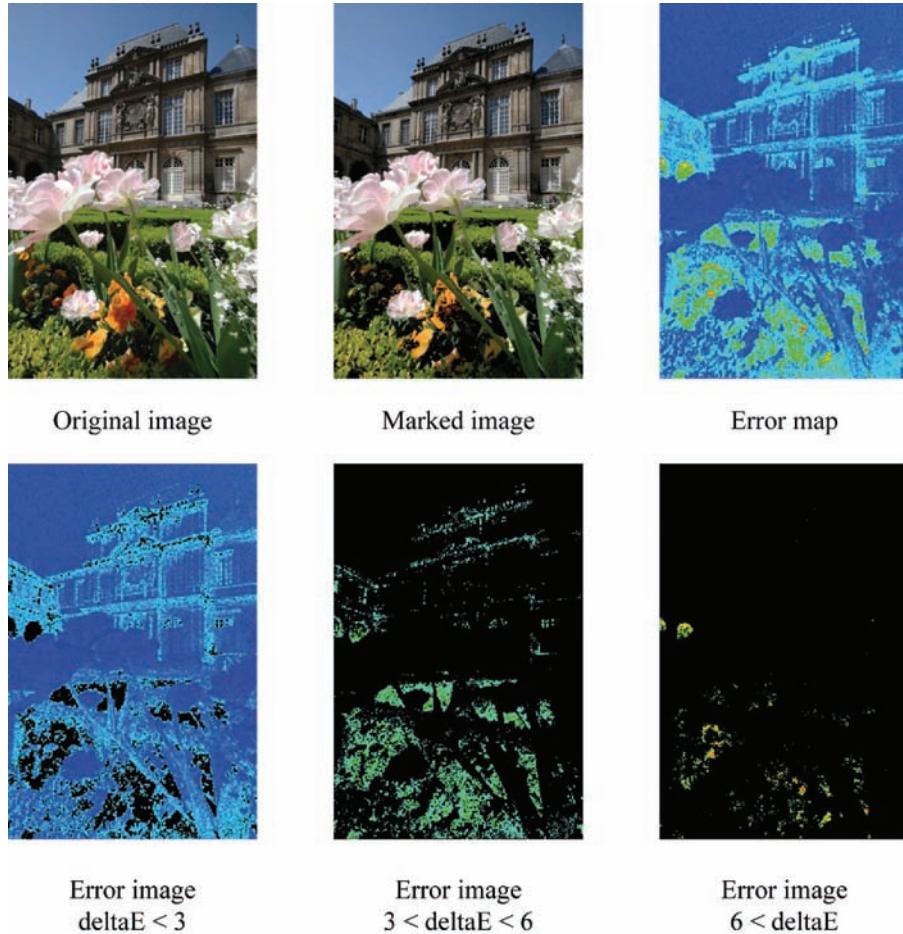


- respectively. This system is unusual in the sense that the randomization process provided is done during the embedding stage.
- *Watermark Embedding.* For every pixel a pseudo-random number x is generated in the range 0 to 1, with the watermarking key used as a seed. If the value of x for a particular pixel is smaller than a “global embedding density parameter ρ ”, then the pixel is used for embedding the watermark. The ρ parameter also lies in the range 0 to 1 and, therefore, implies that the total number of

pixels used for embedding is equal to ρ times the number of pixels in the image. To embed a watermarking mark into a pixel, a pseudo-random bit is chosen from the watermark (again by using the watermarking key as a seed), and encoded by modifying the pixel’s blue channel with a fraction of its luminance:

$$B'_{x,y} = B_{x,y} + (2s-1) L_{x,y} \alpha$$

Figure 7. Illustration of the watermarking process with a spatial insertion (Kutter et al., 1997). Original and marked images are shown. The error maps are computed in the $L^*a^*b^*$ color space with the distance δE . The separated error maps include only pixels with an error in the specified interval ($\delta E < 3$, $3 < \delta E < 6$, $6 < \delta E$).



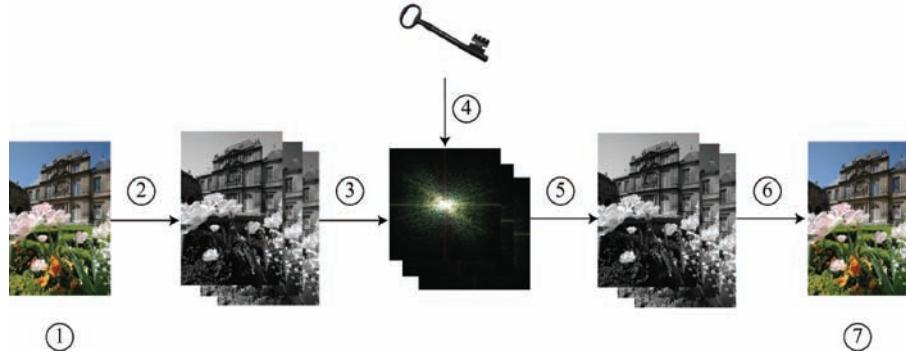
Where s is the value of the chosen bit and α is the embedding strength. The luminance of the pixel $L_{x,y}$ is computed as: $L_{x,y} = 0.299R_{x,y} + 0.587G_{x,y} + 0.114B_{x,y}$. The algorithm is designed to embed multiple copies of the watermark within the image (i.e. X should be small compared to ρ times the total number of pixels). Since both selected pixels and bit positions are randomly chosen, the distribution of the watermark bits is highly irregular.

- *Watermark Detection.* Each watermarked pixel is analyzed by using the same

deterministic sequence used during the embedding process. Since the detection process is blind, for estimate the unknown original value a combination of the values of its neighbors has been proposed. The estimation is then based on the computation of a shaped area of size c :

$$\hat{B}_{x,y} = \frac{1}{4c} \left(\sum_{i=-c}^c B_{x+i,y} + \sum_{i=-c}^c B_{x,y+i} - 2B_{x,y} \right)$$

Figure 8. Principle of the watermarking process in a transform domain. (1) original image; (2) color space (RGB, Yuv) decomposition; (3) domain transformation (FFT, DCT, Fresnel); (4) key insertion through transform coefficient modification; (5) Inverse domain transformation; (6) Final reconstruction; (7) Marked image



The difference between the value of the watermarked pixel and the estimation of its original value is averaged over all pixels used to embed the bit b :

$$\bar{\delta}_b = \frac{1}{N_b} \sum_{i=1}^{N_b} (B_{x,y} - \hat{B}_{x,y})$$

Where N_b is the number of embedding sites for bit b . The value of each $\bar{\delta}_b$ is then compared against an adaptive threshold τ , to determine the value of the watermarking bit s_b . The τ parameter is computed from the signature bits:

$$s_b = \begin{cases} 1 & \text{if } \bar{\delta}_b > \tau \\ 0 & \text{otherwise} \end{cases} \text{ where } \tau = \frac{\bar{\delta}_0 + \bar{\delta}_1}{2}$$

Finally, the Hamming distance between the original and recovered bit string is produced as the detection value.

The main weakness of Kutter's algorithm is that the first two bits have to be known (i.e. 0 and 1) for the signature extraction. Furthermore, a constant decision function has to be used to extract the watermark. This function increases the number of false recovery when the watermarked images are

attacked by geometrical transformations or some classical image processing. Several works have been proposed to improve the performance of the Kutter's technique. For example, (Yu et al., 2001) have proposed to use a neural network that learns the characteristics of the embedded watermark with respect to the watermarked image.

Color Watermarking Through a Transform Domain

Most of the transform domain watermarking schemes use the Discrete Cosine Transform (DCT), as described in *Figure 8*, to insert a mark in a image (Barni et al., 1998; Hsiang-Cheh Huang et al., 2008; Lo-Varco et al., 2005; Mohanty et al., 2006; Piva et al., 1999; Vidal et al., 2002; Xiaoqiang Li & Xiangyang Xue, 2004). These algorithms are more robust to JPEG lossy compression which is also based on the DCT. Unfortunately, these DCT based schemes are not robust to basic transformations. This masking technique embeds the marking information in significant areas of the image and therefore the hidden mark is not simply hidden in the image noise. This is the reason why this technique is preferable over the LSB approach (N. Johnson & Jajodia, 1998).

Several masking and filtering techniques can be found in the literature. For example, a DCT scheme that takes into account the statistical dependency between the color channels has been proposed (Piva et al., 1999). For each color channel, a set of coefficients is associated and then modified to embed the watermark. The strength of the watermark may be adjusted by taking into account the sensitivity of each channel. One problem with this scheme is that it embeds the watermark in the DCT domain, whereas it is known that the DFT domain would be preferable when it comes to deal with geometric manipulations such as cropping and translation (Barni et al., 2002). With this scheme, the optimality is sought with respect to the Neyman-Pearson perspective (i.e. the minimization of the probability of missing the watermark). Another problem with the DCT approach is that it may induce noise in images when the transform is used to hide a large quantity of data (Toutant et al., 2006). To avoid this problem, (Meng et al., 2007) have proposed a method based on phase-shifting interferences which enhances the imperceptibility of the large set of hidden data. Other transform based watermarking schemes which uses the DFT have been proposed: (Tsz Kin Tsui et al., 2006) encode chromatic and achromatic components separately and watermark pixels in the spatio-chromatic discrete Fourier transform by estimating the just-noticeable distortion (JND). This new approach is interesting since it performs the watermarking in the frequency domain of chromatic components. These schemes are robust to the image rotation.

Other transform watermarking scheme based on the Discrete Wavelet Transform (DWT) have been also proposed (Barni et al., 1999; Chae et al., 1998; Elbasi & Eskicioglu, 2006; T. Liu & Zheng-ding Qiu, 2002; Ming-Shing Hsieh & Din-Chang Tseng, 2006). One fundamental advantage of wavelet-based watermarking scheme is that it takes into account the local image characteristics at various resolution levels (Chou & K. Liu, 2006). Through a simultaneously spatial localization and

frequency spread of the watermark within the host image, it is then possible to embed more strongly the salient components of the image (Kundur & D. Hatzinakos, 1997). In a general way, the watermark is inserted in the transform coefficients, which is modified following different algorithms. The insertion process may be separated in 3 phases: compute the DWT coefficients, add watermark to those coefficients (for example modifying those that are above a given threshold (T_1) in the sub-bands other than the low pass sub-band) and compute the inverse DWT to reconstruct the watermarked image. Another way is to embed a pseudo-random number (PRN) sequence in a selected set of the DWT coefficients and to adjust the strength of the embedded mark with the help of scaling factors for each band. (Ming-Shing Hsieh & Din-Chang Tseng, 2006) have proposed to compute the contextual entropies of the host wavelet coefficients by fully controlling the imperceptibility of watermarked images and the robustness of watermarks. Image adaptive transform domain watermarks are particularly resistant to removal by signal processing attacks such as filtering or compression (Wolfgang et al., 1998). Thus, the DWT watermarking schemes are robust to JPEG and JPEG2000 compression. Another advantage is that they permit to determine the salient areas of an image (i.e. the perceptually most significant information) where the strength of the embedded watermark must be adjusted (Kundur & D. Hatzinakos, 2004). Another strategy has been proposed by (Lyu & Farid, 2004). This scheme is based on a first-order and high-order wavelet statistics which exploits the color statistics with the help of a non-linear Support Vector Machine (SVM) which simplify the detection of the mark. In this approach the wavelet decomposition is applied independently to each color component.

Recently some studies present combination of frequency domain transform. Firstly, some watermarking schemes which combine different frequency domain transforms have been proposed. For example, (Zhao et al., 2004) have proposed

to use a DCT-DWT domain dual watermarking scheme based on the image sub-spaces orthogonal components which provide a robust authentication process. This semi-fragile watermarking exploits the orthogonality of various domains used for authentication, color decomposition and compression. The digital watermark is made by two components: a watermark for authentication and a chrominance watermark specifically build for the DCT compression. Exploiting the same approach, (Kougiannos et al., 2009) have proposed a DCT-DWT domain dual watermarking scheme which is embedded in a hardware processor which provides near real-time performance and high reliability. These works are similar to the one done in the integration of watermarking scheme in video (J. Wang et al., 2009). Lastly, less common transforms such as the Hadamard transform (Maity & Kundu, 2009) or the Zernike transform (X. Wang et al., 2009) have been used to lower the computation cost and improve the resiliency during the compression process.

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This chapter has presented a large panel of watermarking methods which are based on the image color information. Table 1 shows the variety of approaches and lists the most important algorithms that can be considered as good color watermarking techniques. From the first studies to the recent ones, this table classifies algorithms by insertion domain (i.e. color histograms and quantization, spatial domain and transform domain). Unfortunately, it is not possible to recommend a single method with respect to the security context. Furthermore, no insertion domain is more efficient than another one and recent works still explore all the facets of color image processing. A very promising research direction would consist in developing hybrid schemes which combine both spatial and color features, which will increase

the robustness without decreasing the imperceptibility. In addition, a very promising research direction is emerging in the field of color images through multi-spectral primaries which increase the capacity and robustness while preserving the invisibility of the watermark. It will be also interesting to undertake new investigations on color appearance models (CAM) and on saliency maps that will further push the development of a new generation of watermarking schemes. The main difficulty associated with these approaches is the combination of the various saliency maps that influence the visual attention (i.e. the intensity map, the contrast map, the edginess map, the texture map, the location map) (Mohanty et al., 2006; Wilkinson, 2005; Michalis Xenos et al., 2005).

One of the next challenges of color watermarking will be also to develop watermarking algorithms specifically targeted to color videos. The main difficulty with videos, as with images, is to define good metrics which accurately evaluate the perceptual differences between videos. A very promising research direction consists in characterizing the most salient spatial-temporal components (Shukran et al., 2007) which could be used to embed into videos. Indeed, it will be interesting to undertake new investigations on color watermarking schemes based on high level color descriptors such as those used in MPEG7, as it had been done in image indexing and content-based image retrieval (Qiu, 2004). Then, to ensure watermarking of video, hardware real-time embedded system will also have to be developed (Meerwald & Uhl, 2008).

The scientific community is also faced to the benchmarking problem and unfortunately there is no standard metric that enables a systematic comparison of watermarking methods which makes the benchmarking process a subjective one. Actually, a number of separate performance metrics must be computed at low level (i.e. pixel level) and high level (i.e. region level) and combined to better fully describe the quality of a watermarked image. The future of color watermarking schemes will

Table 1. List of important algorithms for color image watermarking

Color Watermarking Through Color Histograms and Quantization	
(Bevilacqua & Azzari, 2007) (Chao et al., 2006) (Chareyron et al., 2006) (Chou & Wu, 2003) (Coltuc & Bolon, 2000) (C. Lin et al., 2006)	(T. Liu & Zheng-ding Qiu, 2002) (Lukac & Plataniotis, 2007) (Roy & E. Chang, 2004) (Thomas et al., 2007) (P. Tsai et al., 2004)
Color Watermarking Through the Spatial Domain	
(Kutter et al., 1997) (S. Pei & Cheng, 2000) (van Schyndel et al., 1994)	(Yu et al., 2001) (Xinpeng Zhang & S. Wang, 2009)
Color Watermarking Through the Transform Domain	
<i>DCT</i>	<i>DWT</i>
(Barni et al., 1998) (Campisi et al., 2002) (Chao et al., 2006) (Chou & K. Liu, 2006) (Hsiang-Cheh Huang et al., 2008) (Kundur & D. Hatzinakos, 1997) (Xiaoqiang Li & Xiangyang Xue, 2004) (Lo-Varco et al., 2005) (Meng et al., 2007) (Mohanty et al., 2006) (Piva et al., 1999) (Toutant et al., 2006) (Vidal et al., 2002) (J. Wang et al., 2009)	(Barni et al., 1999) (Chae et al., 1998) (Ping S. Huang & Chiang, 2005) (Kundur & D. Hatzinakos, 2004) (T. Liu & Zheng-ding Qiu, 2002) (Lyu & Farid, 2004)
Other Transforms	
(Barni et al., 2002) (Barni et al., 2002) (Fleet & Heeger, 1997) (Kougianos et al., 2009) (Maity & Kundu, 2009) (Ping S. Huang & Chiang, 2005) (Tsz Kin Tsui et al., 2006) (Zhao et al., 2004)	

also require the development of fidelity metrics that are more correlated with the human visual system (Lee & W. Tsai, 2009) which is by nature very complex. A new approach to this problem will necessitate the development of fidelity metrics which conjugate both human sensitivity to color differences and human sensitivity to spatial frequencies, as it is done with the S-CIELAB space (X. Zhang & Wandell, 1996) or the iCAM color space (Fairchild & G. M. Johnson, 2004). Although the CIE L*a*b* deltaE metric can be seen as a Euclidean color metric, the S-CIELAB

space has the advantage to take into account the differences of sensitivity of the human visual system in the spatial domain, such as homogeneous or textured areas. Likewise, it appears that it will be necessary to propose a new generation of benchmarking systems that measure accurately the fidelity of a watermark process in terms of color perception and the relative impact of color perception on robustness.

REFERENCES

- Barni, M., Bartolini, F., Cappellini, V., Lippi, A., & Piva, A. (1999). DWT-based technique for spatio-frequency masking of digital signatures. In *Security and Watermarking of Multimedia Contents* (Vol. 3657, pp. 31–39). SPIE.
- Barni, M., Bartolini, F., Cappellini, V., & Piva, A. (1998). A DCT-domain system for robust image watermarking. *Signal Processing*, 66(3), 357–372. doi:10.1016/S0165-1684(98)00015-2
- Barni, M., Bartolini, F., & Piva, A. (2002). Multichannel watermarking of color images. *Circuits and Systems for Video Technology. IEEE Transactions on*, 12(3), 142–156.
- Barni, M., Bartolini, F., Rosa, A. D., & Piva, A. (2002). Color image watermarking in the Karhunen-Loeve transform domain. *Journal of Electronic Imaging*, 11(1), 87–95. doi:10.1117/1.1426383
- Bevilacqua, A., & Azzari, P. (2007). A High Performance Exact Histogram Specification Algorithm. In *Image Analysis and Processing, 2007, (ICIAP 2007), 14th International Conference on* (pp. 623-628).
- Campisi, P., Kundur, D., Hatzinakos, D., & Neri, A. (2002). Compressive data hiding: an unconventional approach for improved color image coding. *EURASIP Journal on Applied Signal Processing*, (1): 152–163. doi:10.1155/S1110865702000550
- Chae, J., Mukherjee, D., & Manjunath, B. (1998). Color image embedding using multidimensional lattice structures. In *International Conference on Image Processing* (Vol. 1, pp. 460-464).
- Chao, S., Huang, H., & Chen, C. (2006). Digital watermarking of color image. In *Color imaging XI: (processing, hardcopy, and applications)* (Vol. 6058, p. 605815). SPIE.
- Chareyron, G., Coltuc, D., & Trémeau, A. (2006). Watermarking and Authentication of Color Images Based on Segmentation of the xyZ Color Space. *Journal of Imaging Science and Technology*, 50(5), 411–423. doi:10.2352/J.ImagingSci.Techol.(2006)50:5(411)
- Chou, C., & Liu, K. (2006). Performance Analysis of Color Image Watermarking Schemes Using Perceptually Redundant Signal Spaces. In *International Conference on Intelligent Information Hiding and Multimedia*, (pp. 651-654).
- Chou, C., & Wu, T. (2003). Embedding color watermarks in color images. *EURASIP Journal on Applied Signal Processing*, 2003, 32–40. doi:10.1155/S1110865703211227
- Chrysochos, E., Fotopoulos, V., Skodras, A., & Xenos, M. (2007). *Reversible Image Watermarking Based on Histogram Modification* (pp. 93–104). PCI.
- Coltuc, D., & Bolon, P. (2000). Color image watermarking in HSI space. In *International Conference on Image Processing* (Vol. 3, pp. 698-701).
- Ebner, M., Tischler, G., & Albert, J. (2007). Integrating Color Constancy Into JPEG2000. *Image Processing. IEEE Transactions on*, 16(11), 2697–2706.
- Elbasi, E., & Eskicioglu, A. (2006). A Semi-Blind Watermarking Scheme for Color Images Using a Tree Structure. In *Western New York Image Processing Workshop* (pp. 1-8).
- Fairchild, M. D., & Johnson, G. M. (2004). iCAM framework for image appearance, differences, and quality. *Journal of Electronic Imaging*, 13(1), 126–138. doi:10.1117/1.1635368
- Fleet, D., & Heeger, D. (1997). Embedding invisible information in color images. In *1997 Proceedings International Conference on Image Processing*, (Vol. 1, pp. 532-535).

- Hsieh, M.-S., & Tseng, D.-C. (2006). Wavelet-based Color Image Watermarking using Adaptive Entropy Casting. In *Multimedia and Expo, 2006 IEEE International Conference on* (pp. 1593-1596).
- Huang, H., Chu, C., & Pan, J. (2008). The optimized copyright protection system with genetic watermarking. *Soft Computing*, 13(4), 333–343. doi:10.1007/s00500-008-0333-9
- Huang, P. S., & Chiang, C. (2005). Novel and robust saturation watermarking in wavelet domains for color images. *Optical Engineering (Redondo Beach, Calif.)*, 44(11), 117002. doi:10.1117/1.2128416
- Johnson, N., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, 31(2), 26–34. doi:10.1109/MC.1998.4655281
- Kougianos, E., Mohanty, P., & Mahapatra, R. N. (2009). Hardware assisted watermarking for multimedia. *Computers & Electrical Engineering*, 35(2), 339–358. doi:10.1016/j.compeleceng.2008.06.002
- Kundur, D., & Hatzinakos, D. (1997). A robust digital image watermarking method using wavelet-based fusion. In *International Conference on Image Processing* (Vol. 1, pp. 544-547).
- Kundur, D., & Hatzinakos, D. (2004). Toward robust logo watermarking using multiresolution image fusion principles. *Multimedia. IEEE Transactions on*, 6(1), 185–198.
- Kutter, M., Jordan, F., & Bossen, F. (1997). Digital signature of color images using amplitude modulation. In *Storage and retrieval for image and video databases* (Vol. 3022, pp. 518–526). SPIE.
- Lee, I., & Tsai, W. (2009). Data hiding in gray-scale images by dynamic programming based on a human visual model. *Pattern Recognition*, 42(7), 1604–1611. doi:10.1016/j.patcog.2009.01.014
- Li, X., Tao, D., Gao, X., & Lu, W. (2009). A natural image quality evaluation metric. *Signal Processing*, 89(4), 548–555. doi:10.1016/j.sigpro.2008.10.007
- Li, X., & Xue, X. (2004). Improved robust watermarking in DCT domain for color images. In *Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on* (Vol. 1, pp. 53-58).
- Lin, C., Chan, D., Su, H., & Hsieh, W. (2006). Histogram-oriented watermarking algorithm: colour image watermarking scheme robust against geometric attacks and signal processing. *Vision. Image and Signal Processing*, 153(4), 483–492. doi:10.1049/ip-vis:20050107
- Liu, T., & Zheng-ding Qiu. (2002). ADWT-based color image steganography scheme. In *Signal Processing, 2002 6th International Conference on* (Vol. 2, pp. 1568-1571).
- Lo-Varco, G., Puech, W., & Dumas, W. (2005). Content Based Watermarking for Securing Color Images. *The Journal of imaging science and technology*, 49(5), 464-473.
- Lukac, R., & Plataniotis, K. (2007). *Color Image Processing* (p. 580). Boca Raton, FL: CRC Press.
- Lyu, S., & Farid, H. (2004). Steganalysis using color wavelet statistics and one-class support vector machines. In *Security, stenography, and watermarking of multimedia contents* (Vol. 5306, pp. 35–45). SPIE.
- Macadam, D. (1942). Visual Sensitivities to Color Differences in Daylight. *Journal of the Optical Society of America*, 32(5), 247–273. doi:10.1364/JOSA.32.000247
- Maity, S. P., & Kundu, M. K. (2009). DHT domain digital watermarking with low loss in image informations. *AEU - International Journal of Electronics and Communications*.

- Meerwald, P., & Uhl, A. (2008). Watermarking of Raw Digital Images in Camera Firmware: Embedding and Detection. In *Proceedings of the 3rd Pacific Rim Symposium on Advances in Image and Video Technology* (pp. 340-348). Tokyo, Japan: Springer-Verlag.
- Meng, X., Cai, L., Yang, X., Xu, X., Dong, G., & Shen, X. (2007). Digital color image watermarking based on phase-shifting interferometry and neighboring pixel value subtraction algorithm in the discrete-cosine-transform domain. *Applied Optics*, 46(21), 4694–4701. doi:10.1364/AO.46.004694
- Mohanty, P., Guturu, P., Kougianos, E., & Pati, N. (2006). A Novel Invisible Color Image Watermarking Scheme Using Image Adaptive Watermark Creation and Robust Insertion-Extraction. In *Multimedia, 2006. ISM'06. Eighth IEEE International Symposium on* (pp. 153-160).
- Pei, S., & Chen, J. (2006). Color Image Watermarking by Fibonacci Lattice Index Modulation. In *Colour in Graphics* (pp. 211–215). Imaging, and Vision.
- Pei, S., & Cheng, C. (2000). *Palette-based color image watermarking using neural network training and repeated LSB insertion*. In *13th* (Vol. 1, pp. 1–8). IPPR Conf. on Computer Vision, Graphics and Image Processing.
- Piva, A., Bartolinin, F., Cappellini, V., & Barni, M. (1999). Exploiting the cross-correlation of RGB-channels for robust watermarking of color images. In *International Conference on Image Processing* (Vol. 1, pp. 306-310).
- Qiu, G. (2004). Embedded colour image coding for content-based retrieval. *Journal of Visual Communication and Image Representation*, 15(4), 507–521. doi:10.1016/j.jvcir.2003.11.002
- Roy, S., & Chang, E. (2004). Watermarking color histograms. In *International Conference on Image Processing* (Vol. 4, pp. 2191-2194).
- Schanda, J. (2007). *Colorimetry: Understanding the CIE System*. Wiley.
- Sharma, G. (2002). *Digital Color Imaging Handbook*. Boca Raton, FL: CRC Press, Inc.
- Shukran, M., Chung, Y., & Chen, X. (2007). Implementation of a New H.264 Video Watermarking Algorithm with Usability Test. In *Human-Computer Interaction. HCI Intelligent Multimodal Interaction Environments*.
- Simone, F. D., Ticca, D., Dufaux, F., Ansorge, M., & Ebrahimi, T. (2008). A comparative study of color image compression standards using perceptually driven quality metrics. In *Applications of Digital Image Processing XXXI* (Vol. 7073, pp. 70730Z-70730Z-11). SPIE.
- Thomas, J., Chareyron, G., & Treméau, A. (2007). Image watermarking based on a color quantization process. In A. Hanjalic (Ed.), *Multimedia Content Access: Algorithms and Systems* (Vol. 6506, pp. 650603-650603-12). SPIE.
- Toutant, J., Puech, W., & Fiorio, C. (2006). Minimizing Data-Hiding Noise in Color JPEG Images by Adapting the Quantization. In *Conference on Colour in Graphics Imaging and Vision* (pp. 387-391).
- Trémeau, A., Tominaga, S., & Plataniotis, K. (2008). *Color in Image and Video Processing: Most Recent Trends and Future Research Directions*. EURASIP Journal on Image and Video Processing.
- Tsai, P., Hu, Y., & Chang, C. (2004). A color image watermarking scheme based on color quantization. *Signal Processing*, 84(1), 95–106. doi:10.1016/j.sigpro.2003.07.012
- Tsui, T. K., Zhang, X.-P., & Androulacos, D. (2006). Color Image Watermarking Using the Spatio-Chromatic Fourier Transform. In *Acoustics, Speech and Signal Processing, 2006. ICASSP 2006 Proceedings. 2006 IEEE International Conference on* (Vol. 2, pp. II-II).

- van Schyndel, R., Tirkel, A., & Osborne, C. (1994). A digital watermark. In *International Conference on Image Processing* (Vol. 2, pp. 86-90).
- Vidal, J., Madueno, M., & Sayrol, E. (2002). Color image watermarking using channel-state knowledge. In *Security and watermarking of multimedia contents IV* (Vol. 4675, pp. 214-221).
- Wang, J., Liu, J. C., & Masilela, M. (2009). A real-time video watermarking system with buffer sharing for video-on-demand service. *Computers & Electrical Engineering*, 35(2), 395–414. doi:10.1016/j.compeleceng.2008.06.011
- Wang, X., Xu, Z., & Yang, H. (2009). A robust image watermarking algorithm using SVR detection. *Expert Systems with Applications*, 36(5), 9056–9064. doi:10.1016/j.eswa.2008.12.040
- Wang, Z., Bovik, A., Sheikh, H., & Simoncelli, E. (2004). Image quality assessment: from error visibility to structural similarity. *Image Processing. IEEE Transactions on*, 13(4), 600–612.
- Watson, A. B. (Ed.). (1993). *Digital images and human vision* (p. 224). Cambridge, MA: MIT Press.
- Wilkinson, S. (2005). *Hide and seek: robust digital watermarking*. Technical Report, School of computing. Leeds, UK: University of Leeds.
- Wolfgang, R., Podilchuk, C., & Delp, E. (1998). The effect of matching watermark and compression transforms in compressed color images. In *Image Processing, ICIP 98, Proceedings, 1998 International Conference on* (Vol. 1, pp. 440-444 vol.1).
- Xenos, M., Hantzara, K., Mitsou, E., & Kostopoulos, I. (2005). A model for the assessment of watermark quality with regard to fidelity. *Journal of Visual Communication and Image Representation*, 16(6), 621–642. doi:10.1016/j.jvcir.2005.03.006
- Yu, P., Tsai, H., & Lin, J. (2001). Digital watermarking based on neural networks for color images. *Signal Processing*, 81(3), 663–671. doi:10.1016/S0165-1684(00)00239-5
- Zhang, X., & Wandell, B. (1996). A spatial extension of cielab for digital color image reproduction. *Journal of the Society for Information Display*, 5(1), 61–63. doi:10.1889/1.1985127
- Zhang, X., & Wang, S. (2009). Fragile watermarking scheme using a hierarchical mechanism. *Signal Processing*, 89(4), 675–679. doi:10.1016/j.sigpro.2008.10.001
- Zhao, Y., Campisi, P., & Kundur, D. (2004). Dual domain watermarking for authentication and compression of cultural heritage images. *Image Processing. IEEE Transactions on*, 13(3), 430–448.

ADDITIONAL READING

- Al-Otum, H. A., & Al-Taba'a, A. O. (n.d.). Adaptive color image watermarking based on a modified improved pixel-wise masking technique. *Computers & Electrical Engineering, In Press. Corrected Proof*.
- Androutsos, P., Kushki, A., Plataniotis, K. N., & Venetsanopoulos, A. N. (2005). Aggregation of color and shape features for hybrid query generation in content based visual information retrieval. *Signal Processing*, 85(2), 385–393. doi:10.1016/j.sigpro.2004.10.005
- Bartolini, F., Barni, M., Cappellini, V., & Piva, A. (1998). Mask building for perceptually hiding frequency embedded watermarks. In *International Conference on Image Processing* (Vol. 1, pp. 450-454).
- Bas, P., & Chassery, J. (2004). Tatouage couleur adaptatif fondé sur l'utilisation d'espaces percep-tifs uniformes. *Traitemet du Signal*, 21, 517–531.

- Battiato, S., Catalano, D., Gallo, G., & Gennaro, R. (2000). Robust Watermarking for Images Based on Color Manipulation. In *Proceedings of the Third International Workshop on Information Hiding* (Vol. 1768, pp. 302-317). Springer-Verlag.
- Benedetto, F., Giunta, G., & Neri, A. (2005). A new color space domain for digital watermarking in multimedia applications. In *International Conference on Image Processing* (Vol. 1, pp. I-249-52).
- Chan, C., Chang, C., & Hu, Y. (2005). Color image hiding scheme using image differencing. *Optical Engineering (Redondo Beach, Calif.)*, 44(1), 017003. doi:10.1117/1.1827223
- Chareyron, G., & Tréneau, A. (2006). Color Images Watermarking Based on Minimization of Color Differences. In *Multimedia Content Representation* (pp. 82–89). Classification and Security. doi:10.1007/11848035_13
- Chaumont, M., & Puech, W. (2007). A fast and efficient method to protect color images. In *Visual Communications and Image Processing* (Vol. 6508, p. 65081T). SPIE.
- Cheng, J., & Kot, A. C. (2009). Steganalysis of halftone image using inverse halftoning. *Signal Processing*, 89(6), 1000–1010. doi:10.1016/j.sigpro.2008.12.002
- Colombari, A., Fusillo, A., & Murino, V. (2007). Segmentation and tracking of multiple video objects. *Pattern Recognition*, 40(4), 1307–1317. doi:10.1016/j.patcog.2006.07.008
- Cox, I., Miller, M., & Bloom, J. (2001). *Digital Watermarking*. Morgan Kaufmann Publishers.
- Da Rugna, J., Konik, H., & Chareyron, G. (2007). Content verification scheme for peer-2-peer video sharing. In *Signal Processing and Its Applications, 2007. ISSPA 2007. 9th International Symposium on* (pp. 1-4).
- Findık, O., Bayrak, M., Babaoglu, İ., & Çomak, E. (2008). *Color Image Watermarking Scheme Based on Efficient Preprocessing and Support Vector Machines*. Communications in Computer and Information Science (Springer Berlin Heidelberg., Vol. 15, pp. 398-406).
- Kilner, J., Starck, J., Guillemaut, J., & Hilton, A. (2009). Objective quality assessment in free-viewpoint video production. *Signal Processing Image Communication*, 24(1-2), 3–16. doi:10.1016/j.image.2008.10.004
- Kuo, C., & Cheng, S. (2007). Fusion of color edge detection and color quantization for color image watermarking using principal axes analysis. *Pattern Recognition*, 40(12), 3691–3704. doi:10.1016/j.patcog.2007.03.025
- Leung, B. W., Ng, F. Y., & Wong, D. S. (2009). On the security of a visual cryptography scheme for color images. *Pattern Recognition*, 42(5), 929–940. doi:10.1016/j.patcog.2008.08.031
- Qi, X., & Qi, J. (2007). A robust content-based digital image watermarking scheme. *Signal Processing*, 87(6), 1264–1280. doi:10.1016/j.sigpro.2006.11.002
- Qian-Chuan Zhong, Qing-Xin Zhu, & Ping-Li Zhang. (2008). A Spatial Domain Color Watermarking Scheme based on Chaos. In *Apperceiving Computing and Intelligence Analysis, 2008. ICACIA 2008. International Conference on* (pp. 137-142).
- Tzeng, C.-H., Yang, Z.-F., & Tsai, W.-H. (2004). Adaptive data hiding in palette images by color ordering and mapping with security protection. *Communications. IEEE Transactions on*, 52(5), 791–800. doi:10.1109/TCOMM.2004.826379
- Voyatzis, G., & Pitas, I. (1999). The use of watermarks in the protection of digital multimedia products. *Proceedings of the IEEE*, 87(7), 1197–1207. doi:10.1109/5.771072

KEY TERMS AND DEFINITIONS

CAM: Color Appearance Model establishes the relationships between viewing conditions and color appearance. These models are design for the prediction of the appearance of the spatially-simple color stimuli under a wide variety of viewing conditions.

CIE: The International Commission on Illumination (usually known as the CIE for its French name *Commission internationale de l'éclairage*) is the international authority on light, illumination, color, and color spaces. Official web site: http://www.cie.co.at/index_ie.html.

DeltaE: The deltaE also called CIE76 provides a perceptual measure of distance between two colors. To better resolve the perceptual uniformity issues, CIE provides also other distance, like CIE94 and CIEDE2000.

Color-Opponent: The color opponent process is a color theory that states that the human visual system interprets information about color

by processing signals from cones and rods in an antagonistic manner (http://en.wikipedia.org/wiki/Opponent_process)

Illuminant: Characteristic of the light applied to the scene during acquisition or viewing. It includes use of both artificial sources such as lamps and natural illumination such as daylight.

Palette: A palette is a finite set of colors, usually small, which defines all available colors to an image or a display. Also called colormap or Look-Up Table (LUT).

PSNR: The peak signal-to-noise ratio, abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.

XYZ: The CIE 1931 XYZ color space is based on a direct graph of the original X, Y and Z tristimulus functions defined by the CIE in 1931. This color space is used by all perceptual color spaces: $Lu'v'$, $L^*a^*b^*$.

Chapter 4

Geometric Distortions— Invariant Digital Watermarking Using Scale-Invariant Feature Transform and Discrete Orthogonal Image Moments

Shiraz Ahmad

Pakistan Atomic Energy Commission, Pakistan

Zhe-Ming Lu

Zhejiang University, P. R. China

ABSTRACT

Many proposed digital image watermarking techniques are sensitive to geometric attacks, such as rotation, scaling, translation, or their composites. Geometric distortions, even by slight amounts, can inevitably damage the watermark and/or disable the capability of the watermark detector to reliably perform its function. In this chapter, the authors exploit the invariant image features to design geometric distortions-invariant watermarking system, and present two watermarking techniques. First technique utilizes the bounding box scale-invariant feature transform and discrete orthogonal Hahn moments to embed the watermark into the selective image patches, and the second technique uses only the Hahn moments to globally embed watermark into the whole image. First technique is non-blind and uses the original image during detection. While exhibiting excellent resistance against different geometric distortions, this technique also has fairly good resistance to image cropping like attacks. However, this technique exhibits a reduced data payload. The second technique is designed to be blind and the watermark is blindly extracted using the independent component analysis. For this technique an improved data payload is achieved but with a little compromise on resistance against cropping like attacks. The implementations are supported with thorough discussions and the experimental results prove and demonstrate the effectiveness of the proposed schemes against several kinds of geometric attacks.

DOI: 10.4018/978-1-61520-903-3.ch004

Figure 1. A screenshot of worldwide information growth ticker showing total bytes of information created from January 1, 2009 to June 1, 2009, 11:42:07 am (GMT+08:00 time zone) (© 2009 EMC Corporation. Used with permission)



INTRODUCTION

Digital universe is exploding and expanding at an enormous speed, and in year 2008 it was forecasted (Gantz, Chute, Manfrediz, Minton, Reinsel, Schlichting, & Toncheva, 2008) that the amount of information created, captured, or replicated had already exceeded the available storage capacity for the first time in 2007. The digitized information created and replicated during January 10, 2008 to March 12, 2008, 10:27:12 am, alone, was amounted to “80,709,885,774,375, 825,096” bytes of data (Paul 2008), and similarly from January 1, 2009 to June 1, 2009 (11:42:07 am – GMT+08:00 time zone) only the bytes of information created amounted to a total of “320,837,056,065,112,513,148” bytes (EMC, 2009), as shown in Figure 1. While not all the information created and transmitted is stored, it was also estimated that by 2011, almost half of the digital universe will not have a permanent home (Gantz, Chute, Manfrediz, Minton, Reinsel, Schlichting, & Toncheva, 2008). However, the size and explosive growth of the digital universe are only two of its characteristics. The most critical associated issues include: handling, storage, management, and security. It is noted that the visual contents like images and video account for the largest portion of the digital universe (Paul

2008). So if we look at digitized multimedia data (a combination of any of text, image, video, or other types of data), then it turns out to be largest in terms of size of the digital universe. As estimated figures, 30 per cent of information created today is “*security intensive*”, and it may grow to 45 per cent by the end of year 2012 (Gantz & Reinsel, 2009). Evidently, an unlimited set of options, opportunities, and challenges can be realized and perceived in the life cycle of the digital data from birth, creation, replication, manipulation and composite creation (using different types of digital data), to non-stopping and endless distribution and sharing. Hence, this creates more challenging and complex issues regarding data authenticity, security, and protection.

As a matter of fact, and with the advent of digital media, exact replication of multimedia contents and their swift distribution through open networks is no more a problem in this mature digital age. The availability of modern technology and contemporary techniques has not only reduced the time spans involved in the reproduction of digital media data, associated duplication efforts, and quick distribution of contents over the globe by great factors but also eliminated the quality degradation problems as those associated with the analog domain (Ahlzen & Song, 2003). While, without requiring much effort, this fact is

helping the content owners, creators, and distributors in easy creation, production and distribution of their works; the same fact is raising serious security concerns about the acts of illicit copying and manipulations, breaching the rightful ownership. All this has created a pressing need to defy the contemporary dilemma of media reliability, authenticity, security, copyright legitimacy, and protection (Dugelay & Petitcolas, 2000). Especially and more specifically this need arises due to the existence and easy realization of numerous kinds of digital intimidations, counterfeiting, and forgery threats (including incidental, accidental, and intentional manipulations and doctoring to the digital contents). Modern digital watermarking techniques, with a broad spectrum of classifications (Ahmad, 2001), provide a marvelous way to get out of this vicious circle and ensure the embedding of trustworthy, robust, and undetectable/imperceptible watermarks in digital assets (audio, video, images, text data, or multimedia) for later truthful recovery. These unique watermarks (or identity information) can be used to discourage illicit reproduction and malicious data tampering (Fridrich 1999) through tracing, detecting, and some times even compensating (Kutter, 1999) the possible malicious media modifications. Furthermore, instead of just ensuring the authenticity or integrity of the media data, as a digital signature or a digital seal does, digital watermarks may also be aimed to identify (Ahmad, 2000) the author, owner, distributor, authorized user, origin, or usage rights of multimedia data (an image, video clip, or audio clip). However, in order to be useful, a watermark must be perceptually invisible and have robustness against image processing and a variety of possible attacks by those who seek to pirate the material (Voloshynovskiy, Pereira, Herrigel, Baumgartner, & Pun, 2000; Voloshynovskiy, Pereira, Pun, Eggers, & Su, 2001). Therefore, while keeping in view the possibility of a number of potential media attacks (Petitcolas, Anderson, & Kuhn, 1998; Ruanaidah & Pun, 1998), such as: rotation, scaling, translation, composite (af-

fine) transformations, geometric distortions, A/D conversion, low-pass filtering, compression, cropping, etc.; often the attention is paid to, and the intentions are aimed at designing the watermarking systems with the capabilities that: the watermark information can not only survive different kinds of attacks and yet remain intact or detectable (Lin, Wu, Bloom, Cox, Miller, & Lui, 2001) but alternatively (and as the least level of requirement) the system can also be used to establish a level of confidence (Cox, Miller, & Bloom, 2001) about the authenticity or presence/absence of the watermark, when the watermarked media undergoes even quite a minor levels of modifications and manipulations. As a result, there has been much emphasis on the work to introduce robustness to the watermarking systems against common signal processing operations. However, recently it has become clear that for many cases even very small level of modifications to media data can prevent the detection of watermark in many watermarking techniques, and can easily fail the detector. This problem can be more pronounced for the blind watermarking systems, where the original image is not available to the detector. Moreover, in many applications, the attackers may also attempt to defeat the security feature of the watermarking system by intentionally and slightly modifying the state of media (through minor levels of scaling, rotation, translation, etc. attacks) in such a manner that although the commercial value of the media still remains (or appear to remain) intact and acceptable but the watermark detector's capability to check the presence of watermark is lost. Hence, the security or protection feature associated with the media product is lost and/or compromised. Therefore, a robust watermarking system must be capable of re-synchronizing itself against scaling and rotation (Alattar & Meyer, 2003).

For practical watermarking systems, robustness against common signal processing and geometric attacks is highly desirable so as to meet the different application requirements. One of the main obstacles in the image watermarking systems is the

geometric manipulation of watermarked images. Examples of geometric attacks include transformations such as: rotation, scaling, translation, shearing and random bending, change of aspect ratio, etc. (Petitcolas, Anderson, & Kuhn, 1998; Kutter & Petitcolas, 1999; Cox & Linnartz, 1997). Geometric distortions can inevitably damage the watermark signal and affect the synchronization mechanism which is crucial for the correct detection of watermark signal. This is due to the fact that even quite minor geometric manipulations to the watermarked image could dramatically reduce the detector's ability to perform the watermark detection function. Furthermore, while such attacks are easy to implement they can easily render many of the affective watermarking systems ineffective. It is also well known that many existing image watermarking algorithms are vulnerable to geometric attacks (Lee & Lee, 2005). Despite all the efforts and progress made in this direction, making the watermarking system robust against geometric distortions is still a challenging problem and remains an open issue.

Some research has been done to deal with the watermark's vulnerability to geometric distortions, and various methods have been proposed (Alghoniemy & Tewfik 2004; Xin, Liao, & Pawlak, 2004; Xin, Liao, & Pawlak, 2004b) to cater with these attacks. These can briefly be summarized and categorized into three major groups as follows. First category is based on the geometric distortion inversion, i.e. the possible geometric distortions are first attempted to be reversed so as to bring the image to its potential normal/original state, and then follows the watermark detection. For this purpose either a registration pattern, known as "*pilot signal*", is inserted into the host signal along with the watermark (Pereira & Pun, 2000) or the watermark is designed with a specialized structure (Kutter, 1999), so that during the stage of watermark detection the involved geometric distortions can be identified, measured, and compensated. Thus, the geometric distortions can be removed by an inversion process. In such systems

the image is first corrected with the estimated distortions and the detection of the watermark is performed afterwards. The nature of this approach is the incorporation of two watermarks, one for data payload and the other for the detection of distortion. A theoretical analysis on the bit error rate for this pilot-based approach, under a number of geometric attacks has also been studied and investigated (Rodríguez & González, 2002). This approach requires the detection of both the synchronization pattern and the watermark. A potential problem arises when a common template is used for different watermarked images, making it susceptible to collusion-type detection of the template (Cox, Miller, & Bloom, 2001). Similarly, an alternative approach through the usage of a deformable mesh (Davoine, 2000; Dong, Brankov, Galatsanos, & Yang, 2002; Dong, Brankov, Galatsanos, Yang, & Davoine, 2005) has also been adopted so that the introduced distortions can be corrected and improved watermark synchronization can be achieved. The second category is based on image normalization (Alghoniemy & Tewfik, 2000; Dong & Galatsanos, 2002; Dong, Brankov, Galatsanos, Yang, & Davoine, 2005; Kang & Delp, 2004; Mohamed, & Abbes, 2007; Zheng & Zhao, 2007). An image can be normalized to a certain position, orientation and size, which are invariant to image translation, rotation and scaling. The host image is normalized prior to watermark insertion, and the watermarked image is de-normalized back to its original look after watermark insertion. At the watermark detector, the test image has to undergo the same normalization process before watermark detection. An outstanding disadvantage of this approach is that an image is to be transformed twice in the watermarking process, which inevitably causes extra quality degradation of the image on top of the watermark-induced distortion. The third category is based on the invariance properties of some image features. Different image features have different invariance properties and these properties can be exploited to design the watermarking systems which can

exhibit resistance against different attacks. Many geometrically robust watermarking schemes are based on invariant domains, such as Fourier-Mellin transform and the Zernike transform. Ruanaidh and Pun (1998) first reported the rotation, scaling, and translation (RST) invariant watermarking in the Fourier-Mellin transform domain. Kim and Lee (2003) designed an RST invariant watermark in the Zernike domain. The main drawback was that the watermarked images were considerably degraded and could not resist the cropping attacks, as the watermark was embedded in the global image. A solution to this problem was proposed by using a feature-based watermark synchronization method (Bas, Chassery, & Macq, 2002). Since certain image features exhibit robustness properties against different geometric distortions and these properties can be exploited to design robust watermarking systems therefore they used the Harris corner detector to extract interest points. Then the Delaunay tessellation was applied on the detected points to produce a set of triangles. The watermark was then embedded into all of the triangles additively in the spatial domain. Another famous approach for invariant feature detection is Scale-invariant feature transform (SIFT), proposed by Lowe (Lowe, 2004). SIFT feature points are highly distinctive and they can be detected with high repeatability. Compared with Harris corners, SIFT features are more stable thus are more suitable for watermark synchronization. Recently, a SIFT based watermarking scheme was developed (Lee, Kim, & Lee, 2006). The authors extracted the feature points by SIFT and used them to generate a series of patches. The watermark was then embedded into all patches, also in the spatial domain. Similarly, the discrete orthogonal moment invariants of the images can also be used for designing the geometric distortion-invariant watermarking system.

The moments, due to their ability to represent global features, have found extensive applications in the field of image processing (Teague, 1980; Teh & Chin, 1988; Lo & Don, 1989; Papademetriou,

1992; Flusser & Suk, 1993; Luo, Hamitouche, Dilenseger, & Coatrieux, 1993; Luo, Xie, & Bao, 1994; Tuceryan, 1994; Liao & Pawlak, 1996; Shen, & Ip, 1997; Mukundan & Ramakrishnan, 1998; Shen, Ip, Cheung, & Teoh, 1999). Geometric moments of digital images are used to capture global features for applications in pattern recognition, image analysis and object classification. Moments of orthogonal basis functions, such as the Legendre and Zernike polynomials introduced by Teague (1980) can be used to represent the image by a set of mutually independent descriptors with a minimal amount of information redundancy (Kan & Srinath, 2002). However, these moments present several problems. The most important of these problems is inaccuracy arising due to quantization errors introduced by the discrete approximation of the continuous integrals and the space-coordinate transformations. Additionally, these approximations present a very large computational burden. The above problems motivated to the use of discrete orthogonal polynomials as the basis set, and to define the corresponding moments directly on the image coordinate space. Discrete orthogonal moments can directly be defined in the domain of the image coordinate space and their realization does not involve any discrete approximation in the numerical implementation. Hence, the basis functions exactly satisfy the orthogonality property and yield a superior image reconstruction. Furthermore, in order to ensure numerical stability, the basis polynomials can be pre-normalized to create a set of weighted orthonormal polynomials to define the corresponding discrete orthogonal moments. In effort to this, Tchebichef moments were proposed by Mukundan, Ong, and Lee (2001). These are discrete orthogonal moments and present a number of advantages over moments of continuous orthogonal basis (Mukundan, 2004). Mukundan's study showed that the implementation of Tchebichef moments do not involve any numerical approximation since the basis set is orthogonal in the discrete domain of the image coordinate space. This property made Tchebichef

moments superior to the conventional continuous orthogonal moments in terms of preserving the analytical property needed to ensure information redundancy in a moment set. In later studies, the same was investigated and observed for the sets of discrete orthogonal moments such as Krawtchouk moments (Yap, Paramesran, & Ong, 2003), Hahn moments (Zhou, Shu, Zhu, Toumoulin, & Luo, 2005; Yap, Paramesran, & Ong, 2007), and Racah moments (Zhu, Shu, Liang, Luo, & Coatrieux, 2007), by using corresponding discrete orthogonal polynomials as the basis functions.

Blind source separation, also known as blind signal separation, is the process of separating a set of signals from a set of mixed signals, without the aid of information (or with very little information) about the source signals or the mixing process. The strength of the blind signal separation model relies on the assumption of statistical independence (i.e., the mixed signals do not correlate with each other and are mutually statistically independent or de-correlated), and no a-priori information about, e.g., the characteristics of the source signals, the mixing matrix or the arrangement of the sensors is needed. Blind signal separation separates a set of signals into another set of signals such that the regularity of each resulting signal is maximized, and the regularity between the signals is minimized (i.e. statistical independence is maximized). Because temporal redundancies (statistical regularities in the time domain) are “clumped” in this way into the resulting signals, the resulting signals can be more effectively de-convolved than the original signals. There are different methods of blind signal separation, such as: independent component analysis, principal components analysis, singular value decomposition, non-negative matrix factorization, etc. Recently, blind source separation using independent component analysis (ICA) has gained increased attention in research because of its potential applications in signal processing such as in speech recognition systems, medical signal processing, telecommunications, etc. ICA is a general purpose statistical technique, which

extracts a linear transformation for a given set of observed data such that the resulting variables are as statistically independent as possible. Viewing the watermarked image as a mixed source of the original image and the watermark signal, the ICA technique can be applied to detect and extract the watermark signal form the original source signal.

In this chapter two geometric-invariant digital image watermarking techniques have been proposed which apply the source-independent watermark signals to the original images. These techniques exploit the invariant properties of images for the watermarking purposes. Since the proposed techniques rely on using certain invariant image features therefore the presented watermarking systems are robust against several geometric attacks (affine transformations). The first technique utilizes the scale-invariant features and discrete moment invariants of the images to establish a non-blind watermarking system. In this technique the watermark is applied only to some selected local image patches, instead of applying to the whole image. The scale-invariant feature transform (SIFT) is used to select suitable affine-invariant (invariant to rotation, scale, translation, or any combination of these) patches from the image and then the watermark information is embedded into these selected patches. Since the original image is needed for watermark detection therefore it is a non-blind scheme. The second technique utilizes only the discrete moment invariant features of the images and the whole image is used for embedding the watermark information. For this technique no prior information of the watermark or the source image is required therefore this is a blind watermarking system. For this system, ICA is utilized by the watermark detector to blindly detect and extract the watermark signal. The watermark signal is designed to be random and independent to the original image. Discrete orthogonal Hahn moments (with the settings for Tchebichef moments and Krawtchouk moments) are used for constructing the moment invariants in both the schemes and the watermark is

embedded by modifying the selected invariant moments of the original image. The accuracy of the watermark detector depends on the secret key used in the embedding process, and the statistical independence between the original image and the watermark. Experimental results demonstrate that the presented watermarking systems are robust to various geometric attacks performed by Stirmark.

The organization of the chapter is as follows. The next section of this chapter presents some preliminary stuff and explains some basic ideas which serve as essential tool for better understanding. The basic details of some simple kinds of geometric transformations and their composites; the method for finding the distinctive invariant features of an image; and a thorough discussion on the construction, formulation and significance of the image moments is covered in this section. For the purpose of clarity and better understanding some simple yet very useful nice examples are presented in this section. The presented discussion serves as the building block for upcoming discussions and formulations in the next sections. The third section contains a detailed discussion about the prime tool used in this chapter: the discrete orthogonal moments. Starting from the definition of different kinds of discrete orthogonal polynomials, this section presents detailed discussion on the computation of discrete orthogonal image moment descriptors, reconstruction of images using these descriptors, and the construction of their invariant counterparts (moment invariants). Since watermarked images may be attacked by a set of geometric operations (rotation, scale, translation, or a composite of these operations) therefore construction of moment invariants plays very important role in the estimation of distortion parameters, and hence the restoration of the original state of the signal. The set of Tchebichef, Krawtchouk, and Hahn moments are covered in this section and it has also been proved that Hahn moments provide a unified representation of both Tchebichef and Krawtchouk moments. This is useful in the sense that by adjusting just

Hahn polynomial parameters both Tchebichef and Krawtchouk polynomials, and hence their moments and moment invariants, can be realized. The methodology of the watermark embedding and detection for the two proposed watermarking schemes, one of which is non-blind and the other is blind, is presented in the fourth section of this chapter. The presented methods use invariant properties of the images and the discrete orthogonal moment invariant descriptors to embed the watermark signal, so as to be robust to different geometric operations. The fifth section presents experimental results for the presented watermarking schemes and demonstrates effectiveness of the proposed watermarking systems against different geometric operations. Sixth section highlights the future research directions and section seven concludes the chapter. Finally, the acknowledgements are presented in the last section of the chapter.

SOME SYSTEM PRELIMINARIES

A brief discussion of some preliminaries presented in the following sub-sections will be helpful to gain a clear and better understanding of the details appearing in the next sections.

Geometric Distortions and Transformations for Digital Images

Geometrical distortions or transformations change the spatial relationship between the objects in an image. One of the principle applications of geometric transformations concerns the possibility of correcting the digital images for which the spatial relationships might have been distorted some way. Geometric distortions are a common type of attacks applied to the digital images and can be applied in many ways as single or composite transformations. In watermarking applications a variety of geometric attacks can be applied to digital images so as to distort the media in such a way that either the watermark is lost or, at least,

the synchronization/detection capability of the watermark detector is distorted to make watermark detection difficult, expensive, or impossible. Therefore, understanding of the phenomena of distortions and how they affect the images is helpful in applying corrections and compensations for the resulting distortions. With understanding of different kinds of geometric attacks a possible compensation can be applied to the digital image so that the detector can reliably perform watermark detection/assertion function. While simple and basic geometric transforms include rotation, scaling, translation, etc. more complex operations can be formulated as a combination of these, such as: rigid transformation (translation + rotation), similarity transformation (translation + rotation + uniform scaling), and the generalized affine transformation (translation + rotation + scaling + shear). Different composite geometric transform groups can be viewed as: rigid transforms \subset similarity transforms \subset affine transforms.

If an image $g(x_a, y_b)$ is said to be an affine transform of $f(x, y)$ then the generalized relationship between their coordinates can mathematically be formulated as:

$$\begin{bmatrix} x_a \\ y_a \end{bmatrix} = \mathbf{A} \begin{bmatrix} x \\ y \end{bmatrix} + \mathbf{d} \quad (1)$$

where \mathbf{A} is transformation matrix and \mathbf{d} is the translation vector, given by:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \quad (2)$$

and

$$\mathbf{d} = \begin{bmatrix} d_1 \\ d_2 \end{bmatrix} \quad (3)$$

The important issues associated with the geometric distortions include: (a) parameter estimation of the transformed coordinates, and (b) calculate/interpolate the pixel intensity values for new (integer or non-integer) coordinate positions of the transformed images. By understanding the transformation, parameter estimation can be established and implemented in the form of a mathematical relationship. Similarly new pixel intensity values for new coordinates of the transformed images can be computed through some form of weighted or un-weighted neighborhood approximation. Let us present some brief details about some of the basic and composite transformations. These details will be useful for the estimation of distortion parameters in the case when an image undergoes a geometrical transformation.

Scaling

The scaling operation performs a geometric transformation which shrinks or increases the size of an image (or part of an image). Image shrinking, commonly known as *sub-sampling*, is performed by replacement (of a larger group of pixel values by fewer arbitrarily chosen pixel values from within the group) or by interpolating the pixel values in a local neighborhood. Similarly, image *up-scaling* or zooming is performed by the other way pixel replication or interpolation. Scaling is a special case of an affine transformation and one of the most frequently used operations in image processing applications. Scaling can be applied to either whole or a part of an image and is used to change the visual appearance of an image by altering the quantity of information stored in a visual scene representation. Scaling either reduces or increases the image size along the coordinate directions. In 2D scaling operation the coordinate directions are scaled by the respective scaling factors and if the x - and y -directions are respectively scaled by the scaling factors a and b then this scaling operation can mathematically be expressed as:

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \quad (4)$$

So the coordinate position relationship is governed by:

$$\begin{cases} x_2 = ax_1 \\ y_2 = by_1 \end{cases} \quad (5)$$

The scaling can be grouped into two categories:

1. Symmetric scaling: the situation when the scaling factor in x direction is same as in the y direction. i.e. $a = b$. This group of scaling maintains the image aspect-ratio and for $a, b > 1$ the image is up-scaled and increased in size while for $a, b < 1$ the image is sub-sampled and downsized.
2. Asymmetric or non-symmetric scaling: the situation when both the x direction and y direction scaling factors are different. i.e. $a \neq b$. This group of scaling distorts the image aspect-ratio.

While coordinates for scaling operation can be related as described above, the new pixel intensity values are computed by either direct dropping (for *sub-sampling*) or by direct replication (for *zooming*) of the neighboring pixel values. As described earlier, an alternative approach is by weighted nearest-neighbor interpolation. A scaling operation example (sub-sampling and zooming) is presented in Figure 2(a).

Rotation

The rotation operator performs a geometric transform which maps the pixel position (x_1, y_1) of the input image to another pixel position (x_2, y_2) in the output image. This is achieved by rotating it about an origin through a user specified value of

angle θ . The rotation operator performs a transformation of the form:

$$\begin{cases} x_2 = \cos \theta * (x_1 - x_0) - \sin \theta * (y_1 - y_0) + x_0 \\ y_2 = \sin \theta * (x_1 - x_0) + \cos \theta * (y_1 - y_0) + y_0 \end{cases} \quad (6)$$

where (x_0, y_0) are the coordinates of the center of rotation (in the input image). In the matrix form this relationship can be represented as:

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} (x_1 - x_0) \\ (y_1 - y_0) \end{bmatrix} + \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \quad (7)$$

If the rotation center is normalized as $(0, 0)$ then this relationship simplifies to:

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \quad (8)$$

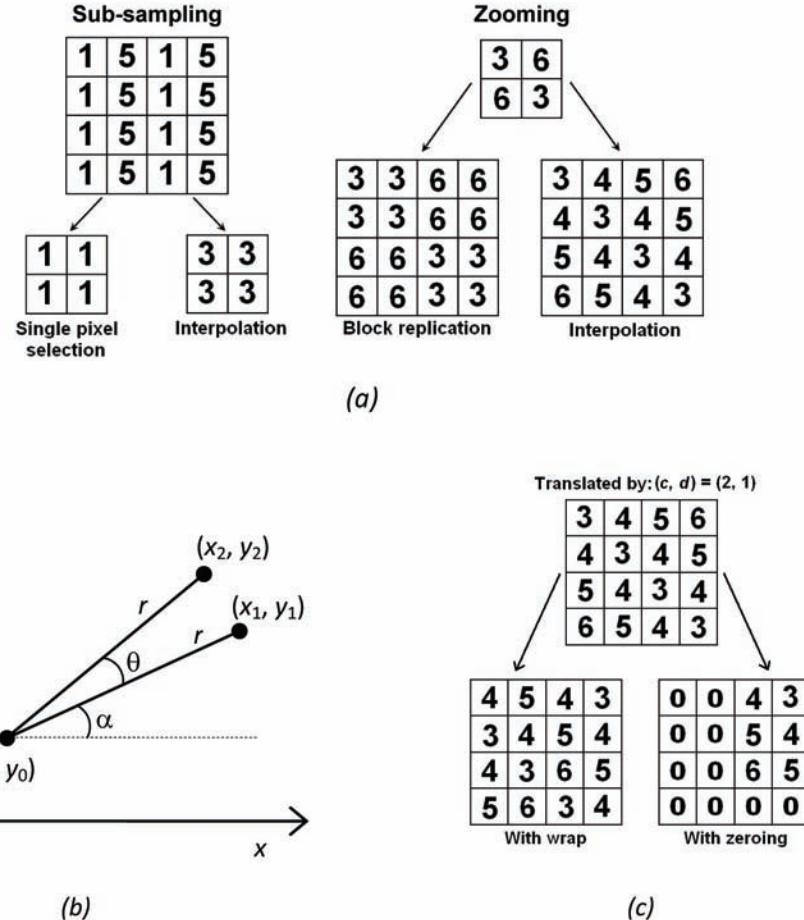
Pictorially the rotation process is illustrated in Figure 2(b). With rotation center normalized as $(0, 0)$, an alternative way to deduce the same relation is:

$$\begin{cases} x_2 = r \cos(\theta + \alpha) = r \left(\frac{x_1}{r} \cos \theta - \frac{y_1}{r} \sin \theta \right) = x_1 \cos \theta - y_1 \sin \theta \\ y_2 = r \sin(\theta + \alpha) = r \left(\frac{x_1}{r} \sin \theta + \frac{y_1}{r} \cos \theta \right) = x_1 \sin \theta + y_1 \cos \theta \end{cases} \quad (9)$$

$$\text{where } \cos \alpha = \frac{x_1}{r} \text{ and } \sin \alpha = \frac{y_1}{r}$$

Rotation is also a special case of affine transformation and it is to be noted that the rotation operation maps some output locations (x_2, y_2) outside the boundary of the image, as these locations do not fit within the original dimensions of the input image. In such cases, and depending upon the implementation, the locations moving out the image dimensions are either simply ignored or

Figure 2. Illustration of scaling, rotation and translation operations for picture elements: (a) Image patch scaling (sub-sampling and zooming) (b) pixel rotation sketch, (c) image patch translation



specifically compensated by extending the image domain size. After rotation operation, the pixel locations from which the image data has been rotated (and no other data occupy their places) are usually filled with black pixels. Unlike the translation operation, following in the next sub-section, the rotation operations can produce non-integer coordinates and different resampling techniques may be employed to generate the intensity of pixels at each integer position. For example, either the pixel intensity value can be approximated by the nearest non-integer neighbor or the by computing a weighted average of n nearest non-integer neighbor values.

Translation

The translation operation performs a geometric transformation which maps the position of each picture element in an input image to a new position in an output image, such that the dimensionality of the two images is often, but not necessarily be, the same. This operation is carried out by moving or sliding the picture elements, by user specified parameters, along the image coordinate directions. If c and d represent the translation parameters along respective x - and y -directions then the this transformation results in moving the picture elements located at image coordinates (x_i, y_i) to

the new position (x_2, y_2) such that the following relationship holds.

$$\begin{cases} x_2 = x_1 + c \\ y_2 = y_1 + d \end{cases} \quad (10)$$

And in matrix form this relation can be expressed as:

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} + \begin{bmatrix} c \\ d \end{bmatrix} \quad (11)$$

Since due to translation operation (along certain direction) picture elements near the image borders may move out of the image dimensions (such as described above for the rotation operation), therefore different implementations can be realized for the purpose. For example, either the displaced out image points may simply be ignored while filling the new empty locations with black pixels, as or wrap around the result on the visible space. An illustrative example of this operation is presented in Figure 2(c).

Flipping

The flipping operation maps the coordinates (x_1, y_1) of the input image to the new position $(x_1, -y_1)$ of an output image, if the flipping operation is performed in y direction. Thus the new coordinates can be described as:

$$\begin{cases} x_2 = x_1 \\ y_2 = -y_1 \end{cases} \quad (12)$$

In this case the relationship in the matrix form becomes:

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \quad (13)$$

Mixed Transformations

As described earlier, geometric transformations can also be implemented as a combination of some basic transforms: such as rotation + scaling, scaling + flipping, flipping + rotation, etc. Here below we present examples for some the composite transformation operations. For example, if (a, b) represent the scaling parameters for respective x and y directions and θ is the angle of rotation (anti-clockwise) then the relationship for the composite operation of rotation performed after the scaling can be written as:

$$\begin{cases} x_2 = x_1 a \cos \theta - y_1 b \sin \theta \\ y_2 = x_1 a \sin \theta + y_1 b \cos \theta \end{cases} \quad (14)$$

And in matrix notation we get:

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} a \cos \theta & -b \sin \theta \\ a \sin \theta & b \cos \theta \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \quad (15)$$

Similarly, for the operation of scaling with (a, b) and then translation by (c, d) , we can write:

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} + \begin{bmatrix} c \\ d \end{bmatrix} \quad (16)$$

In the same way, the relationships for other composite operations can also be easily derived.

Scale-Invariant Feature Transform

Scale-invariant feature transform (SIFT) was introduced by Lowe (1999), and is an algorithm to detect and describe local features in images. SIFT features are local and highly distinctive, and exhibit a number of interesting properties. For example, SIFT features are invariant to image scale and rotation; robust to changes in illumination, noise, and minor changes in viewpoint;

relatively easy to extract and match for a (large) database of local features; and correct detection with high repeatability. Object description by set of SIFT features is also robust to partial occlusion since as few as 3 SIFT features from an object may be enough to compute its location and pose. And more importantly, for small databases, the recognition task can be performed in close-to-real time without any special software or hardware requirements. The SIFT algorithm takes an image and transforms it into a collection of local feature vectors which are supposed to be distinctive with above mentioned properties. SIFT keypoints are extracted through a cascade filtering approach (Lowe, 2004) and four steps are necessary for SIFT feature extraction. These steps include: 1) scale-space extrema detection (through difference-of-Gaussian (DoG) function); 2) accurate keypoint localization (by eliminating low-contrast points and points that are poorly localized along edges); 3) orientation assignment (based on local image properties); 4) SIFT descriptor generation. The brief description of these processes is as follows.

Scale-Space Extrema Detection

The first stage is to construct a Gaussian scale space function from the input image. In this stage the interest points, which are called keypoints in the SIFT framework, are detected. For this purpose the original image $I(x, y)$ is successively convolved with the Gaussian filters at different scales, as shown in the Figure 3(a), and then the difference of successive Gaussian-blurred images (the difference-of-Gaussian (DoG), $D(x, y, \sigma)$) are computed as below.

$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma) \quad (17)$$

where $L(x, y, k\sigma)$ is the result of convolving the original image $I(x, y)$ with the Gaussian blur $G(x, y, k\sigma)$ at scale $k\sigma$. i.e.,

$$L(x, y, k\sigma) = G(x, y, k\sigma) * I(x, y) \quad (18)$$

In order to detect the local maxima and minima, each sample point in DoG image is compared with its eight neighbors in the current image and nine neighbors in the scale above and below, as shown in Figure 3(b). It is selected only if it is larger or smaller than all of these neighbors.

Keypoint Localization

Scale-space extrema detection produces too many keypoint candidates, some of which are unstable. Therefore, once a candidate keypoint has been found, a detailed fit is performed to the nearby data for location, scale, and ratio of principle curvatures, aiming at rejecting the points that have low contrast. To eliminate keypoints that are poorly localized along an edge, the principle curvature is computed from a 2×2 Hessian matrix, H , computed at the location and scale of the keypoint, as:

$$H = \begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix} \quad (19)$$

If r is the ratio between the largest magnitude eigenvalue and the smallest one, and D_{xx} , D_{xy} , and D_{yy} are the respective derivatives of the scale-space image then we check the stability of a feature point from the inequality given by:

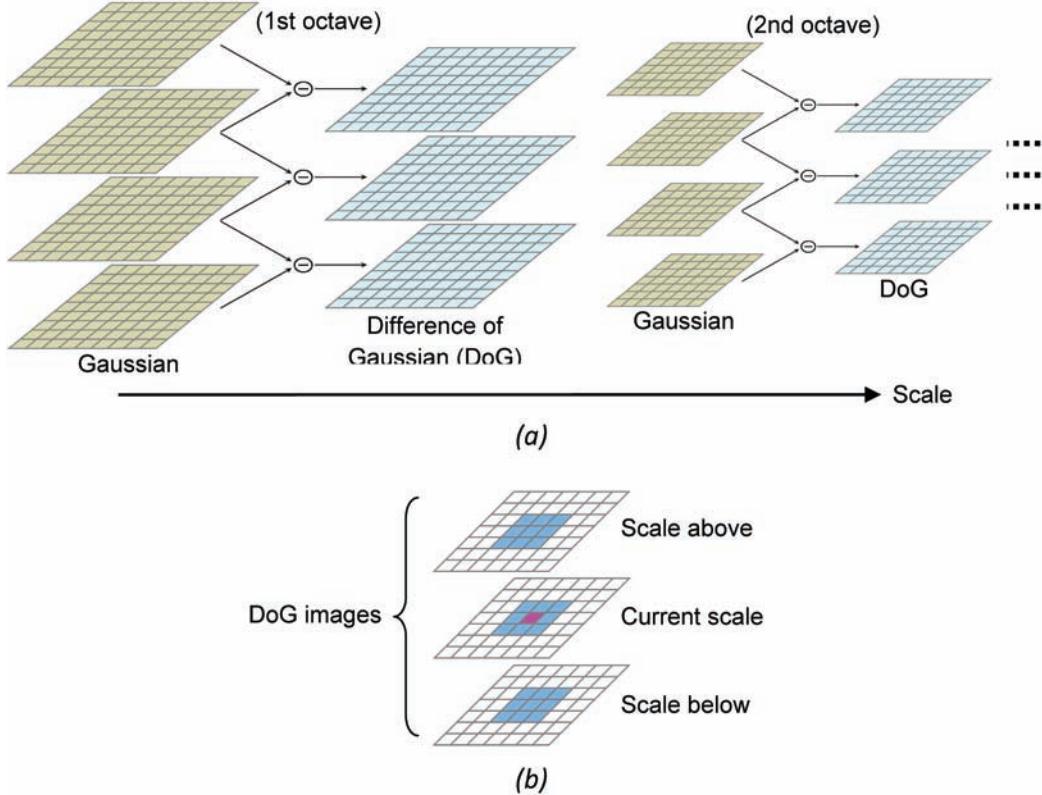
$$\frac{(D_{xx} + D_{yy})^2}{D_{xx} D_{yy} - D_{xy}^2} < \frac{(r+1)^2}{r} \quad (20)$$

If this inequality fails then the key point is rejected and removed from the candidate list.

Orientation Assignment

This step aims to assign a consistent orientation to keypoints based on the local image properties. By assigning a consistent orientation to each keypoint based on local image properties, keypoint descrip-

Figure 3. Using differences-of-Gaussian (DoG) for scale-space extrema detection and keypoint localization (a) pyramid of successive DoGs with varying scales, (b) keypoints for neighboring scales



tor can be represented relative to this orientation and therefore achieve invariance to image rotation. First, the Gaussian-smoothed image $L(x, y, \sigma)$ at the keypoint's scale σ is taken so that all computations are performed in a scale-invariant manner. For an image sample $L(x, y)$ at scale σ , the gradient magnitude, $m(x, y)$, and orientation, $\theta(x, y)$, are pre-computed using pixel differences, as:

$$m(x, y) = \sqrt{(L(x+1, y) - L(x-1, y))^2 + (L(x, y+1) - L(x, y-1))^2} \quad (21)$$

$$\theta(x, y) = \tan^{-1} \left[\frac{L(x, y+1) - L(x, y-1)}{L(x+1, y) - L(x-1, y)} \right] \quad (22)$$

The magnitude and direction calculations for the gradient are done for every pixel in a neighbor-

ing region around the keypoint in the Gaussian-blurred image L . An orientation histogram with 36 bins is formed, with each bin covering 10 degrees. Each sample in the neighboring window added to a histogram bin is weighted by its gradient magnitude and by a Gaussian-weighted circular window with a σ that is 1.5 times that of the scale of the keypoint. The peaks in this histogram correspond to dominant orientations. Once the histogram is filled, the orientations corresponding to the highest peak and local peaks that are within 80% of the highest peaks are assigned to the keypoint. In the case of multiple orientations being assigned, an additional keypoint is created having the same location and scale as the original keypoint for each additional orientation.

SIFT Descriptor Computation

In this stage, a descriptor is computed for the local image region at each candidate keypoint such that it is highly distinctive and as invariant as possible to remaining variations, such as change in illumination or 3D viewpoint. This step aims to assign a consistent orientation to the keypoints based on local image properties. As described earlier, the contribution of each pixel is weighted by the gradient magnitude and by a Gaussian with σ times the scale of the keypoint. After assigning location, scale and orientation to a keypoint, a 128-dimension keypoint descriptor for the local image region is computed. This descriptor is normalized to enhance invariance to changes in illumination and is highly distinctive. Further details of the feature point extraction procedure can be found in the main reference (Lowe, 2004).

The SIFT extracts keypoints with their location (p_1, p_2) , scale σ , and orientation θ . We adopt the extracted location and scale information to generate circular patches centered at the feature points as:

$$(x - p_1)^2 + (y - p_2)^2 = (k\sigma)^2 \quad (23)$$

where k is a magnification factor to control the radius of the patch.

Image Moments

Image moments are particular averages of either binary objects (un-weighted) or their pixel intensities (weighted). Due to their ability to represent local and global image features, the image moments have found extensive applications in the field of image processing (Teague, 1980; Teh & Chin, 1988; Lo & Don, 1989; Papademetriou, 1992; Flusser & Suk, 1993; Luo, Hamitouche, Dilenseger, & Coatrieu, 1993; Luo, Xie, & Bao, 1994; Tuceryan, 1994; Liao & Pawlak, 1996; Mukundan & Ramakrishnan, 1998). Moments are applicable to many different aspects of image

processing, ranging from invariant pattern recognition and image encoding to pose estimation. When applied to images, they describe the image content (or distribution) with respect to its axes (Shutler 2002). The moments are designed to capture both the global and detailed geometric information about the images. We use image moments to characterize the images so as to extract properties that have analogies in statistics or mechanics. In continuous form an image can be considered as a two-dimensional Cartesian density distribution function $f(x, y)$. With this assumption, the general form of a moment of order $(p+q)$, evaluated over the complete image plane ξ is:

$$M_{pq} = \int \int_x \psi_{pq}(x, y) f(x, y) dx dy \quad ; \quad p, q = 0, 1, 2, \dots, \infty \quad (24)$$

where ψ_{pq} is the *weighting kernel* or the *basis* function and produces a weighted description of $f(x, y)$ over the entire plane ξ . The basis functions may have a range of useful properties that may be passed onto the moments, producing descriptions which can be invariant under rotation, scale, translation and orientation. In order to extend this to digital images, equation (24) needs to be expressed in the discrete form. The probability density function (of a continuous distribution) is different from that of the probability of a discrete distribution. For simplicity we assume that ξ is divided into square pixels of dimensions 1×1 , with constant intensity I over each square pixel. So if P_{xy} is a discrete pixel value then:

$$P_{xy} = I(x, y) \Delta A \quad (25)$$

where ΔA is the sample or pixel area equal to one. Thus, the analysis over the entire discrete image intensity plane gives:

$$M_{pq} = \sum_x \sum_y \psi(x, y) P_{xy} \quad ; \quad p, q = 0, 1, 2, \dots, \infty \quad (26)$$

The choice of the basis function depends on the application and any desired invariant properties. The choice of basis may also introduce constraints including limiting the x and y range, or translating the description and image to polar co-ordinates (e.g. mapping it to the unit disc).

The Moment Generating Function

To describe the distribution of a random variable x the *characteristic function* can be used (Papoulis, 1992) as:

$$X(w) = \int_{-\infty}^{\infty} f(x) \exp(jwx) dx = E[\exp(jwx)] \quad (27)$$

shown here for the signal density $f(x)$, where $j = \sqrt{-1}$ and w is the spatial frequency. This is essentially the Fourier transform of the signal and has a maximum at the origin $w=0$, as $f(x)>0$.

If one dimensional continuous function $f(x)$ is the density of a positive, real valued random variable x , such that $x \in \mathbb{R}$, then a continuous exponential distribution can be defined. Replacing jw in equation (27) with s produces a real valued integral of the form:

$$M^x(s) = \int_{-\infty}^{\infty} f(x) \exp(xs) dx = E[\exp(xs)] \quad (28)$$

where $E[.]$ is the expectation and $M^x(s)$ exists as a real number. $M^x(s)$ is called the *moment generating function*, shown here for a one-dimensional distribution. It is used to characterize the distribution of an ergodic signal. Expressing the exponential in terms of an expanded Taylor series produces:

$$\exp(xs) = \sum_{n=0}^{\infty} \frac{x^n s^n}{n!} = 1 + xs + \frac{1}{2!} x^2 s^2 + \dots + R_n(x) \quad (29)$$

where $R_n(x)$ is the error term. It can be seen that the series will only converge and represent $x(s)$ completely if $R_n(x) = 0$. Therefore, if the distribution is finite in length, all values outside this length must be zero (or in terms of an image, all values outside the sampled image plane must be zero). Assuming this and substituting equation (29) into equation (28) produces:

$$\begin{aligned} M^x(s) &= \int_{-\infty}^{\infty} f(x) \exp(xs) dx \\ &= \int_{-\infty}^{\infty} 1 + xs + \frac{1}{2!} x^2 s^2 + \dots f(x) dx \\ &= 1 + sm_1 + \frac{1}{2!} s^2 m_2 + \dots, \end{aligned} \quad (30)$$

where m_n is the n th moment about the origin. By differentiating equation (28) n times with respect to s produces:

$$M_n^x(s) = E[x^n \exp(xs)] \quad (31)$$

If $M_n^x(s)$ is differentiable at zero, then the n th order moments about the origin are given by:

$$M_n^x(0) = E[x^n] = m_n \quad (32)$$

So the first three moments of this distribution are:

$$\begin{cases} M_0^x(0) = 1 \\ M_1^x(0) = x \\ M_2^x(0) = x^2 \end{cases} \quad (33)$$

If the distribution of the signal is a Gaussian, then it is completely described by its two moments, mean ($M_1^x(0)$) and variance ($M_2^x(0) - (M_1^x(0))^2$), while the total area ($M_0^x(0)$) is 1. If the joint

moment $M^{xy}(s)$ for two signals is required (i.e. a two-dimensional image) then it is noted that:

$$M^{xy}(s) = E[\exp((x + y)s)] = E[\exp(xs)\exp(ys)] \quad (34)$$

and assuming that x and y are independent, then:

$$M^{xy}(s) = E[\exp(xs)\exp(ys)] = M^x(s)M^y(s) \quad (35)$$

In conclusion, it is possible to evaluate the moments of a distribution by two methods: either by using the direct integration (equation (24)), or by use of the moment generating function (equation (28)). However, in practice the moment generating function is more widely applied to the problem of calculating moment invariants, while the direct integration method is used to calculate specific moment values.

Non-Orthogonal Moments

Hu (Hu, 1961; Hu, 1962), stated that the continuous two-dimensional $(p + q)$ th order Cartesian moment is defined in terms of Riemann integrals as:

$$m_{pq} = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} x^p y^q f(x, y) dx dy \quad (36)$$

Here it is assumed that $f(x, y)$ is a piecewise continuous, bounded function and that it can have non-zero values only in the finite region of the $x-y$ plane (i.e. all values outside the image plane are zero - see the Taylor series expansion (equation (29)) and explanation in the previous section). If this is so, then the moments of all orders exist and the following uniqueness theorem holds (Hu, 1962).

Theorem 1. (Uniqueness theorem):

The moment sequence m_{pq} (equation (36) - the basis $x^p y^q$) is uniquely defined by $f(x, y)$ and conversely, $f(x, y)$ is uniquely defined by m_{pq} . This

implies that the original image can be described and reconstructed, if sufficiently high order moments are used. By adapting equation (28) to two dimensions, the Cartesian moments (equation (36)) can be expressed in terms of the moment generating function. Analyzing a two-dimensional irradiance distribution $f(x, y)$:

$$M^{xy}(u, v) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \exp(ux + vy) f(x, y) dx dy \quad (37)$$

and expanding the exponential using Taylor series produces:

$$M^{xy}(u, v) = \sum_{p=0}^{\infty} \sum_{q=0}^{\infty} \frac{u^p}{p!} \frac{v^q}{q!} m_{pq} \quad (38)$$

where m_{pq} are the moments of this two dimensional distribution.

Cartesian Moments

The discrete version of the two dimensional Cartesian moment m_{pq} (equation (36)) for an image $f(x, y)$, by replacing the integrals with summations, is written as:

$$m_{pq} = \sum_{x=1}^M \sum_{y=1}^N x^p y^q f(x, y) \quad (39)$$

where M and N are the image dimensions, and the monomial product $x^p y^q$ is the basis function.

The zero order moment m_{00} is defined as the total mass (or power) of the image. If this is applied to a binary (i.e. a silhouette) $M \times N$ image of an object, then this is literally a pixel count of the number of pixels comprising the object, and is given by:

$$m_{00} = \sum_{x=1}^M \sum_{y=1}^N f(x, y) \quad (40)$$

The two first order moments are used to find the Centre of Mass (COM) of an image. If this is applied to a binary image and the results are then normalized with respect to the total mass (m_{00}), then the result is the centre co-ordinates of the object. Accordingly, the co-ordinates of the centre of mass are given by:

$$\bar{x} = \frac{m_{10}}{m_{00}}, \bar{y} = \frac{m_{01}}{m_{00}} \quad (41)$$

The COM describes a unique position within the field of view which can then be used to compute the centralized moments of an image.

Centralized Moments

The definition of a two dimensional discrete centralized moment (μ_{pq}) as described by Hu is (Hu, 1962):

$$\mu_{pq} = \sum_{x=1}^M \sum_{y=1}^N (x - \bar{x})^p (y - \bar{y})^q f(x, y) \quad (42)$$

This is essentially a translated Cartesian moment, which means that the centralized moments are invariant under translation. To enable invariance to scale, two dimensional scale-normalized centralized moments (η_{pq}) are used (Wood, 1996), which can be written as:

$$\eta_{pq} = \frac{\mu_{pq}}{\mu_0^\gamma} \quad (43)$$

where

$$\gamma = \frac{p+q}{2} + 1 \quad \forall (p+q) \geq 2 \quad (44)$$

Image Reconstruction

Having described an image by a set of moments, it may prove useful to investigate which moments give rise to which characteristics of the image, or vice versa. This can be achieved by reconstructing the original image from the calculated moments. Moment reconstruction, for moments with orthogonal basis functions (such as Legendre, Zernike, Chebyshev moments, etc.) has been developed extensively, (Pawlak, 1992; Prokop & Reeves, 1992; Teague, 1980; Teh & Chin, 1988). Although non-orthogonal transform methods exist, where the basis set is non-orthogonal (such as Cartesian and centralized moments), one method of moment matching for non-orthogonal moment reconstruction has appeared in (Teague, 1980). The method is based upon creating a continuous function that has identical moments to that of the original function. In this section it has been applied first to Cartesian moments and then to the centralized moments. It must be noted that in applying the theory to sampled images, the continuous conditions are replaced by discrete versions, reducing the accuracy of the final function.

Assuming that all moments M_{pq} of a function $f(x, y)$ and of order $N = (p+q)$ are known from zero through to order N_{\max} , it is then possible to obtain the continuous function $g(x, y)$ whose moments match those of the original function $f(x, y)$, up to order N_{\max} . With reference to the Taylor series expansion in equation (29), and assuming that the given continuous function can be defined as:

$$g(x, y) = g_{00} + g_{10}x + g_{01}y + g_{20}x^2 + g_{11}xy + \dots + g_{pq}x^p y^q \quad (45)$$

which reduces to:

$$g(x, y) = \sum_{p=0}^{N_{\max}} \sum_{q=0}^{N_{\max}} g_{pq} x^p y^q; \quad N_{\max} = p + q \quad (46)$$

then the constant coefficients g_{pq} are calculated so that the moments of $g(x, y)$ match those of $f(x, y)$, assuming that the image is a continuous function bounded by:

$$x \in [-1, 1], y \in [-1, 1] \quad (47)$$

These limits can be achieved by normalizing the pixel range over which the Cartesian moments are calculated, thus:

$$\int_{-1}^1 \int_{-1}^1 g(x, y) x^p y^q dx dy \equiv M_{pq} \quad (48)$$

Substituting equation (45) into equation (48) and then solving the integration produces a set of Linear Equations (LE), the number of which is determined by the order $(p + q)$ of reconstruction. These can then be solved for the coefficients g_{pq} (in terms of the moments M_{pq}) by using matrix inversion. For order three ($(p + q) \leq 3$), the LEs in matrix form are:

$$\begin{bmatrix} 1 & 1/3 & 1/3 \\ 1/3 & 1/5 & 1/9 \\ 1/3 & 1/9 & 1/5 \end{bmatrix} \begin{bmatrix} g_{00} \\ g_{20} \\ g_{02} \end{bmatrix} = \frac{1}{4} \begin{bmatrix} M_{00} \\ M_{20} \\ M_{02} \end{bmatrix} \quad (49)$$

$$\begin{bmatrix} 1/3 & 1/5 & 1/9 \\ 1/5 & 1/7 & 1/15 \\ 1/9 & 1/15 & 1/15 \end{bmatrix} \begin{bmatrix} g_{10} \\ g_{30} \\ g_{12} \end{bmatrix} = \frac{1}{4} \begin{bmatrix} M_{10} \\ M_{30} \\ M_{12} \end{bmatrix} \quad (50)$$

$$\begin{bmatrix} 1/3 & 1/5 & 1/9 \\ 1/5 & 1/7 & 1/15 \\ 1/9 & 1/15 & 1/15 \end{bmatrix} \begin{bmatrix} g_{01} \\ g_{03} \\ g_{21} \end{bmatrix} = \frac{1}{4} \begin{bmatrix} M_{01} \\ M_{03} \\ M_{21} \end{bmatrix} \quad (51)$$

and finally:

$$g_{11} = \frac{9}{4} M_{11} \quad (52)$$

Applying matrix inversion to the first matrix, equation (49) produces:

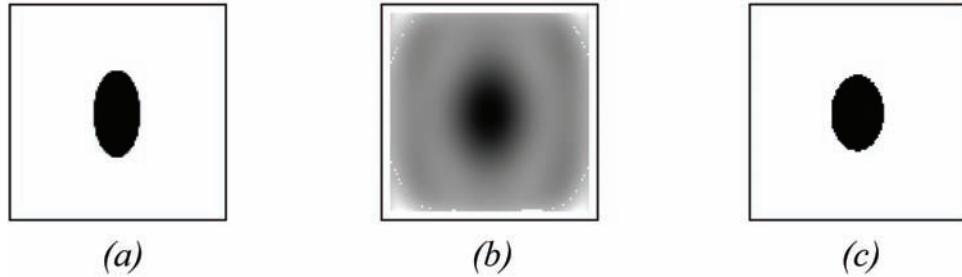
$$\begin{bmatrix} 14 & -15 & -15 \\ -15 & 45 & 0 \\ -15 & 0 & 45 \end{bmatrix} \begin{bmatrix} M_{00} \\ M_{20} \\ M_{02} \end{bmatrix} = \frac{1}{16} \begin{bmatrix} g_{00} \\ g_{20} \\ g_{02} \end{bmatrix} \quad (53)$$

By repeating this process for all the matrices, it is possible to calculate all the coefficients. If they are then substituted back into equation (45) an expression for $g(x, y)$ is produced. This expression can then be used to reconstruct an approximation of the original image. The reconstruction function $g(x, y)$ is now represented in terms of weighted sums of the moments M_{pq} , which have been previously calculated from the original function $f(x, y)$. The resultant function $g(x, y)$ for order three is:

$$\begin{aligned} 16g(x, y) = & (14M_{00} - 15M_{20} - 15M_{02}) \\ & + (90M_{10} - 105M_{30} - 45M_{12})x \\ & + (90M_{01} - 105M_{03} - 45M_{21})y \\ & + (-15M_{00} + 45M_{20})x^2 + 36M_{11}xy \\ & + (-15M_{00} + 45M_{02})y^2 + (-105M_{10} + 175M_{30})x^3 \\ & + (-45M_{01} + 135M_{21})x^2y + (-45M_{10} + 135M_{12})xy^2 \\ & + (-105M_{01} + 175M_{03})y^3 \end{aligned} \quad (54)$$

Example 1 (Reconstruction of a binary ellipse image using Cartesian moments of order 8) Let us implement the above method to order $(p + q) = 8$ for reconstructing a binary ellipse image, as shown in Figure 4. The reconstruction of (a) using Cartesian moments of order 8 produces

Figure 4. Cartesian reconstruction of an image using moments of order 8: (a) the original ellipse image, (b) the reconstructed image as a continuous function, and (c) thresholded reconstruction



recognizable results, as shown in (b). Because of using a limited number of moments in the reconstruction process the shape of the image borders appear unclear. However, they appear when the reconstructed image is thresholded, as shown in (c). Here the level of the applied threshold was adjusted by visual comparison with the original image. Due to the nature of the continuous function, the final shape is dependent on the threshold level, as clearly seen from (a) and (c).

Example 2 (Reconstruction of a binary rectangle image using Cartesian moments of order 8)
The same analysis, as presented in example 1, is repeated here for the rectangle shown in Figure 5. The corners of the rectangle in (c) are missing. The corners represent the high frequency content in the image, thus will be described fully by higher order moments. So the thresholded shape will converge to the original shape as the number of moments (and thus the order) increases. Similarly for more complex shapes, higher accuracy ($p + q \gg 8$) is needed. This is analogous to the high frequency information needed to reconstruct pulsed time domain waveforms, using methods like Fourier series. As the order (and accuracy) increases, so does the number of LEs that need to be solved (reconstruction for order eight resulted in forty five LEs). Further, if it was required to increase the order of reconstruction (using equation (54)), then all coefficients need to be re-calculated. This is due to the correlated nature of the Cartesian moments; each moment does not simply pro-

vide its own individual contribution, (unlike the orthogonal case which will be discussed later). It is interesting to note the effects of the Gibbs phenomena (Sinha, 1991) which are more evident in the reconstructed ellipse - Figure 4(b). The Gibbs phenomena (explained in terms of Fourier series) is the inability for a continuous function to recreate a step function - no matter how many finite high order terms are used, an overshoot of the function will occur. Here discontinuous edge of the original intensity function of the ellipse (between the ellipse and the background) appears unclear in the reconstruction. While outside of the original area of the ellipse, ripples of overshoot of the continuous function are visible.

By assuming the same constraints as for Cartesian moment matching, the theory can be extended to centralized moments. The continuous function $g(x, y)$ is now defined as:

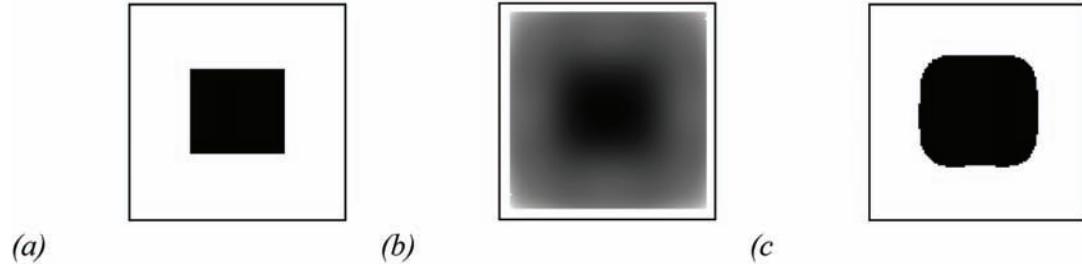
$$g(x, y) = \sum_{p=0}^{\infty} \sum_{q=0}^{\infty} g_{pq} (x - \bar{x})^p (y - \bar{y})^q; \quad N_{\max} = p + q \quad (55)$$

Similarly, equation (48) becomes:

$$\int_{-1}^1 \int_{-1}^1 g(x, y) (x - \bar{x})^p (y - \bar{y})^q dx dy \equiv M_{pq} \quad (56)$$

where \bar{x} and \bar{y} are the x and y COM's, respectively. Solving for $g(x, y)$ is then achieved in

Figure 5. Cartesian reconstruction of an image using moments of order 8: (a) the original rectangle image, (b) the reconstructed image as a continuous function, and (c) thresholded reconstruction



the same manner as already described for the Cartesian case.

Symmetry Properties

A measure of asymmetry in an image is given by its *skewness*. Here the description is the statistical measure of the distribution's degree of deviation from symmetry about the mean (Mukundan & Ramakrishnan, 1998). The third order moments (skewness and bi-correlations) will be zero if the distribution is symmetric e.g. Gaussian. The degree of skewness can be determined using the two third order moments, μ_{30} and μ_{03} . Prokop and Reeves (1992) used these moments as a basis to define the coefficients of skewness. The direction of skewness can be determined by analyzing the signs of these results.

More generally, Li (1990) described the basis function $x^p y^q$ (equation (39)), as a weighting function which extracts features of the image $f(x, y)$ concerning the symmetry in the irradiance distribution. Li (1990) used this property to show how low order ($p + q$)th normalized centralized moments (equation (43)) produce the descriptions which are directly comparable to the existence of symmetry within the image. Here the symmetry is being detected about the COM of the image, hence the use of the centralized moments. The first seven scale-normalized centralized moments ($\eta_{11}, \eta_{20}, \eta_{02}, \eta_{21}, \eta_{12}, \eta_{30}, \eta_{03}$) were analyzed using typed characters as binary input images. It was shown

that by looking at the sign and the magnitude of the centralized moments, character recognition based on symmetry properties is possible. Here follows a summary of this work. Shapes that are either symmetric about the x or y axes will produce $\eta_{11} = 0$. For shapes symmetrical about the y axis $\eta_{12} = 0$ and $\eta_{30} = 0$, Figure 6(a) and Table 1. However for shapes symmetric about the x axis, $\eta_{03} = 0$ and η_{12} is positive, Figure 6(b) and Table 1. Further to this the following generalities are true:

$$\eta_{pq} = 0 \quad \forall p = 0, 2, 4, \dots ; \quad q = 1, 3, 5, \dots \quad (57)$$

for shapes symmetric about the x axis. However shapes which are asymmetric about the x axis produce:

$$\eta_{pq} < 0 \quad \forall p = 0, 2, 4, \dots ; \quad q = 1, 3, 5, \dots \quad (58)$$

and

$$\eta_{p0} > 0, \eta_{0p} > 0 \quad \forall p = 0, 2, 4, \dots ; \quad f(x, y) > 0 \quad (59)$$

In this way it can be seen that the sign of the normalized centralized moments can be arranged to give *qualitative* information about the shape being described (i.e. the existence of symmetry), while the magnitude of the centralized moments

Figure 6. Axes of symmetry for two English characters (a) character symmetric around vertical axis, and (b) character symmetric around horizontal axis



Table 1. Scale-normalized centralized moments indicating symmetry

English Character	η_{11}	η_{20}	η_{02}	η_{21}	η_{12}	η_{30}	η_{03}
M	0	+	+	-	0	0	-
C	0	+	+	0	+	+	0

gives a *quantitative* description (i.e. their size and density).

Hu's Invariant Set

The non-orthogonal centralized moments are translation invariant and can be normalized with respect to changes in scale. However, to enable invariance to rotation they require reformulation. Hu (1962) described two different methods for producing rotation invariant moments. The first used a method called principal axes, however it was noted that this method can break down when images do not have unique principal axes. Such images are described as being rotationally symmetric. The second method Hu described is the method of absolute moment invariants and is discussed here. Hu derived these expressions from algebraic invariants applied to the moment generating function under a rotation transformation. They consist of groups of nonlinear centralized moment expressions. The result is a set of absolute orthogonal moment invariants, which can be used

for scale, position, and rotation invariant pattern identification. These were used in a simple pattern recognition experiment to successfully identify various typed characters. They are computed from normalized centralized moments up to order three and are shown below as:

$$I_1 = \eta_{20} + \eta_{02} \quad (60)$$

$$I_2 = (\eta_{20} - \eta_{02})^2 + 4(\eta_{11})^2 \quad (61)$$

$$I_3 = (\eta_{30} - 3\eta_{12})^2 + (3\eta_{21} - \eta_{03})^2 \quad (62)$$

$$I_4 = (\eta_{30} + \eta_{12})^2 + (\eta_{21} + \eta_{03})^2 \quad (63)$$

$$I_5 = (\eta_{30} - 3\eta_{12})(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2] \quad (64)$$

$$+ (3\eta_{21} - \eta_{03})(\eta_{21} + \eta_{03})[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2] \\ I_6 = (\eta_{20} - \eta_{02})[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2 + 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03})] \quad (65)$$

Finally a skew invariant, to help distinguish mirror images, is:

$$I_7 = (3\eta_{21} - \eta_{03})(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2] \\ + (\eta_{30} - 3\eta_{12})(\eta_{21} + \eta_{03})[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2] \quad (66)$$

These moments are of finite order, therefore, unlike centralized moments they do not comprise a complete set of image descriptors (Li, 1990). However, higher order invariants can be derived (Belkasim, Shridhar, & Ahmadi, 1991; Hu, 1962). It should be noted that this method also breaks down, as with the method based on the principal axis for images which are rotationally symmetric as the seven invariant moments will be zero (Prokop & Reeves, 1992).

Orthogonal Moments

Cartesian moments, equation (36), are formed using a monomial basis set $x^p y^q$. This basis set is non-orthogonal and this property is passed onto the Cartesian moments. These monomials increase rapidly in range as the order increases, producing highly correlated descriptions. This can result in important descriptive information being contained within small differences between moments, which lead to the need for high computational precision. However, moments produced using orthogonal basis sets exist. These orthogonal moments have the advantage of needing lower precision to represent differences to the same accuracy as the monomials. The orthogonality condition simplifies the reconstruction of the original function from the generated moments. Orthogonality means mutually perpendicular. When expressed mathematically, two functions y_m and y_n are orthogonal over an interval $a \leq x \leq b$ if and only if:

$$\int_a^b y_m(x) y_n(x) dx = 0; \quad m \neq n \quad (67)$$

Here we are primarily interested in discrete images, so the integrals within the moment descriptors are replaced by summations. It is noted that a sequence of polynomials which are orthogonal with respect to integration, are also orthogonal with respect to summation (Yudell, 1975). Some well established orthogonal moments are Legendre, Zernike, and Chebyshev moments. A further discussion about discrete orthogonal polynomials, discrete orthogonal moments, and some selective discrete orthogonal moments (Chebyshev, Krawtchouk, and Hahn) will be presented later in the next sections.

Moment Noise Sensitivity

Various invariant moment schemes have proved useful in recognition and reconstruction tests (Freeman, Anderson, Beardsley, Dodge, Roth, Weissman, Yerazunis, Kage, Kyuma, Miyake,

& Tanaka, 1998; Dudani, Breeding, & McGhee, 1977; Hu, 1962; Takamatsu, Sato, & Kawarada, 1997). They have proved successful and have shown invariance properties for images containing very little or no noise. However in the presence of noise, the computed Hu invariant moments $M_{1,7}$, begin to degrade. One study (Teh & Chin, 1988) showed that higher order moments are more vulnerable to white noise, thus making their use undesirable for pattern recognition. A later study (Shen & Ip, 1998) compared the performance of the Hu's invariant moments with a set of moments based on wavelet basis functions. This study showed that when using Hu's moments, even a slight discrepancy in the image can cause considerable confusion (i.e. minor shape deformation or digitization errors) if trying to discriminate between two similar images. However, noise simulation (in terms of image analysis) is very involved, and is highly dependent on the type of noise being simulated, its distribution, how it is applied, etc. It must be noted that while studies involving noise analyses may be correct for each specific test condition, care must be taken when generalizing to alternative noise-related conditions.

The preceding sub-sections have detailed the conventional use of statistical moments – the analysis of two-dimensional images. Non-orthogonal and orthogonal descriptors have been discussed, describing moments which possess various useful properties including translation, scale and rotation invariance. We have considered both image description and reconstruction. These techniques are applied to images and describe a shape in terms of its spatial (or pixel) distribution.

ORTHOGONAL POLYNOMIALS AND DISCRETE ORTHOGONAL MOMENTS FOR DIGITAL IMAGES

A brief introduction of the discrete orthogonal polynomials and the discrete orthogonal moments

will be presented in the following sub-sections. Furthermore, details regarding representation of three different discrete polynomials (Krawtchouk polynomials, Chebyshev polynomials, and Hahn polynomials), computation of corresponding discrete orthogonal moments, and their invariant counterparts will also be presented. This will enable us to give a clear understanding about the details of computing the image moments as well as their corresponding moment invariants.

Discrete Orthogonal Polynomials and Discrete Orthogonal Moments

Before proceeding for a more detailed discussion and presenting more details, in this sub-section, we present and define some basic terms which will be useful in the next sections.

Discrete Orthogonal Polynomials

The field of orthogonal polynomials was developed in the late 19th century from a study of the continued fractions by P. L. Chebyshev and later was kept on by A.A. Markov, T.J. Stieltjes and some other mathematicians. Since then, applications have been developed in many areas of mathematics, physics, and computer science. An orthogonal polynomial sequence is an infinite sequence of real polynomials, $\{p_n(x)\} = \{p_1, p_2, p_3, \dots\}$ of one variable x (with each p_n having degree n) such that any two different polynomials in the sequence are orthogonal to each other under a particular version of the L^2 -inner product. i.e.,

$$\langle p_m, p_n \rangle = 0 \quad \forall m \neq n \quad (68)$$

In other words, a sequence of orthogonal polynomials is an orthogonal basis for the (infinite-dimensional) vector space of all polynomials, with the extra requirement that p_n has degree n . The set of discrete polynomials satisfying the orthogonality condition are said to be discrete

orthogonal polynomials. For the polynomials to be orthogonal, the orthogonality condition will be presented ahead, shortly.

Pochhammer Symbol

For $(a)_0 = 1$, and $k = 1, 2, 3, \dots$, the *Pochhammer symbol* (Koepf, 1998) is defined as:

$$(a)_k = a(a+1)\dots(a+k-1) = \frac{\Gamma(a+k)}{\Gamma(a)} \quad (69)$$

Hypergeometric Series

A *hypergeometric series* (Koepf, 1998), in the most general sense, is a power series in which the ratio of successive coefficients indexed by n is a rational function of n . A hypergeometric series is defined as:

$${}_r F_s \left(\begin{matrix} a_1, \dots, a_r \\ b_1, \dots, b_s \end{matrix} \middle| z \right) = \sum_{k=0}^{\infty} \frac{(a_1, \dots, a_r)_k z^k}{(b_1, \dots, b_s)_k k!} \quad (70)$$

where $(a_1, \dots, a_r)_k = (a_1)_k, \dots, (a_r)_k$ and $(b_1, \dots, b_s)_k = (b_1)_k, \dots, (b_s)_k$.

Orthogonality Condition

For a set of *discrete orthogonal polynomials* $\{v_n(x)\}$, $n, x = 0, 1, \dots, N$, with weight $w(x)$ and norm $\rho(n)$, we have the *orthogonality condition* (Koepf, 1998) defined as:

$$\sum_{x=0}^N w(x) v_m(x) v_n(x) = \rho(n) \delta_{mn} \quad (71)$$

Weighted Polynomials

Weighted polynomials, distinguished with an overline, are defined as:

$$\bar{v}_n(x) = \left[\frac{w(x)}{r(n)} \right]^{\frac{1}{2}} v_n(x) \quad (72)$$

And for weighted polynomials we have the orthogonality condition simplified as:

$$\sum_{x=0}^N \bar{v}_m(x) \bar{v}_n(x) = \delta_{mn} \quad (73)$$

where it is simple to prove that: $|\bar{v}_n(x)| \leq 1$.

Discrete Moments

The discrete moment of order $(m + n)$ of a two-dimensional image with intensity function $f(x, y)$ (where for the sake of simplicity $f(x, y)$ is denoted as $f(x, y)$), $x \in S_{M-1}$, $y \in S_{N-1}$, $S_k = \{0, 1, 2, \dots, k\}$ is defined as:

$$\Psi_{mn} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \Phi_{mn}(x, y) f(x, y) \quad (74)$$

where $\Phi_{mn}(x, y)$, $m \in S_{M-1}$, $n \in S_{N-1}$, are the moment kernel or basis function of the moment. Moments, due to their ability to represent local and global image features, have found extensive applications in the field of image processing (Teague, 1980; Teh & Chin, 1988; Lo & Don, 1989; Papademetriou, 1992; Flusser & Suk, 1993; Luo, Hamitouche, Dilenseger, & Coatrieux, 1993; Luo, Xie, & Bao, 1994; Tuceryan, 1994; Liao & Pawlak, 1996; Mukundan & Ramakrishnan, 1998).

Discrete Orthogonal Moments

The discrete orthogonal moments are the set of moments formed by using a specific set of discrete orthogonal polynomials as the basis function set. If the moment kernels are mutually orthogonal then we call these moments, *discrete orthogonal*

moments. In cases where the kernel is separable, we can express the kernel in two separate terms as:

$$\Phi_{mn}(x, y) = \phi_m(x) \phi_n(y) \quad (75)$$

If the basis set is complete, the image is completely characterized by the total of $M \times N$ moments.

Image Reconstruction

The image intensity function, $f(x, y)$, can be reconstructed easily by the linear combination of the set of moments, $\{\Psi_{mn}\}$, i.e.

$$f(x, y) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \Psi_{mn} \Phi_{mn}(x, y) \quad (76)$$

If the order of $\{\Psi_{mn}\}$ is limited to $m \leq m_{\max}$, $n \leq n_{\max}$, where $m_{\max} \leq M - 1$ and $n_{\max} \leq N - 1$, then $\hat{f}(x, y)$ is an approximation of $f(x, y)$ as:

$$\hat{f}(x, y) \approx \sum_{m=0}^{m_{\max}} \sum_{n=0}^{n_{\max}} \Psi_{mn} \Phi_{mn}(x, y) \quad (77)$$

The quadratic error related to this approximation is:

$$\epsilon^2(\hat{f}) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [\hat{f}(x, y) - f(x, y)]^2 \quad (78)$$

which further simplifies to:

$$\epsilon^2(\hat{f}) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x, y)]^2 - \sum_{m=0}^{m_{\max}} \sum_{n=0}^{n_{\max}} [\Psi_{mn}]^2 \quad (79)$$

If the maximum order of $\{\Psi_{mn}\}$ is restricted to $(m + n) \leq P$, where $P \leq M + N - 2$, then we have:

$$\hat{f}(x, y) \simeq \sum_{m=0}^P \sum_{n=0}^m \Psi_{m-n,n} \Phi_{m-n,n}(x, y) \quad (80)$$

and the error related to this approximation further simplifies to:

$$\epsilon^2(\hat{f}) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x, y)]^2 - \sum_{m=0}^P \sum_{n=0}^m [\Psi_{m-n,n}]^2 \quad (81)$$

Krawtchouk Polynomials, Krawtchouk Moments, and Krawtchouk Moment Invariants

Krawtchouk (or Kravchuk) polynomials are classical orthogonal polynomials (Krawtchouk, 1929) associated with the binomial distribution and were introduced by the Ukrainian mathematician Mikhail Kravchuk in 1929. In the following sub-sections the definitions of Krawtchouk and weighted Krawtchouk polynomials are first provided, followed by Krawtchouk moments and Krawtchouk moment invariants.

Krawtchouk Polynomials and Weighted Krawtchouk Polynomials

The classical Krawtchouk polynomials of the n -th order are defined as:

$$K_n(x; p, N) = \sum_{k=0}^N a_{k,n,p} x^k = {}_2F_1\left(-n, -x; -N; \frac{1}{p}\right) \quad (82)$$

where $x, n = 0, 1, 2, \dots, N, N > 0, p \in (0, 1)$, and ${}_2F_1$ is the hypergeometric function (equation (70)), defined as:

$${}_2F_1(a, b; c; z) = \sum_{k=0}^{\infty} \frac{(a)_k (b)_k}{(c)_k} \frac{z^k}{k!} \quad (83)$$

here $(a)_k$ is the Pochhammer symbol (equation (69)) given by:

$$(a)_k = a(a+1)\dots(a+k-1) = \frac{\Gamma(a+k)}{\Gamma(a)} \quad (84)$$

The set of $(N+1)$ Krawtchouk polynomials $\{K_n(x, p, N)\}$ form a complete set of discrete basis functions with weight function:

$$w(x; p, N) = \binom{N}{x} p^x (1-p)^{N-x} \quad (85)$$

and satisfies the orthogonality condition:

$$\sum_{x=0}^N w(x; p, N) K_n(x; p, N) K_m(x; p, N) = \rho(n; p, N) \delta_{nm} \quad (86)$$

where $n, m = 1, 2, \dots, N$, and

$$\rho(n; p, N) = (-1)^n \left(\frac{1-p}{p} \right)^n \frac{n!}{(-N)_n} \quad (87)$$

Examples of Krawtchouk polynomials up to the second order are:

$$K_0(x; p, N) = 1 \quad (88)$$

$$K_1(x; p, N) = 1 - \left[\frac{1}{Np} \right] x \quad (89)$$

$$K_2(x; p, N) = 1 - \left[\frac{2}{Np} + \frac{1}{N(N-1)p^2} \right] x + \left[\frac{1}{N(N-1)p^2} \right] x^2 \quad (90)$$

The conventional method of avoiding numerical fluctuations in the computations of moment and moment invariant is by means of normalization (Rothe, Susse, & Voss, 1996), say by the norm. Therefore the normalized Krawtchouk polyno-

mials with respect to the norm $\{\tilde{K}_n(x; p, N)\}$ are defined as:

$$\tilde{K}_n(x; p, N) = \frac{K_n(x; p, N)}{\sqrt{\rho(n; p, N)}} \quad (91)$$

Empirical results show that the range of values may exceed $O(5)$ for large values of N therefore the set of normalized polynomials can be further scaled with the square root of the weight to achieve numerical stability. Thus the set of weighted Krawtchouk polynomials $\{\bar{K}_n(x; p, N)\}$ can be defined as:

$$\bar{K}_n(x; p, N) = K_n(x; p, N) \sqrt{\frac{w(x; p, N)}{\rho(n; p, N)}} \quad (92)$$

such that the orthogonality condition becomes:

$$\sum_{x=0}^N \bar{K}_n(x; p, N) \bar{K}_m(x; p, N) = \delta_{nm} \quad (93)$$

Here note that the square norm of the weighted Krawtchouk polynomials is unity, and hence the values of the weighted Krawtchouk polynomials are confined within the range of $[-1, 1]$. It can be observed that as p deviates from the value of 0.5 by Δp , i.e. if $p = 0.5 + \Delta p$, the weighted Krawtchouk polynomials are approximately shifted by $N\Delta p$. The direction of shifting is dependent on the sign of Δp , with the weighted Krawtchouk polynomials shifting in the $+x$ direction when Δp is positive and vice-versa. This property is crucial in the region-of-interest feature extraction capability of Krawtchouk moments.

Krawtchouk Moments

Krawtchouk moments are the set of moments constructed by using Krawtchouk polynomials as the basis function set. The Krawtchouk moments

of order $(n+m)$ in terms of weighted Krawtchouk polynomials, for an image with intensity function, $f(x, y)$, is defined as:

$$Q_{nm} = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \bar{K}_n(x; p_1, N-1) \bar{K}_m(y; p_2, M-1) f(x, y) \quad (94)$$

To match the $N \times M$ pixel points of an image here the parameters N and M are substituted with $(N-1)$ and $(M-1)$ respectively. The Krawtchouk moment corresponding to $n=m=0$ is the weighted mass of the image. i.e.,

$$Q_{00} = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \sqrt{w(x; p_1, N-1) w(y; p_2, M-1)} f(x, y) \quad (95)$$

Image Reconstruction Using Krawtchouk Moments

By solving equations (92), (93), and (94) for $f(x, y)$, the image intensity function can be written completely in terms of the Krawtchouk moments as:

$$f(x, y) = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} Q_{nm} \bar{K}_n(x; p_1, N-1) \times \bar{K}_m(y; p_2, M-1) \quad (96)$$

i.e. the image intensity function can be represented as a series of weighted Krawtchouk polynomials weighted by the Krawtchouk moments. If the moments are limited to order $\leq P < (2N - 2)$, the series is truncated to:

$$f(x, y) = \sum_{x=0}^P \sum_{y=0}^N \varphi(n-m, m, x, y) \quad (97)$$

where if $S_N = \{0, 1, 2, \dots, N-1\}$ then

$$\varphi(k, l, x, y) = \begin{cases} Q_{nm} \bar{K}_n(x; p_1, N-1) \times \bar{K}_m(y; p_2, M-1) & k \in S_N, l \in S_M \\ 0 & \text{Otherwise} \end{cases} \quad (98)$$

It can be Observed from (94) that Krawtchouk moments are in fact the inner product of $f(x, y)$ and $\bar{K}_n(x; p_1, N - 1)\bar{K}_m(y; p_2, M - 1)$. The appropriate selection of p_1 and p_2 enables localized image feature extraction using Krawtchouk moments. From equation (81), evidently the reconstruction error reduces for each additional moment used in reconstructing the image.

Krawtchouk Moment Invariants

If the geometric moments of an image with image intensity function $f(x, y)$ is defined using discrete sum approximation (as in equation (39) and redefining the range to accommodate image dimensions), as:

$$m_{nm} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} x^n y^m f(x, y) \quad (99)$$

then the standard set of geometric moment invariants, which are independent to rotation, scaling and translation (Yap, Paramesran, & Ong, 2003) can be written as:

$$\begin{aligned} v_{nm} = m_{00}^{-\gamma} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} & [(x - \bar{x}) \cos \theta + (y - \bar{y}) \sin \theta]^n \\ & \times [(y - \bar{y}) \cos \theta - (x - \bar{x}) \sin \theta]^m f(x, y) \end{aligned} \quad (100)$$

where

$$\gamma = \frac{n+m}{2} + 1 \quad (101)$$

$$\theta = \frac{1}{2} \tan^{-1} \left[\frac{2\mu_{11}}{\mu_{10} - \mu_{02}} \right] \quad (102)$$

\bar{x}, \bar{y} are given by equation (41) and μ_{nm} are the central moments.

And then the Krawtchouk moments of $\tilde{f}(x, y) = [w(x)w(y)]^{-(1/2)} f(x, y)$ can be written in terms of geometric moment as:

$$\begin{aligned} Q_{nm} &= \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \bar{K}_n(x) \bar{K}_m(y) \tilde{f}(x, y) \\ &= [\rho(n)\rho(m)]^{-(1/2)} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} K_n(x) K_m(y) f(x, y) \\ &= [\rho(n)\rho(m)]^{-(1/2)} \sum_{i=0}^n \sum_{j=0}^m a_{i,n,p_1} a_{j,m,p_2} m_{ij} \end{aligned} \quad (103)$$

where $\{a_{k,n,p}\}$ are coefficients determined by equation (82). Hence, Q_{nm} is a linear combination of geometric moments, m_{ij} , up to order $i = n$ and $j = m$, weighted by coefficients $\{a_{k,n,p}\}$. Notice that equation (103) transforms the non-orthogonal geometric moments to form the orthogonal Krawtchouk moments, and that the normalized image according to equation (100) does not fall inside the domain of $[0, N - 1] \times [0, N - 1]$, as required by Krawtchouk moments; therefore, it is modified to

$$\begin{aligned} \tilde{v}_{nm} &= \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \frac{N^2}{2m_{00}} f(x, y) \times \left[[(x - \bar{x}) \cos \theta + (y - \bar{y}) \sin \theta] \sqrt{\frac{N^2}{2m_{00}}} + \frac{N}{2} \right]^n \\ &\quad \times \left[[(y - \bar{y}) \cos \theta - (x - \bar{x}) \sin \theta] \sqrt{\frac{N^2}{2m_{00}}} + \frac{N}{2} \right]^m \end{aligned} \quad (104)$$

which can be written in terms of $\{v_{nm}\}$ as:

$$\tilde{v}_{nm} = \sum_{p=0}^n \sum_{q=0}^m \binom{n}{p} \binom{m}{q} \left(\frac{N^2}{2} \right)^{\frac{p+q}{2}+1} \times \left(\frac{N}{2} \right)^{n+m-p-q} v_{pq} \quad (105)$$

The centroid of the image is now shifted to $((N/2), (N/2))$, and the image is scale-normalized such that $\tilde{v}_{00} = (N^2 / 2)$. The new set of moments can be formed by replacing the regular geometric

moments $\{m_{nm}\}$ by their invariant counterparts $\{\tilde{v}_{nm}\}$. From equation (103), we have:

$$\tilde{Q}_{nm} = [\rho(n)\rho(m)]^{-(1/2)} \sum_{i=0}^n \sum_{j=0}^m a_{i,n,p_1} a_{j,m,p_2} \tilde{v}_{ij} \quad (106)$$

Note that the new set of moments is rotation, scale and translation invariant. We designate this set of moments as Krawtchouk moment invariants. Some of the Krawtchouk moment invariants are:

$$\tilde{Q}_{00} = \Omega_{00} v_{00} \quad (107)$$

$$\tilde{Q}_{10} = \Omega_{10} \left[\tilde{v}_{00} - \frac{1}{(N-1)p_1} \tilde{v}_{10} \right] \quad (108)$$

$$\tilde{Q}_{01} = \Omega_{01} \left[\tilde{v}_{00} - \frac{1}{(N-1)p_2} \tilde{v}_{01} \right] \quad (109)$$

$$\tilde{Q}_{11} = \Omega_{11} \left[\tilde{v}_{00} - \frac{1}{(N-1)p_1} \tilde{v}_{10} - \frac{1}{(N-1)p_2} \tilde{v}_{01} + \frac{1}{(N-1)^2 p_1 p_2} \tilde{v}_{11} \right] \quad (110)$$

where $\Omega_{01} = [\rho(n; p_1, N-1)\rho(m; p_2, N-1)]^{-(1/2)}$. Note that the choice of $p_1 = p_2 = 0.5$ keeps the emphasis of moments at the center of the image. This is consistent with the fact that equation (104) normalizes the image and shift the centroid to the center of the $[0, N-1] \times [0, N-1]$ plane.

Tchebichef Polynomials, Tchebichef Moments, and Tchebichef Moment Invariants

Tchebichef (Chebyshev or Tschebycheff) polynomials are a sequence of orthogonal polynomials which are related to de Moivre's formula and which are easily defined recursively, like Fibonacci or

Lucas numbers. Tchebichef polynomials were named after mathematician Pafnuty Chebyshev. The following sub-sections present a little more concise discussion of Tchebichef and weighted Tchebichef polynomials, Tchebichef moments, and the Tchebichef moment invariants. While extending the similar approach (used earlier as for Krawtchouk polynomials, and Krawtchouk moments) here more details have been avoided.

Tchebichef Polynomials and Weighted Tchebichef Polynomials

The discrete Tchebichef polynomials of the n -th order are expressed as:

$$t_n(x) = (1-N)_n {}_3F_2(-n, -x, 1+n; 1, 1-N; 1) \quad (111)$$

where $x, n = 0, 1, 2, \dots, N-1$, and ${}_3F_2$ is the hypergeometric function defined by equation (70). So we can also write:

$$t_n(x) = n! \sum_{k=0}^n (-1)^{n-k} \binom{N-1-k}{n-k} \binom{n+k}{n} \binom{x}{k} \quad (112)$$

Adopting the same approach as used for Krawtchouk polynomials, the set of weighted Tchebichef polynomial $\{\tilde{t}_n(x)\}$ can be written as:

$$\tilde{t}_n(x) = \frac{t_n(x)}{\beta(n, N)} = \sum_{k=0}^n c_{k,n,N} x^k \quad (113)$$

where

$$c_{k,n,N} = (-1)^{n-k} \frac{n!}{k!} \binom{N-1-k}{n-k} \binom{n+k}{n} \quad (114)$$

Tchebichef Moments

The discrete Tchebichef moments of order $(p+q)$ of image $f(x,y)$ are defined as (using equation (99)):

$$T_{pq} = \frac{1}{\rho(p,N)\rho(q,N)} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} t_p(x)t_q(y)f(x,y) \quad (115)$$

where

$$\begin{aligned} \rho(n,N) &= \sum_{x=0}^{N-1} \{t_n(x)\}^2 = \frac{N^2(N^2-1)(N^2-2^2)...(N^2-n^2)}{2n+1} \\ &= (2n)! \binom{N+n}{2n+1} \end{aligned} \quad (116)$$

Using equations (99) and (113), the equation (115) simplifies to yield Tchebichef moments (employing weighted Tchebichef polynomials) as:

$$T_{pq} = \frac{1}{\tilde{\rho}(p,N)\tilde{\rho}(q,N)} \sum_{i=0}^p \sum_{j=o}^q c_{j,q,N} c_{i,p,N} m_{ij} \quad (117)$$

where $\beta(n,N)$ is a suitable constant independent of x (and the simplest choice is $\beta(n,N) = N^n$), and

$$\tilde{\rho}(n,N) = \frac{\rho(n,N)}{\beta(n,N)^2} = \frac{N(1-\frac{1}{N^2})(1-\frac{2^2}{N^2})...(1-\frac{n^2}{N^2})}{2n+1} \quad (118)$$

It is seen that the Tchebichef moments depend on geometric moments up to the same order. The explicit expression of Tchebichef moments in terms of geometric moments up to second order (for $\beta(n,N) = N^n$) are as follows:

$$T_{00} = \frac{m_{00}}{N^2} \quad (119)$$

$$T_{10} = \frac{6m_{10} + 3(1-N)m_{00}}{N(N^2-1)} \quad (120)$$

$$T_{01} = \frac{6m_{01} + 3(1-N)m_{00}}{N(N^2-1)} \quad (121)$$

$$T_{20} = \frac{30m_{20} + 30(1-N)m_{10} + 5(1-N)(2-N)m_{00}}{(N^2-1)(N^2-2)} \quad (122)$$

$$T_{02} = \frac{30m_{02} + 30(1-N)m_{01} + 5(1-N)(2-N)m_{00}}{(N^2-1)(N^2-2)} \quad (123)$$

$$T_{11} = \frac{36m_{11} + 18(1-N)(m_{10} + m_{01}) + 9(1-N^2)m_{00}}{(N^2-1)^2} \quad (124)$$

Image Reconstruction Using Tchebichef Moments

Using equations (113) and (117) and following the same approach as used for image reconstruction using Krawtchouk moments, the image intensity function $f(x,y)$ can also be written completely in terms of the Tchebichef moments.

Tchebichef Moment Invariants

In order to construct Tchebichef moment invariants, the center of the image $f(x,y)$ is translated to its centroid (\bar{x}, \bar{y}) , and then adopting earlier approach (using equations (100), (104), (108), and (117)), Tchebichef moment invariants are obtained as:

$$\tilde{T}_{pq} = \frac{1}{\tilde{\rho}(p,N)\tilde{\rho}(q,N)} \sum_{i=0}^p \sum_{j=o}^q c_{j,q,N} c_{i,p,N} \tilde{v}_{ij} \quad (125)$$

where \tilde{v}_{nm} can be determined using equations (104) and (105).

Hahn Polynomials, Hahn Moments, and Hahn Moment Invariants

Hahn polynomials belong to the family of orthogonal polynomials and were introduced by Hahn in 1949. Under the notion that discussion presented above is also directly applicable to Hahn polynomials (i.e., the construction of weighted orthogonal polynomials, formulation of discrete orthogonal moments, and computation of their corresponding moment invariants), following sub-sections present a very concise discussion on the topic.

Hahn Polynomials and Weighted Hahn Polynomials

Hahn polynomials of order n , for $n, x = 0, 1, \dots, N-1$ (Zhou, Shu, Zhu, Toumoulin, & Luo, 2005) are given as:

$$h_n^{(\mu, \nu)}(x, N) = (N + \nu - 1)_n (N - 1)_n \\ \times \sum_{k=0}^n (-1)^k \frac{(-n)_k (-x)_k (2N + \mu + \nu - n - 1)_k}{(N + \nu - 1)_k (N - 1)_k} \frac{1}{k!} \quad (126)$$

where $(a)_k$ is the Pochhammer symbol (equation (69)) and μ, ν ($\mu > -1, \nu > -1$) are adjustable parameters controlling the shape of polynomials. The orthogonality condition (equation (71)) for discrete Hahn polynomials can be written as:

$$\sum_{x=0}^{N-1} \rho(x) h_m^{(\mu, \nu)}(x, N) h_n^{(\mu, \nu)}(x, N) = d_n^2 \delta_{mn}, \quad 0 \leq m, n \leq N-1 \quad (127)$$

where weighting function $\rho(x)$ is given by:

$$\rho(x) = \frac{1}{\Gamma(x+1)\Gamma(x+\mu+1)\Gamma(N+\nu-x)\Gamma(N-n-x)} \quad (128)$$

and the square norm d_n^2 has the expression:

$$d_n^2 = \frac{\Gamma(2N + \mu + \nu - n)}{(2N + \mu + \nu - 2n - 1)\Gamma(N + \mu + \nu - n)} \\ \times \frac{1}{\Gamma(N + \mu - n)\Gamma(N + \nu - n)\Gamma(n + 1)\Gamma(N - n)} \quad (129)$$

Same as for Krawtchouk and Tchebichef polynomials, and to avoid numerical fluctuations in moment computation, weighted Hahn polynomials are given by:

$$\tilde{h}_n^{(m, u)}(x, N) = h_n^{(m, u)}(x, N) \sqrt{\frac{r(x)}{d_n^2}}, \quad n = 0, 1, \dots, N-1 \quad (130)$$

Hence, orthogonality condition for normalized Hahn polynomials becomes:

$$\sum_{x=0}^{N-1} \tilde{h}_m^{(\mu, \nu)}(x, N) \tilde{h}_n^{(\mu, \nu)}(x, N) = \delta_{mn}, \quad 0 \leq m, n \leq N-1 \quad (131)$$

Hahn Moments

The discrete Hahn moments of order $(m + n)$ of image $f(x, y)$ are defined as (using equation (99)):

$$H_{mn} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \tilde{h}_m^{(\mu, \nu)}(x, N) \tilde{h}_n^{(\mu, \nu)}(y, N), \quad m, n = 0, 1, \dots, N-1 \quad (132)$$

Image Reconstruction Using Hahn Moments

Equations (131) and (132) lead to the following inverse moment transform:

$$f(x, y) = \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} H_{mn} \tilde{h}_m^{(\mu, \nu)}(x, N) \tilde{h}_n^{(\mu, \nu)}(y, N) \quad (133)$$

It indicates that the image can be completely reconstructed by calculating its discrete orthogonal moments up to order $2N - 2$. This property makes the discrete orthogonal moments superior to the conventional continuous orthogonal moments.

If moments are limited to an order M , we can approximate f by \hat{f} as:

$$\hat{f}(x, y) = \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} H_{m-n, n} \tilde{h}_{m-n}^{(\mu, \nu)}(x, N) \tilde{h}_n^{(\mu, \nu)}(y, N), \quad x, y = 0, 1, \dots, N - 1 \quad (134)$$

Hahn Moment Invariants

Adopting same description, construction, and formulation (as those used above for Krawtchouk moment invariants and Tchebichef moment invariants), Hahn moment invariants can also be computed easily (left as an exercise to the reader). When using for digital images, Tchebichef moments are global descriptors (i.e., the features are extracted from the image as a whole while giving equal emphasis to all the pixels in the image) but on contrary Krawtchouk moments are local descriptors (i.e., the features are extracted from only a particular portion of the image while giving more emphasis to a certain portion or region of the image). Investigations have shown that under special conditions (i.e., specific choice of parameters) Hahn moments provide a unified understanding of both Tchebichef and Krawtchouk moments (Yap, Paramesran, & Ong, 2007). Hence a connection between the moment set of these polynomials is obvious to realize and it can be said that Tchebichef and Krawtchouk polynomials/ moments are particular cases of Hahn polynomials/ moments. A direct implication of this fact is that Hahn moments encompass all the properties of both Tchebichef and Krawtchouk polynomials/ moments. Additionally, Hahn moments also exhibit intermediate properties between the extremes set by Chebyshev and Krawtchouk moments. This makes Hahn moments a unique

set of feature descriptors, and an obvious better choice over both.

Connection of Hahn Moments with Tchebichef and Krawtchouk Moments

The weighted Hahn polynomials are related to weighted Krawtchouk and Tchebichef polynomials and hence, under special conditions, serve as the basis function for their corresponding orthogonal moments. Recently it was shown that Hahn moments provide a unified understanding of Tchebichef and Krawtchouk moments (Yap, Paramesran, & Ong, 2007) and under specific choice of parameters Hahn moments become Tchebichef moments or Krawtchouk moments.

It has also been shown that the weighted version of polynomials gives greater numerical stability (Yap, Paramesran, & Ong, 2003). Table 2 presents a summary of weighted Krawtchouk, Tchebichef, and Hahn polynomials, the weights by which the polynomials can be derived from monomials using Gram-Schmidt orthogonalization (Golub & Loan, 1996), the norms, and also the parameters available for each. Here it is to be noted that: the polynomials are used in a separable sense, i.e. one set of polynomials is used for each dimension, and for all these polynomials we have $x = 0, 1, 2, \dots, N - 1$.

The Relation between Weighted Hahn and Weighted Tchebichef Polynomials

The weighted Hahn polynomials and weighted Tchebichef polynomials are related, and if we take $\alpha = pt$ and $\beta = (1 - p)t$ (or simply let $\alpha = \beta = 0$) and let $t \rightarrow 0$, then we find that the weighted Hahn polynomials become the weighted Tchebichef polynomials. i.e.,

$$\lim_{t \rightarrow 0} \bar{h}_n(x; \alpha, \beta, N) = \bar{t}_n(x)$$

Table 2. Discrete orthogonal moments and their respective kernels, weights, norms, and parameters

Moments	Kernels	Weight, $w(x)$	Norm, $\rho(n)$	Parameters
Tchebichef Moments	$t_n(x; N) = {}_3F_2 \left(\begin{matrix} -n, -x, 1+n \\ 1, -N \end{matrix} \middle 1 \right)$	$w(x; N) = \frac{1}{N+1}$	$\rho(n; N) = \frac{(2n)!}{N+1} \binom{N+n+1}{2n+1}$	-
Krawtchouk Moments	$k_n(x; p, N) = {}_2F_1 \left(\begin{matrix} -n, -x \\ -N \end{matrix} \middle \frac{1}{p} \right)$	$w(x; p, N) = \binom{N}{x} p^x (1-p)^{N-x}$	$\rho(n; p, N) = \frac{(-1)^n n!}{(-N)_n} \left(\frac{1-p}{p} \right)^n$	$0 < p < 1$
Hahn Moments	$h_n(x; \alpha, \beta, N) = {}_3F_2 \left(\begin{matrix} -n, n+\alpha+\beta+1, -x \\ \alpha+1, -N \end{matrix} \middle 1 \right)$	$w(x; \alpha, \beta, N) = \binom{\alpha+x}{x} \binom{\beta+N-x}{N-x}$	$\rho(n; \alpha, \beta, N) = \frac{(-1)^n (n+\alpha+\beta+1)_{N+1} (\beta+1)_n n!}{(2n+\alpha+\beta+1)(\alpha+1)_n (-N)_n N!}$	$\alpha > -1 \& \beta > -1$

Proof: To prove the relationship of weighted Hahn polynomials with weighted Tchebichef polynomials let we start form Hahn polynomials, as described in Table 2. Let we set the limit $t \rightarrow 0$ under the choice $\alpha = \beta = 0$. Then it follows from Table 2 that:

$$\lim_{t \rightarrow 0} h_n(x; \alpha, \beta, N) = \lim_{t \rightarrow 0} {}_3F_2 \left(\begin{matrix} -n, n+\alpha+\beta+1, -x \\ \alpha+1, -N \end{matrix} \middle| 1 \right) = {}_3F_2 \left(\begin{matrix} -n, n+1, -x \\ 1, -N \end{matrix} \middle| 1 \right) \quad (135)$$

Similarly,

$$\lim_{t \rightarrow 0} w(x; \alpha, \beta, N) = \lim_{t \rightarrow 0} \binom{\alpha+x}{x} \binom{\beta+N-x}{N-x} = \binom{x}{x} \binom{N-x}{N-x} = 1 \quad (136)$$

and

$$\lim_{t \rightarrow 0} \rho(n; \alpha, \beta, N) = \lim_{t \rightarrow 0} \frac{(-1)^n (n+\alpha+\beta+1)_{N+1} (\beta+1)_n n!}{(2n+\alpha+\beta+1)(\alpha+1)_n (-N)_n N!}$$

$$= \frac{(-1)^n (n+1)_{N+1} (1)_n n!}{(2n+1)(1)_n (-N)_n N!}$$

$$\begin{aligned} &= \frac{(-1)^n (n+1)_{N+1} n!}{(2n+1)(-N)_n N!} \\ &= \frac{(-1)^n (n+1)_{N+1} n!}{(2n+1)(-N)_n [(-1)^n (-N)_n (N-n)!]} ; \\ &\because [N!] = (-1)^n (-N)_n (N-n)! \end{aligned}$$

this yield:

$$= \frac{(N+n+1)!}{(2n+1)(N-n)! [(-N)_n]^2}$$

and, this further simplifies as:

$$\begin{aligned} &= \frac{(2n)!(N+n+1)!}{(2n+1)!(N-n)! [(-N)_n]^2} \\ &= \frac{(2n)!}{[(-N)_n]^2} \binom{N+n+1}{2n+1} \end{aligned} \quad (137)$$

Hence, finally we can get that:

$$\lim_{t \rightarrow 0} \bar{h}_n(x; \alpha, \beta, N) = \lim_{t \rightarrow 0} \left\{ \left[\frac{w(x; \alpha, \beta, N)}{\rho(n; \alpha, \beta, N)} \right]^{\frac{1}{2}} h_n(x; \alpha, \beta, N) \right\} = \bar{t}_n(x) \quad (138)$$

This proves the required relationship.

The Relation between Weighted Hahn and Weighted Krawtchouk Polynomials

The weighted Hahn polynomials and weighted Krawtchouk polynomials are related, and if we take $\alpha = pt$ and $\beta = (1-p)t$ and let $t \rightarrow \infty$, then we find that the weighted Hahn polynomials become the weighted Krawtchouk polynomials. i.e.,

$$\lim_{t \rightarrow \infty} \bar{h}_n(x; \alpha, \beta, N) = \bar{k}_n(x; p, N)$$

Proof: To prove the relationship of weighted Hahn polynomials with weighted Krawtchouk polynomials let we start form Hahn polynomials, as described in Table 2. Let we set the limit $t \rightarrow \infty$ under the choice $\alpha = pt$ and $\beta = (1-p)t$. Then it follows from Table 2 that:

$$\begin{aligned} \lim_{t \rightarrow \infty} h_n(x; \alpha, \beta, N) &= \lim_{t \rightarrow \infty} {}_3F_2 \left(\begin{matrix} -n, n + \alpha + \beta + 1, -x \\ \alpha + 1, -N \end{matrix} \middle| 1 \right) \\ &= \lim_{t \rightarrow \infty} {}_3F_2 \left(\begin{matrix} -n, n + pt + (1-p)t + 1, -x \\ pt + 1, -N \end{matrix} \middle| 1 \right) \\ &= \lim_{t \rightarrow \infty} {}_3F_2 \left(\begin{matrix} -n, n + t + 1, -x \\ pt + 1, -N \end{matrix} \middle| 1 \right) \\ &= \lim_{t \rightarrow \infty} \sum_{k=0}^{\infty} \frac{(-n)_k (n+t+1)_k (-x)_k}{(pt+1)_k (-N)_k} \frac{(1)^k}{k!} \end{aligned}$$

As we know that:

$$\lim_{t \rightarrow \infty} \frac{1}{t^k} (a + pt)_k = p^k \quad \text{and} \quad \lim_{t \rightarrow \infty} \frac{1}{t^k} (a + t)_k = 1$$

Therefore above expression reduces to the new form as:

$$\begin{aligned} &= \lim_{t \rightarrow \infty} \sum_{k=0}^{\infty} \frac{(-n)_k \left(\frac{1}{t^k} \right) (1+n+t)_k (-x)_k \frac{(1)^k}{k!}}{\left(\frac{1}{t^k} \right) (1+pt)_k (-N)_k} \\ &= \sum_{k=0}^{\infty} \frac{(-n)_k \left[\lim_{t \rightarrow \infty} \frac{1}{t^k} (1+n+t)_k \right] (-x)_k \frac{(1)^k}{k!}}{\left[\lim_{t \rightarrow \infty} \frac{1}{t^k} (1+pt)_k \right] (-N)_k} \\ &= \sum_{k=0}^{\infty} \frac{(-n)_k (-x)_k \frac{(1)^k}{k!}}{p^k (-N)_k} = \sum_{k=0}^{\infty} \frac{(-n)_k (-x)_k}{(-N)_k} \frac{(1/p)^k}{k!} \\ &= {}_2F_1 \left(\begin{matrix} -n, -x \\ -N \end{matrix} \middle| \frac{1}{p} \right) \end{aligned} \quad (139)$$

Similarly,

$$\begin{aligned} \lim_{t \rightarrow \infty} \frac{1}{t^N} w(x; \alpha, \beta, N) &= \lim_{t \rightarrow \infty} \frac{1}{t^N} \left(\begin{matrix} pt+x \\ x \end{matrix} \right) \left(\begin{matrix} (1-p)t+N-x \\ N-x \end{matrix} \right) \\ &= \lim_{t \rightarrow \infty} \frac{1}{t^N} \frac{(pt+x)(pt+x-1)\dots(pt+x-x+1)}{x(x-1)\dots(1)} \times \\ &\quad \frac{[(1-p)t+N-x][(1-p)t+N-x-1]\dots[(1-p)t+N-x-(N-x)+1]}{(N-x)(N-x-1)\dots(1)} \\ &= \lim_{t \rightarrow \infty} \frac{(p+x/t)(p+(x-1)/t)\dots(p+(x-x+1)/t)}{x!} \times \\ &\quad \frac{[(1-p)+(N-x)/t][(1-p)+(N-x-1)/t]\dots[(1-p)+(N-x-(N-x)+1)/t]}{(N-x)!} \\ &= \frac{p^x (1-p)^{N-x}}{x!(N-x)!} \end{aligned} \quad (140)$$

and also:

$$\lim_{t \rightarrow \infty} \frac{1}{t^N} \rho(n; \alpha, \beta, N) = \lim_{t \rightarrow \infty} \frac{1}{t^N} \frac{(-1)^n (n+pt+(1-p)t+1)_{N+1} ((1-p)t+1)_n n!}{[2n+pt+(1-p)t+1] (pt+1)_n (-N)_n N!}$$

$$\begin{aligned}
 &= \lim_{t \rightarrow \infty} \frac{1}{t^N} \frac{(-1)^n (n+t+1)_{N+1} ((1-p)t+1)_n n!}{(2n+t+1)(pt+1)_n (-N)_n N!} \\
 &= \lim_{t \rightarrow \infty} \frac{(-1)^n \left(\frac{1}{t^{N+1}}\right) (n+t+1)_{N+1} \left(\frac{1}{t^n}\right) ((1-p)t+1)_n n!}{[(2n+1)/t+1] \left(\frac{1}{t^n}\right) (pt+1)_n (-N)_n N!} \\
 &= \frac{(-1)^n (1-p)^n n!}{p^n (-N)_n N!} \\
 &= \frac{(-1)^n n!}{(-N)_n N!} \left(\frac{(1-p)^n}{p^n} \right) \tag{141}
 \end{aligned}$$

Hence, finally we can get that:

$$\lim_{t \rightarrow \infty} \bar{h}_n(x; \alpha, \beta, N) = \lim_{t \rightarrow \infty} \left\{ \left[\frac{w(x; \alpha, \beta, N)}{p(n; \alpha, \beta, N)} \right]^{\frac{1}{2}} h_n(x; \alpha, \beta, N) \right\} = \bar{k}_n(x; p, N) \tag{142}$$

This proves the required relationship.

WATERMARK EMBEDDING AND DETECTION METHODOLOGY

In this section we present two proposed geometric-invariant digital image watermarking techniques which apply the source-independent watermark signals to the original images. These techniques exploit the invariant properties of images for the watermarking purposes. Since the proposed techniques rely on using certain invariant image features therefore the presented watermarking systems are robust against several geometric attacks (affine transformations), as it will be seen later in the next section.

Let \tilde{H}_{nm} and \tilde{H}_{nm}^a be the Hahn moment invariants (HMI) of the original and distorted images. Here the super-script “ a ” can be considered as

either “ r ” for rotation or “ s ” for scaling or “ t ” for translation. Let the set of Hahn moment invariants (or the Hahn moment invariant’s feature vector) of the original image and the rotated (attacked) image are respectively given by:

$$\tilde{H}_{nm} = [\tilde{H}_{00}, \tilde{H}_{01}, \tilde{H}_{10}, \dots, \tilde{H}_{N_{\max} M_{\max}}] \tag{143}$$

and

$$\tilde{H}_{nm}^a = [\tilde{H}_{00}^a, \tilde{H}_{01}^a, \tilde{H}_{10}^a, \dots, \tilde{H}_{N_{\max} M_{\max}}^a] \tag{144}$$

Next we calculate the root mean square error (rms value) between \tilde{H}_{nm} and \tilde{H}_{nm}^a , for all “ a ’s”. Let for the case of a general affine transformation, the rms value between \tilde{H}_{nm} and \tilde{H}_{nm}^a is denoted as “ E_a ”, and mathematically expressed as:

$$E_a = \left[\frac{1}{L} \sum_{i=1}^L [\tilde{H}_{nm}(i) - \tilde{H}_{nm}^a(i)]^2 \right]^{\frac{1}{2}} \tag{145}$$

where “ L ” is the length of the feature vector. Using equation (145), we can compute all the rms values for the potential operations of rotation, scaling and translation, respectively represented as: “ E_r ”, “ E_s ”, and “ E_t ”. Now we select the threshold value “ T ” as maximum among these rms values as:

$$T = \text{Max}[E_r, E_s, E_t] \tag{146}$$

Watermark Pre-Processing and Construction

As described earlier, we will choose a watermark which is statistically independent to the original image (to be watermarked). Such a watermark can be generated either randomly or a semantically meaningful pattern can also be preprocessed to achieve this property. For this purpose, and for additional security, “*toral automorphism*” with a user’s selected secret key to pre-permute the

watermark to noise, can also be used. A two dimensional toral automorphism can be considered as spatial transformation of planar regions. It scatters the image shape in some iterated operations less than a specified number of times, and will return to the original shape while it is further iterated to the specified number of times. This specified number is determined by the toral automorphism parameters and the image size. So before using the watermark for embedding, we use the toral automorphism to pre-process the watermark “ W ” and render it to a chaotic sequence “ H ”. While it is useful in meeting the needed statistical independence characteristic of the watermark, this also helps further to protect the watermark. The transfer function between H and W is given by:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod}(n)) \quad (147)$$

where (x, y) and (x', y') express the pixel locations of W and H , respectively; k denotes the control parameter; and n denotes the image size, respectively. These parameters can be used as private key during the watermark detection process. The “*Cat map*” (with $k = 1$ and $n = 1$) is a classical mixing system in dynamics.

System-I: Watermarking Method Based on Scale-Invariant Feature Transform with Bounding-Box and Discrete Orthogonal Hahn Moments

Watermark Embedding Procedure

The block diagram of the watermarking system based on a scale invariant feature transform with bounding-box and the discrete orthogonal Hahn moments is shown in Figure 7, and is described below. In this method randomly generated watermarks, of the size of selected patches are used.

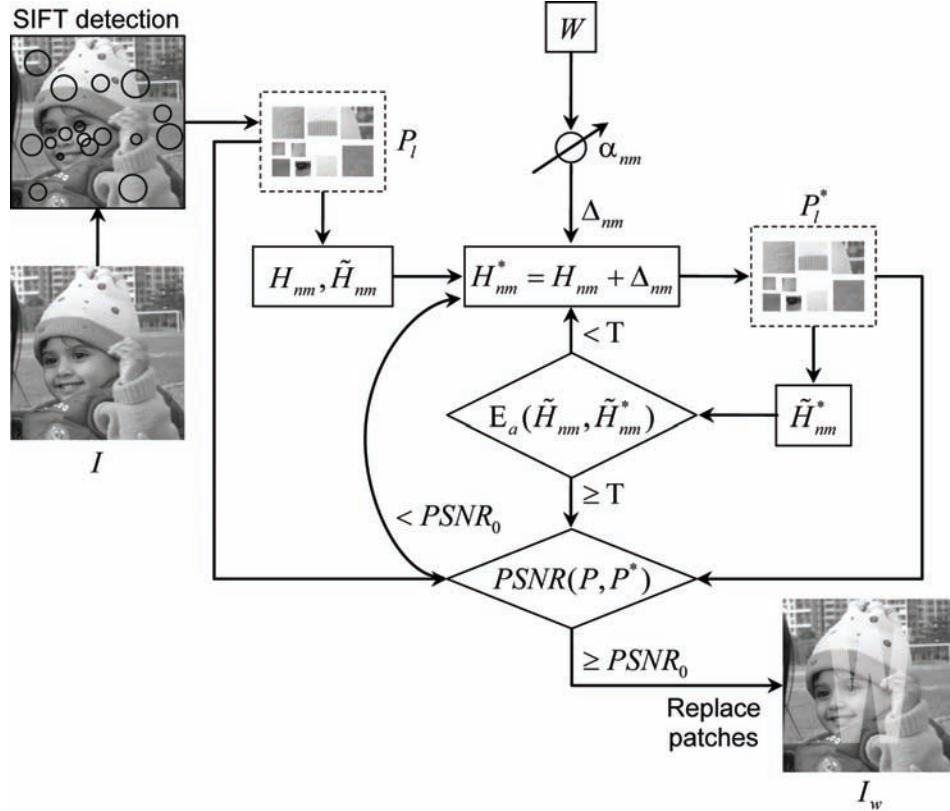
- **Step 1.** Perform the scale-invariant feature transform (SIFT) to find the keypoint parameters of location, scale, and orientation, and form circular patches centered at the feature point locations satisfying the condition given by equation (23).
- **Step 2.** Form rectangular bounding-box patches, aligned with image axes, which inscribe these circular patches.
- **Step 3.** Select “ P ” number of non-overlapping patches P_l and compute the set of Hahn moments H_{nm} for these patches up to the order say $(N_{\max}^{P_l}, M_{\max}^{P_l})$ such that the reconstruction error ϵ^2 (equation (79) between the original patch and the reconstructed patch is minimum. For these patches also calculate the Hahn moment invariants to some order ($\leq N_{\max}$) and construct Hahn moment invariant feature vector \tilde{H}_{nm} .
- **Step 4.** Modify some of the Hahn moments using the relation:

$$H_{nm}^* = H_{nm} + \Delta_{nm} \quad (148)$$

where Δ_{nm} is a suitably chosen random value with controlled strength.

- **Step 5.** Perform patch reconstruction with the modified moments to generate the set of patches P_l^* .
- **Step 6.** Compute the Hahn moment invariants of the reconstructed patches and denote the modified feature vector by \tilde{H}_{nm}^* .
- **Step 7.** Compute the rms value between \tilde{H}_{nm} and \tilde{H}_{nm}^* using equation (145).
- **Step 8.** If the value of E_a is less than a threshold (T) then repeat steps 4 to 7, otherwise go to the next step.
- **Step 9.** Check the reconstructed patches for watermark visibility by computing and comparing the peak-signal-to-noise ratio, $PSNR$, against an acceptable threshold

Figure 7. Block diagram of the watermarking method based on scale-invariant feature transform with bounding-box and the discrete orthogonal Hahn moments



- value of $PSNR_0$. If the computed $PSNR$ is less than the desirable threshold value $PSNR_0$ then repeat the steps 4 to 8 and modify the moment values, otherwise the watermark has no visible or noticeable affect and therefore the reconstructed patch set is treated as to be watermarked.
- Step 10.** Replace the original set of patches in the original image I with these watermarked patches to get the watermarked image.

Watermark Detection Procedure

The watermark detection procedure for this system uses the following steps, and is shown using the block diagram in Figure 8.

- Step 1.** Find SIFT keypoints and form circular patches centered at feature point locations satisfying the condition same as during the watermark embedding procedure.
- Step 2.** Form rectangular bounding-box patches, aligned with image axes and inscribing these patches.
- Step 3.** Select “ l ” number of non-overlapping patches P_l and compute the set of Hahn moment invariants for the given test patches (up to that order for which Hahn moment invariants are computed for the watermarked patches) and construct the set of Hahn moment invariant feature vector. Let the feature vector of the test patch is \tilde{H}_{nm}^{test} .

- **Step 4.** Compute the rms value between \tilde{H}_{nm}^{test} and the Hahn moment invariant feature vector \tilde{H}_{nm}^w of the watermarked patch, and denote it as E_{a2} .
- **Step 5.** If E_{a2} is less than the previous threshold T then the watermark is detected, otherwise watermark is not found in the test patch.
- **Step 2.** A set of low-order invariant Hahn moments $H_o = [H_{om_1,n_1}, \dots, H_{om_k,n_k}]$ and Hahn moments $H_w = [H_{wm_1,n_1}, \dots, H_{wm_k,n_k}]$ are constructed for both of the original image and the watermark.
- **Step 3.** Embed the watermark by adjusting/modifying the invariant Hahn moments of the image as given by equation (148). Now here we chose Δ_{nm} described as the function of the watermark information and with a variable watermark strength controlling parameter α_{nm} . Thus, in accordance with this explanation, now we can write equation (148) as:

$$\hat{H}_{m_i,n_i} = H_{om_i,n_i} + \alpha(m_i, n_i)H_{wm_i,n_i} \quad (149)$$

where

$$\Delta_{m_i,n_i} = \alpha(m_i, n_i)H_{wm_i,n_i} \quad (150)$$

- **Step 4.** Perform image reconstruction using the modified set of invariant Hahn moments.
- **Step 5.** Check the reconstructed image for watermark visibility by computing and comparing the peak-signal-to-noise ratio, $PSNR$, between the original image and the resulting modified image. Check $PSNR$ against an acceptable threshold value of $PSNR_0$. If the computed $PSNR$ is less than the desirable threshold value $PSNR_0$ then repeat the steps 2 to 4 and modify the moment values, otherwise the watermark has no visible or noticeable affect and therefore the reconstructed image is treated as to be watermarked.

Just as a typical example, the original image “Najia” and its watermarked version generated using this scheme are shown in Figure 10.

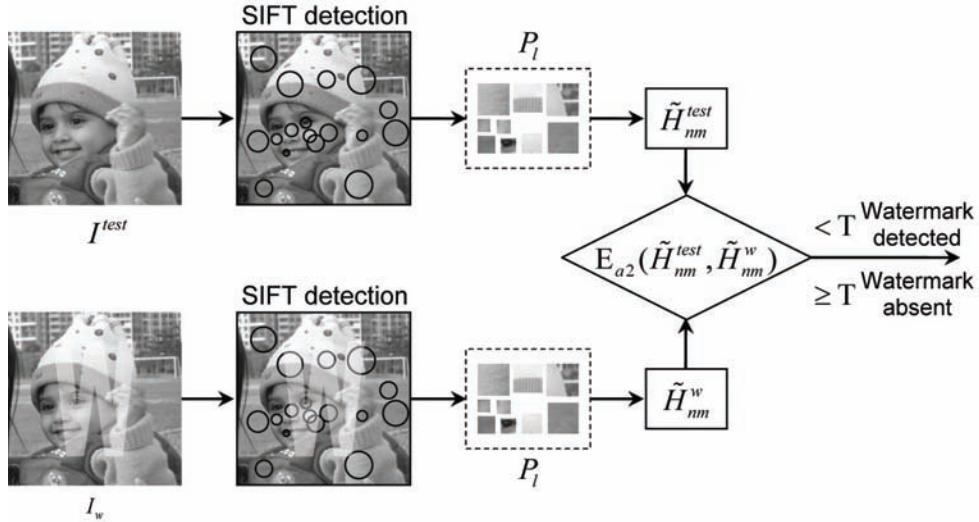
System-II: Watermarking Method Based on Discrete Orthogonal Hahn Moments

Watermark Embedding Procedure

In this system we choose a watermark signal which is equal in size to the original image and is chosen or designed to be statistically independent to the image to be watermarked. In the watermark detection procedure we adopt the blind source separation approach using independent component analysis (Yu, Sattar, & Ma, 2002). Therefore, for reliable performance of the system the statistical independence property is highly desirable. For this purpose, as described above, either we choose a randomly generated watermark signal or preprocess the semantically meaningful watermark pattern to render it random. In this system the watermark is imperceptibly embedded using the Hahn moments of the original image, and the embedding intensity is controlled according to the results of the performance analysis. The watermark embedding steps for this proposed watermarking system are described as follows, and the block diagram of the system is shown in Figure 9.

- **Step 1.** Generate a random watermark signal of the size of original image. For the case of semantically meaningful watermark, or for the purpose of additional security the watermark can be rendered random further by using the toral automorphism, as described earlier.

Figure 8. Block diagram for watermark detection method of system-I



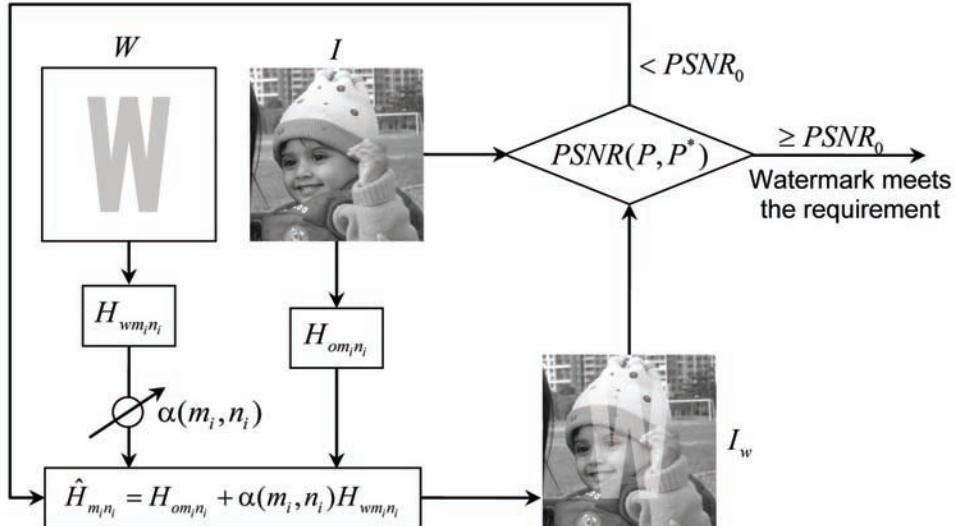
This watermarked image is generated with non-optimized watermarking parameter settings, and with Hahn moments adapted to Krawtchouk settings. Although, neither moment reconstruction nor the watermarking procedure has been adopted with the optimal settings, however it can clearly be seen that both the original and the watermarked images are very similar. Additionally, the watermark was also easily detected for several attacks. Thus, this example supports both the claims that: (a) discrete orthogonal moments (specifically Hahn moments) provide excellent image reconstruction capabilities and, (b) exploiting their moment invariant capabilities can be very useful to design the geometric distortion-invariant watermarking system. This will be further investigated and demonstrated in the results and discussion part of this chapter.

Watermark Detection Procedure

The watermark detection procedure for this system is based on the independent component analysis and uses the FASTICA algorithm (Hyvarinen, & Oja, 1999). The process for watermark extraction is described below.

- **Step 1.** First the test image is pre-processed and prepared for the detection process. The observed variable x is centered by subtracting the mean vector $m = E\{x\}$ from the observed variable; this makes x a zero-mean variable. This pre-processing method is designed to simplify the ICA algorithms. After estimating the mixing matrix A with the centered data, the estimation is completed by adding the mean vector of the original source signal back to the centered estimates of the source data. Another pre-processing method is designed to whiten the observed variables. Whitening means to transform the variable x linearly so that the new variable \tilde{x} is white, i.e., its components are uncorrelated and their variances equal unity. Whitening can be computed by eigenvalue decomposition of the covariance matrix $E\{xx^T\} = EDE^T$, where E is the orthogonal matrix of eigenvector of $E\{xx^T\}$ and D is a diagonal matrix of its eigenvalues. Note that $E\{xx^T\}$ can be estimated in a standard way from the availability of x .

Figure 9. Block diagram of the watermarking method using discrete orthogonal Hahn moments



- **Step 2.** After centering and whitening the ICA is performed to the signal to find the separation matrix L .
 - Choose an initial (e.g., random) weight vector L ; let $L^+ = E\{yG(L^T y)\} - E\{G'(L^T y)\}L$, $L = L^+ / \|L^+\|$, where, $E(\bullet)$ is the mean compute factor, $G(\bullet)$ is a non-linear function, and the following choices of $G(\bullet)$ have been proved to be very useful: $G_1(u) = \tanh(a_1 u)$, $G_2(u) = u \exp(-u^2/2)$.
 - If the difference between the iterative results is less than the threshold, that is, $|L^+ - L| < \epsilon$, it can be concluded that the process is converged and the cycle will terminate; otherwise go back to (2) until the result is converged. The threshold ϵ can be defined by the user, and $\epsilon = 10^{-6}$ is used in our experiments. If the result still is not converged after 3000 cycles, then the process will be forced to terminate and a conclusion can be drawn that there is no independent component for the corrupted watermarked

image. If there are multiple watermarks in the tested image, then the extracted watermark must be subtracted before extracting the next one.

- **Step 3:** Extract the perfect watermark by a secret key in the watermark embedding process.

In this section we have presented two different watermarking schemes which exploit the invariant feature characteristics of the images to introduce robustness in the watermarking system for a number of geometric attacks. Here it is important to mention that we utilize Hahn moments with the special settings for Tchebichef and Krawtchouk moments, already described and proved. Therefore, the explanation is quite straightforward with the choice of these moments.

RESULTS AND DISCUSSIONS

The objective of this section is to provide experimental validation of the theoretical framework

Figure 10. Original “Najia” image (a), and the watermarked image (b) created using system-II



presented earlier. Two watermarking schemes have been proposed in this chapter and one of which is blind watermarking scheme and the other is a non-blind watermarking scheme. The proposed and presented watermarking techniques utilize the invariant features of the image and the watermark is inserted into the images through modifying the set of Hahn moment invariants. In experimentations we utilized Hahn moments with the settings of Tchebichef and Krawtchouk moments, their interrelationship has also been proved, and therefore the results are also directly verifiable through the usage of any of the Tchebichef or Krawtchouk moment invariants. It was also noticed that watermarking systems showed slightly improved performance when the Hahn moments were utilized with the settings of Tchebichef moments, in contrast to using the Hahn moments with the settings of Krawtchouk moments. Perhaps this is due to the reason that: the Tchebichef movements are the global image descriptors, i.e., the features are extracted from the image as a whole and by giving equal emphasis to all pixels in the image, whereas the set of Krawtchouk moments are the set of local image descriptors, i.e., the features are extracted from only a particular portion of the image and more emphasis is given to a certain portion or region of the image.

Normalized correlation (NC) is used to express the similarity between the original watermark w and the extracted watermark w^* quantitatively and the peak-signal-to-noise ratio ($PSNR$) is used to assess the quality of the watermarked image, by finding the difference between the watermarked image $I_w(x, y)$ and the original image $I(x, y)$. Evidently the higher values of NC imply greater similarity between the extracted and the original watermarks. The definitions of the NC and $PSNR$ are given as:

$$PSNR = 10 \log \left[\frac{I_{\max}^2}{MSE} \right] = 10 \log \left[\frac{I_{\max}^2}{\frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - Iw(i, j)]^2} \right] \quad (151)$$

$$NC = \frac{\sum_{i=0}^{255} \sum_{j=0}^{255} w(i, j) w^*(i, j)}{\sum_{i=0}^{255} \sum_{j=0}^{255} (w(i, j))^2} \quad (152)$$

Now we separately analyze and the robustness of both the watermarking systems and present results for their robustness against different kinds of geometric as well as some common signal processing attacks. To implement different attacks we use the Stirmark software (Petitcolas,

2002). The three original images used in our experimentation, named Najia, HIT, and Lake, are shown in Figure 11.

Performance of the Watermarking System – I

Robustness against Signal Processing and Geometric Attacks

The experimental results for the watermarking system-I using different signal processing attacks are presented in Table 3. In the table, the values in the denominator denote the number of synchronized patches during the watermark detection and the numerator gives the number of patches from which the watermark was successfully detected. From Table 3, it can be seen that most patches can be synchronized using SIFT, and the watermark

can be detected with a higher confidence, form a significant number of patches. It can also be noted that the added noise and the median filtering had a considerable affect on the detection results.

Tables 4 to 7 present the watermark robustness results for many single as well as composite geometric attacks. These results show that the presented system is robust to these transformations. It can be noted that for scaling operation the detector's response for watermark detection is considerably degraded when the watermarked image is scaled down. This is due to the reason that down scaling of watermarked image results in permanent loss of information. The simulation results show that the proposed watermarking system-I is robust to several geometric attacks and also survive many signal processing operations. However, one drawback of this system is that this system is non-blind watermarking system

Figure 11. Test images used in watermark experimentations; (a) Najia, (b) HIT, and (c)Lake



Table 3. Robustness of the Watermarking System - I against signal processing attacks

Attack	Hahn Moments used with the settings of Tchebichef (Tcheb.) and Krawtchouk (Krawt.) moments					
	Tcheb.	Krawt.	Tcheb.	Krawt.	Tcheb.	Krawt.
JPEG 50%	5/8	7/8	7/11	8/11	10/8	8/8
JPEG 60%	6/7	5/7	7/10	6/10	7/9	7/9
JPEG 80%	5/7	5/7	6/9	5/9	6/8	5/8
Added Noise	4/8	3/8	4/8	3/8	5/7	3/7
Median filter 3×3	3/7	3/7	4/8	3/8	4/7	2/7
Images	NAJIA		HIT		Lake	

Table 4. Robustness of the Watermarking System - I against rotation attacks

Attack	Hahn Moments used with the settings of Tchebichef (Tcheb.) and Krawtchouk (Krawt.) moments					
	Tcheb.	Krawt.	Tcheb.	Krawt.	Tcheb.	Krawt.
Rotation 5°	7/8	7/8	7/11	7/11	10/12	10/12
Rotation 10°	6/7	5/7	7/12	8/12	7/9	7/9
Rotation 15°	5/7	4/7	7/10	6/10	6/8	5/8
Rotation 30°	4/8	4/8	7/11	6/11	5/7	4/7
Rotation 45°	3/7	2/7	5/10	4/10	4/7	3/7
Images	NAJIA		HIT		Lake	

Table 5. Robustness of the Watermarking System - I against scaling attacks

Attack	Hahn Moments used with the settings of Tchebichef (Tcheb.) and Krawtchouk (Krawt.) moments					
	Tcheb.	Krawt.	Tcheb.	Krawt.	Tcheb.	Krawt.
Scaling 0.3	1/3	0/3	1/3	1/3	1/3	1/3
Scaling 0.7	3/6	3/6	3/4	2/4	1/3	1/3
Scaling 0.9	4/5	4/5	7/7	7/7	5/5	5/5
Scaling 1.2	5/6	5/6	7/8	7/8	5/5	5/5
Scaling 1.5	4/5	3/5	8/11	8/11	6/7	5/7
Images	Najia		HIT		Lake	

Table 6. Robustness of the Watermarking System - I against cropping attacks

Attack	Hahn Moments used with the settings of Tchebichef (Tcheb.) and Krawtchouk (Krawt.) moments					
	Tcheb.	Krawt.	Tcheb.	Krawt.	Tcheb.	Krawt.
Cropping 5%	8/9	7/9	9/11	8/11	8/10	8/10
Cropping 10%	6/7	6/7	7/10	6/10	7/9	6/9
Cropping 25%	5/6	4/6	5/6	4/6	5/6	5/6
Cropping 50%	1/2	1/2	2/3	2/3	2/3	1/3
Images	Najia		HIT		Lake	

and the side information of the original image is used during the watermark detection procedure. In order to cope with this limitation we devised another method and presented the watermarking system-II.

Performance of the Watermarking System-II

The performance results of the watermarking system-II are presented in this section. Two main kinds of investigations performed for this system include: estimation of the geometric distortion parameters from the distorted watermarked images and the watermark robustness tests against

Table 7. Robustness of the Watermarking System - I against different composite transformation attacks; (a) rotation (R) + scaling ($S=0.8$), and (b) rotation (R) + scaling ($S=0.8$) + cropping ($C=7\%$)

Attack	Hahn Moments used with the settings of Tchebichef (Tcheb.) and Krawtchouk (Krawt.) moments					
	Tcheb.	Krawt.	Tcheb.	Krawt.	Tcheb.	Krawt.
$R=3^\circ + S$	5/7	5/7	7/9	7/9	6/8	6/8
$R=5^\circ + S$	4/6	4/6	7/9	6/9	5/7	5/7
$R=15^\circ + S$	4/8	3/8	8/11	7/11	4/5	3/5
$R=3^\circ + S + C$	4/5	4/5	6/8	5/8	7/9	6/9
$R=5^\circ + S + C$	4/5	3/5	8/9	7/9	6/8	5/8
$R=15^\circ + S + C$	3/6	3/6	7/9	6/9	3/6	2/6
Images	Najia		HIT		Lake	

Table 8. Results for the rotation angle estimation (Hahn moments with Krawtchouk settings)

Actual rotation angle	Estimated rotation angle
0.5	0.4999999879572
0.8	0.7999998973524
1.0	1.0000000000103
1.5	1.5000000000021
2.0	1.9999999999997

different kinds of attacks. This system is designed to be blind and therefore no a-prior information is required either about the watermark signal or the original image. The blind source separation approach using ICA (Yu, Sattar, & Ma, 2002) is adopted to blindly detect and extract the watermark signal form the watermarked images. For most cases, the Najia image has been used for performing the tests.

Estimation of Geometric Distortion Parameters

In this system, since the watermark is embedded by selectively modifying the discrete orthogonal Hahn moment invariants (in the Tchebichef or Krawtchouk sense) therefore when the watermarked image undergoes certain geometric operations then the parameters of the geometric

Table 9. Results of scaling parameter estimation (Hahn moments with Krawtchouk settings)

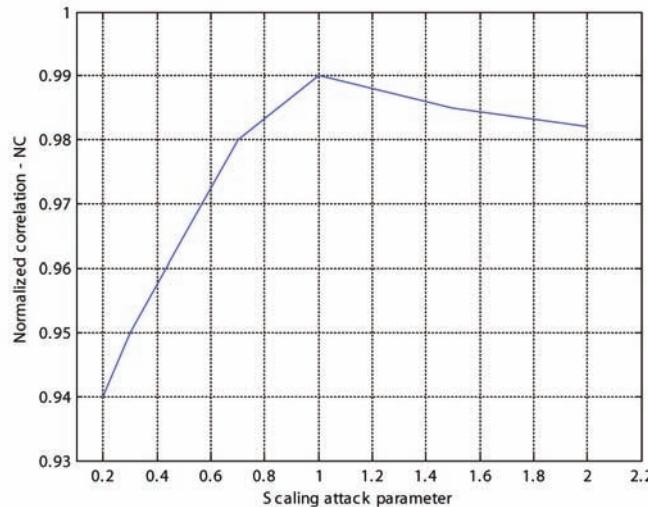
Actually applied scaling factor	Estimated scaling factor
0.5	0.4999895798722
0.75	0.750000032356
1.0	1.0000000000000
1.5	1.5000000000007
2.0	2.000000000132

distortion can be estimated by using the moment invariants. Results for the estimation of geometric distortion parameters for different kinds of distortions, by different amounts, are presented in this sub-section. It was also noticed that for very minor levels of distortions, the estimated parameters were found to be nearly the same irrespective of the fact that whether Hahn moments be used in the Tchebichef or the Krawtchouk sense. Some results of the estimated geometric distortion parameters are presented in Tables 8, 9 and 10. Parameter estimation and computation was performed from lower to an intermediate level of distortions but using a high order of precision so as to check accuracy of estimation. Furthermore, only one of the Hahn moment's settings (Tchebichef or Krawtchouk) was used for the estimation of a specific parameter, as mentioned.

Table 10. Results of translation parameter estimation (Hahn moments with Tchebichef settings)

Actually translation along x-axis	Estimated translation factor	Actually translation along x-axis	Estimated translation Factor
1	1.0000000000037	1	1.0000000000041
2	2.0000000000611	2	2.0000000000156
3	3.0000000000119	3	3.0000000000219
5	5.0000000000073	5	1.5000000000007
10	10.0000000000136	10	2.0000000000132

Figure 12. Normalized correlation values of the watermark for the image scaling attacks

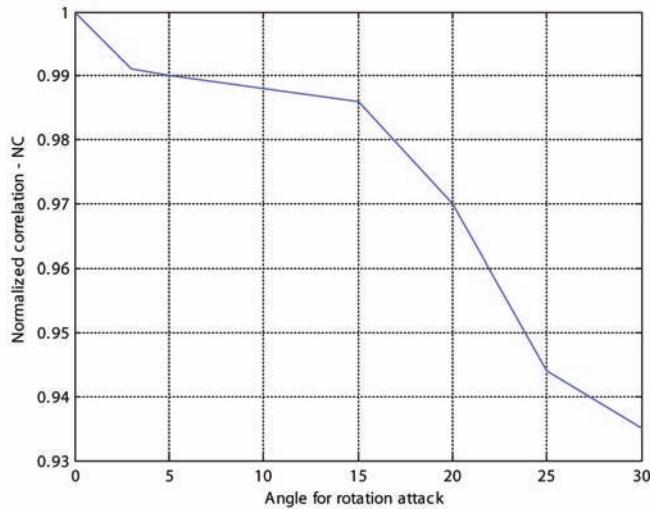


Watermark Detection Results

The watermarking system was designed to keep the peak-signal-to-noise ratio within an acceptable limit and for this purpose the acceptable PSNR threshold values were selected within the range of 39-45. Later different attacks, with varying strengths, were applied to the watermarked images and then the robustness of the system was tested. An ICA based blind watermark detector was employed for the watermark extraction and then the normalized correlation values were computed see that whether the watermark is reliably detected or not. The normalized correlation values for the extracted watermarks, for the case of different attacks are presented in this sub-section and the

results show that the proposed watermarking system is robust against many attacks. The watermark normalized correlation NC results for the scaling attacks are shown in Figure 12. The results show that the system exhibit quite good robustness against the scaling attacks. However, it is noted that the values of the normalized correlation fall abruptly for the down scaling case. This is in conformance to the reason described earlier that the image information is lost in an irrecoverable way for the down-scaling case. Similarly, Figure 13 presents the correlation result for the rotation attacks. The results demonstrate that the system show quite a good performance for up to certain levels of rotation but the normalized correlation start decreasing rapidly with large rotation angle

Figure 13. Normalized correlation values of the watermark for different rotation angles attacks



attacks. These results are presented for the Hahn moments with Krawtchouk moment settings.

FUTURE RESEARCH DIRECTIONS

Image moments and the image moment invariants are very useful tools for analyzing different properties of images, and have been used in a broad spectrum of image processing applications. Furthermore, discrete orthogonal image moments and the discrete orthogonal moment invariants exhibit very interesting and useful property that their numerical implementation involves no approximation and thus no quantization errors are involved. Therefore discrete orthogonal moments provide very accurate and exact representation of the images. In this chapter discrete orthogonal Hahn moments (with special setting for Tchebichef moments and Krawtchouk moments) have been used for the first time for watermarking purposes. Since discrete orthogonal Hahn polynomials (the basis functions of the discrete orthogonal Hahn moments) provide unified understanding of the Tchebichef and Krawtchouk polynomials and also exhibit some intermediate properties therefore the

use of Hahn moments is a better choice in several aspects. It is also assumed that using Hahn moments besides the special settings for Tchebichef or Krawtchouk moments can further reveal some more interesting and useful properties for the watermarking applications. Similarly, since several discrete orthogonal polynomials have been defined therefore further research can be performed by using other set of discrete orthogonal moments to exploit their properties, and to investigate that which set of orthogonal moments provide better performance and improved results for the watermarking applications. Furthermore, it can also be investigated that how the properties of different moments can be exploited to design more robust, reliable, and practical watermarking systems. Robustness properties against different kinds of geometric attacks are highly desirable in practical watermarking systems and some geometric distortions are really crucial to the systems. This necessitates the need of watermarking systems which can effectively survive different geometric attacks. Since different watermarking systems are vulnerable to different kind of geometric attacks and currently no available system can cope with all the attacks therefore it is still an open issue and

Table 11. Watermark robustness against compression and other different kinds of attacks

Attacks	Parameter	NC
JPEG Compression	Q = 90	0.9932
	Q = 80	0.9927
	Q = 70	0.9913
	Q = 50	0.9897
Noise addition		
Gaussian noise	$\mu = 0, \sigma = 0.2$	0.9919
	$\mu = 0, \sigma = 0.3$	0.9612
Salt and pepper	10%	0.8979
	20%	0.8832
Speckle noise	$\mu = 0, \sigma = 0.2$	0.8968
	$\mu = 0, \sigma = 0.3$	0.7546
Random distortion	---	0.9788
Skew	5%, 5%	0.9876
Row / Column removal	1, 5	0.9965
	5, 5	0.9924

there is enough room to perform research in this direction. Several studies in the image processing domain and some specifically in the watermarking area have been proved to be very useful using the discrete orthogonal image moments. Therefore it can be estimated that the further research using discrete orthogonal moments in the watermarking domain can turn out to be useful.

CONCLUSION

In this chapter two geometric-invariant digital image watermarking techniques have been proposed which apply the source-independent watermark signals to the original images. These techniques exploit the invariant properties of images for the watermarking purposes. Since the proposed techniques rely on using certain invariant image features therefore the presented watermarking systems are robust against several geometric attacks (affine transformations). The first technique utilizes the scale-invariant features and discrete

moment invariants of the images to establish a non-blind watermarking system. In this technique the watermark is applied only to some selected local image patches, instead of applying it globally to the whole image. The scale-invariant feature transform (SIFT) is used to select suitable patches from the image and then the watermark information is embedded into these selected patches. Since the original image is needed for watermark detection therefore it is a non-blind scheme. The second technique utilizes only the discrete moment invariant features of the images and the whole image is used for embedding the watermark information. For this technique no prior information of the watermark or the source image is required therefore this is a blind watermarking system. For this system, ICA is utilized by the watermark detector to blindly detect and extract the watermark signal. The watermark signal is designed to be random and independent to the original image. Discrete orthogonal Hahn moments (with the settings for Tchebichef moments and Krawtchouk moments) are used for constructing the moment invariants in both the schemes and for first time the watermark embedding process is implemented by modifying the selected Hahn invariant moments of the original image. Since Hahn moments use the discrete orthogonal Hahn polynomials as their basis function therefore they do not suffer from the numerical approximations and perfect image reconstruction is possible. It is also shown that the Hahn moments provide a unified understanding of both the Tchebichef and Krawtchouk moments, and therefore are superior to both of Tchebichef and Krawtchouk moments. The accuracy of the watermark detector depends on the secret key used in the embedding process, and the statistical independence between the original image and the watermark. Experimental results demonstrate that both of the proposed watermarking systems are robust to various geometric attacks.

ACKNOWLEDGMENT

This work is supported by “The Fifty(50) Excellent Talent Support Scheme in Basic Sciences,” Higher Education Commission (HEC), Government of Pakistan; Pakistan Atomic Energy Commission (PAEC), Pakistan; and the “New Century Excellent Talents in the Universities of China” under the grant number NCET-04-0329. The authors acknowledge all the support from the host institute “Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, P.R. China, where this work was carried out. The materialization of this work has been possible with the extended cooperation and generous editorial support from the book editor and is therefore gratefully acknowledged.

REFERENCES

- Ahlzen, L., & Song, C. (2003). *The sound blaster live! Book: A complete guide to the world's most popular sound card*. San Francisco, CA: No Starch Press, Inc.
- Ahmad, S. (2000). *Introduction to watermarking. Unpublished tutorial*. Islamabad, Pakistan: Pakistan Institute of Engineering and Applied Sciences.
- Ahmad, S. (2001). *Digital signatures and watermarking*. M.Sc. Thesis, Pakistan Institute of Engineering and Applied Sciences, Islamabad, Pakistan.
- Alghoniemy, M., & Tewfik, A. H. (2000, July/August). *Geometric distortion correction through image normalization*. Paper presented at the IEEE International Conference on Multimedia & Expo (ICME), Hilton New York & Towers New York, NY.
- Alghoniemy, M., & Tewfik, A. H. (2004). Geometric invariants in image watermarking. *IEEE Transactions on Image Processing*, 13(2), 145–153. doi:10.1109/TIP.2004.823831
- Bas, P., Chassery, J.-M., & Macq, B. (2002). Geometrically invariant watermarking using feature points. *IEEE Transactions on Image Processing*, 11(9), 1014–1028. doi:10.1109/TIP.2002.801587
- Belkasim, S. O., Shridhar, M., & Ahmadi, M. (1991). Pattern recognition with moment invariants: A comparative study and new results. *Pattern Recognition*, 24(12), 1117–1138. doi:10.1016/0031-3203(91)90140-Z
- Cox, I. J., & Linnartz, J. P. M. G. (1997). *Public watermarks and resistance to tampering*. Paper presented at the IEEE International Conference on Image Processing, Washington, DC.
- Cox, I. J., Miller, M. L., & Bloom, J. A. (2001). *Digital Watermarking*. San Mateo, CA: Morgan Kaufmann.
- Davoine, F. (2000). *Triangular meshes: A solution to resist to geometric distortions based watermark-removal softwares*. Paper presented at the European Signal Processing Conference, Tampere, Finland.
- Dong, P., Brankov, J. G., Galatsanos, N. P., & Yang, Y. (2002, September). *Geometric robust watermarking through mesh model based correction*. Paper presented at the IEEE International Conference on Image Processing, Rochester, NY.
- Dong, P., Brankov, J. G., Galatsanos, N. P., Yang, Y., & Davoine, F. (2005). Digital watermarking robust to geometric distortions. *IEEE Transactions on Image Processing*, 14(12), 2140–2150. doi:10.1109/TIP.2005.857263

- Dong, P., & Galatsanos, N. P. (2002, September). *Affine transformation resistant watermarking based on image normalization*. Paper presented at the IEEE International Conference on Image Processing, Rochester, NY.
- Dudani, S. A., Breeding, K. J., & McGhee, R. B. (1977). Aircraft identification by moment invariants. *IEEE Transactions on Computers*, C-26(1), 39–46. doi:10.1109/TC.1977.5009272
- Dugelay, J. L., & Petitolas, F. A. P. (2000). Possible counter-attacks against random geometric distortions. In P. W. Wong and E. J. Delp (Ed.), *Electronic imaging: Vol. 3971. Security and Watermarking of Multimedia Contents II* (pp. 338–345). San Jose, California: The Society for imaging science and technology (IS&T) and the international Society for optical engineering (SPIE.).
- EMC. (2009). *The digital universe*. EMC Corporation. Retrieved June 1, 2009, from http://www.emc.com-/digital_universe
- Flusser, J., & Suk, T. (1993). Pattern Recognition by affine moment invariants. *Pattern Recognition*, 26, 167–174. doi:10.1016/0031-3203(93)90098-H
- Freeman, W. T., Anderson, D. B., Beardsley, P. A., Dodge, C. N., Roth, M., Weissman, C. D., et al. (1998). Computer Vision for Interactive Computer Graphics. In *Proceedings, IEEE Computer Graphics and Applications: Special issue on Computer Graphics I/O Devices*, 18(3), 42-53. Los Alamitos, CA: IEEE Computer Society Press.
- Fridrich, J. (1999). Methods for tamper detection in digital images. In *Proc. of ACM Workshop on Multimedia and Security* (pp. 19-23). Orlando, FL: ACM
- Gantz, J., & Reinsel, D. (2009). *As the economy contracts, the digital universe expands*. IDC – Multimedia white paper, 1-10.
- Gantz, J. F., Chute, C., Manfrediz, A., Minton, S., Reinsel, D., Schlichting, W., & Toncheva, A. (2008). *The diverse and exploding digital universe*. An IDC White Paper, (pp. 1-16). Framingham, MA: IDC.
- Golub, G. H., & Loan, C. F. V. (1996). *Matrix Computations*, (3rd). Baltimore, MD: The Johns Hopkins University Press.
- Hu, M. K. (1961). Pattern recognition by moment invariants. In *Proceedings of IRE (Correspondence)*, 49, 1428–1961.
- Hu, M. K. (1962). Visual pattern recognition by moment invariants. *I.R.E. Transactions on Information Theory*, 8, 179–187. doi:10.1109/TIT.1962.1057692
- Hyvarinen, A., & Oja, E. (1999). *Independent component analysis: A tutorial*. Notes for International Joint Conference on Neural Networks, Washington, DC.
- Kang, H. I., & Delp, E. J. (2004). *An image normalization based watermarking scheme robust to general affine transformation*. Paper presented at the IEEE International Conference on Image Processing, Singapore.
- Kim, H. S., & Lee, H. K. (2003). Invariant image watermark using Zernike moments. *IEEE Transactions on Circuits System and Video Technology*, 13, 766–775. doi:10.1109/TCSVT.2003.815955
- Koepf, W. (1998). *Hypergeometric Summation - An Algorithmic Approach to Summation and Special Function Identities*. Germany: Vieweg.
- Krawtchouk, M. (1929). Sur une généralisation des polynomes d’Hermite. *C. R. Acad. Sci.*, 189(17), 620–622.

- Kutter, M. (1999). Performance improvement of spread spectrum based image watermarking schemes through M-ary modulation. In A. Pfitzmann (Ed.), *Third International Workshop on Information Hiding, Steganography: Paradigms and Examples* (LNCS Vol. 1728, pp. 238–250). Berlin: Springer.
- Kutter, M., & Petitcolas, F.A. P. (1999, January.) *A fair benchmark for image watermarking Systems*. Paper presented at the Electronic Imaging, Security and Watermarking of Multimedia Contents, Sans Jose, CA.
- Lee, C.-H., & Lee, H.-K. (2005). Geometric attack resistant watermarking in wavelet transform domain. *Optics Express*, 13, 1307–1321. doi:10.1364/OPEX.13.001307
- Lee, H.-Y., Kim, H. & Lee, H.-K. (2006). Robust image watermarking using local invariant features. *Optical Engineering*, 45(3), 037002(1-11).
- Li, B.C. (1990). *Applications of moment invariants to neurocomputing for pattern recognition*. PhD dissertation, The Pennsylvania State University, Pennsylvania.
- Liao, S. X., & Pawlak, M. (1996). On image analysis by moments. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18, 254–266. doi:10.1109/34.485554
- Lin, C. Y., Wu, M., Bloom, J. A., Cox, I. J., Miller, M., & Lui, Y. M. (2001). Rotation, scale, and translation resilient public watermarking for images. *IEEE Transactions on Image Processing*, 10(5), 767–782. doi:10.1109/83.918569
- Lowe, D. G. (1999). Object recognition from local scale-invariant features. In *Proceedings, the IEEE International Conference on Computer Vision*, (Vol. 2, pp. 1150–1157). Kerkyra, Greece: IEEE Computer Society Press.
- Lowe, D. G. (2004). Distinctive Image Features from Scale-Invariant Keypoints. *International Journal of Computer Vision*, 60(2), 91–110. doi:10.1023/B:VISI.0000029664.99615.94
- Luo, L. M., Hamitouche, C., Dilenseger, J. L., & Coatrieux, J. L. (1993). A moment-based three-dimensional edge operator. *IEEE Transactions on Bio-Medical Engineering*, 40, 693–703. doi:10.1109/10.237699
- Luo, L. M., Xie, X. H., & Bao, X. D. (1994). A modified moment-based edge operator for rectangular pixel image. *IEEE Transactions on Circuits and Systems for Video Technology*, 4, 552–554. doi:10.1109/76.340199
- Mohamed, F. K., & Abbes, R. (2007). RST robust watermarking schema based on image normalization and DCT decomposition. *Malaysian Journal of Computer Science*, 20(1), 77–90.
- Mukundan, R. (2004). Some computational aspects of discrete orthonormal moments. *IEEE Transactions on Image Processing*, 13, 1055–1059. doi:10.1109/TIP.2004.828430
- Mukundan, R., Ong, S. H., & Lee, P. A. (2001). Image analysis by Tschebycheff moments. *IEEE Transactions on Image Processing*, 10, 1357–1364. doi:10.1109/83.941859
- Mukundan, R., & Ramakrishnan, K. R. (1998). *Moment functions in image analysis - Theory and applications*. Singapore: World Scientific.
- Papademetriou, R. C. (1992, August/September). Reconstructing with moments. In *Proceedings of 11th International Conference on Pattern Recognition* (Vol. 3. Image, Speech and Signal Analysis, pp 476-480). Los Alamitos, CA: IEEE Computer Society Press.
- Papoulis, A. (1992). *Probability, random variables, and stochastic processes*. New York: McGraw-Hill.

- Paul, R. (2008). Amount of digital info – Global storage capacity. *Ars Technica*. Retrieved June 1, 2009 from <http://arstechnica.com/old/content/2008/03/study-amount-of-digital-info-global-storage-capacity.ars>
- Pawlak, M. (1992). On the reconstruction aspects of moment descriptors. *IEEE Transactions on Information Theory*, 38(6), 1698–1708. doi:10.1109/18.165444
- Pereira, S., & Pun, T. (2000). Robust template matching for affine resistant image watermarks. *IEEE Transactions on Image Processing*, 9(6), 1123–1129. doi:10.1109/83.846253
- Petitcolas, F. A. P. (2002). *StirMark 4.0*. Retrieved from <http://www.petitcolas.net/fabien/watermarking/-stirmark/index.html>
- Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1998). Attacks on copyright marking systems. In D. Aucsmith (Ed.), Second workshop on information hiding (LNCS Vol. 1525). Portland, OR: Springer.
- Prokop, R. J., & Reeves, A. P. (1992). A survey of moment-based techniques for unoccluded object representation and recognition. In *Proceedings, CVGIP: Vol. 54. Graphical models and Image Processing* (pp. 438-460). Orlando, FL: Academic Press, Inc.
- Rodríguez, M.A., & González, F.P. (2002). Analysis of pilot-based synchronization algorithms for watermarking of still images. *Signal Processing Image Communication*, 17(8), 661–633.
- Rothe, I., Susse, H., & Voss, K. (1996). The method of normalization to determine Invariants. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18(4), 366–376. doi:10.1109/34.491618
- Ruanaidh, J. J. K. O., & Pun, T. (1998). Rotation, scale, and translation invariant spread spectrum digital image watermarking. *Signal Processing*, 66, 303–317. doi:10.1016/S0165-1684(98)00012-7
- Shen, D., & Ip, H. S. (1997). Generalized affine invariant image normalization. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(5), 431–440. doi:10.1109/34.589203
- Shen, D., & Ip, H. S. (1998). Discriminative wavelet shape descriptors for recognition of 2-d patterns. *Pattern Recognition*, 32(2), 151–165. doi:10.1016/S0031-3203(98)00137-X
- Shen, D., Ip, H. S., Cheung, K. K. T., & Teoh, E. K. (1999). Symmetry detection by generalized complex (GC) moments: A close-form solution. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 21(5), 466–476. doi:10.1109/34.765657
- Shutler, J. (2002). Statistical moments. In CVonline: On-line compendium of computer vision. R. Fisher (ed.) Available: <http://homepages.inf.ed.ac.uk/rbf/CVonline/>.
- Sinha, N. K. (1991). *Linear Systems*. New York: Wiley.
- Takamatsu, R., Sato, M., & Kawarada, H. (1997). Pointing device gazing at hand based on local moments. In *Proceedings, Real-Time Imaging II* (Vol. 3028, pp. 155-163). San Jose, CA: SPIE.
- Teague, M. R. (1980). Image analysis via the general theory of moments. *Journal of the Optical Society of America*, 70, 920–930. doi:10.1364/JOSA.70.000920
- Teh, C. H., & Chin, R. T. (1988). On Image analysis by the method of moments. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 10, 485–513. doi:10.1109/34.3913

- Tuceryan, M. (1994). Moment-based texture segmentation. *Pattern Recognition Letters*, 15, 115–123. doi:10.1016/0167-8655(94)90069-8
- Voloshynovskiy, S., Pereira, S., Herrigel, A., Baumgartner, N., & Pun, T. (2000). Generalized watermark attack based on watermark estimation and perceptual remodulation. In P. W. Wong, E. J. Delp III (Ed.), Security and Watermarking of Multimedia Contents II, (Vol. 3971, Attack, pp. 445-449). San Jose: SPIE.
- Voloshynovskiy, S., Pereira, S., Pun, T., Egggers, J. J., & Su, J. K. (2001). Attacks on digital watermarks: classification, estimation-based attacks, and benchmarks. *IEEE Communications Magazine*, 8, 2–10.
- Wood, J. (1996). Invariant pattern recognition: A review. *Pattern Recognition*, 29(1), 1–17. doi:10.1016/0031-3203(95)00069-0
- Xin, Y., Liao, S., & Pawlak, M. (2004). *A multibit geometrically robust image watermark based on Zernike moments*. Paper presented at the meeting of International Conference on Pattern Recognition, Cambridge, UK.
- Xin, Y., Liao, S., & Pawlak, M. (2004b). *Geometrically robust image watermarking via pseudo-Zernike moments*. Paper presented at the IEEE Canadian Conference on Electrical and Computer Engineering, Ontario, Canada.
- Yap, P.-T., Paramesran, R., & Ong, S. H. (2003). Image Analysis by Krawtchouk Moments. *IEEE Transactions on Image Processing*, 12(11), 1367–1377. doi:10.1109/TIP.2003.818019
- Yap, P.-T., Paramesran, R., & Ong, S. H. (2007). Image Analysis Using Hahn Moments. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(11), 2057–2062. doi:10.1109/TPAMI.2007.70709
- Yu, D., Sattar, F., & Ma, K. K. (2002). Watermark detection and extraction using independent component analysis method. *EURASIP Journal on Applied Signal Processing*, 1, 92–104. doi:10.1155/S111086570200046X
- Yudell, L. L. (1975). *Mathematical functions and approximations*. New York: Academics Press Inc.
- Zheng, D., & Zhao, J. (2007). *A rotation invariant feature and image normalization based image watermarking algorithm*. Paper presented at the IEEE International Conference on Multimedia and Expo, Beijing, China.
- Zhou, J., Shu, H., Zhu, H., Toumoulin, C., & Luo, L. (2005). Image analysis by discrete orthogonal Hahn moments. In M. Kamel & A. Campilho (Eds.), *Second International Conference on Image Analysis and Recognition, Toronto, Canada*, (Vol. 3656: Image Analysis and Recognition, pp. 524-531). Berlin: Springer.
- Zhu, H., Shu, H., Liang, J., Luo, L., & Coatrieux, J.-L. (2007). Image analysis by discrete orthogonal Racah moments. *Signal Processing*, 8, 687–708. doi:10.1016/j.sigpro.2006.07.007

KEY TERMS AND DEFINITIONS

Watermarking: The process of imperceptibly embedding some extra information to a source signal such that it actually does not disturb the value of the source but can later be extracted for some special purposes.

Transformation: The process of mapping a set of input variables into a set of output variables by applying certain operation.

Affine Transformation: An affine transformation maps variables (e.g. pixel intensity values, or pixel locations in an input image) into new variables (i.e. in an output image) by applying a linear combination of translation, rotation, scaling, and/or shearing operations. It preserves collinearity

(i.e., all points lying on a line initially still lie on a line after transformation) and ratios of distances (e.g., the midpoint of a line segment remains the midpoint after transformation).

Similarity Transformation: An equivalence relation or operation that refers to a geometric similarity or to a matrix transformation resulting in a similarity, and leaves the characteristic polynomial, determinant, and trace of the matrix invariant.

Rigid Transformation: A transformation that preserves the inter-object (or inter-point) distances as well angles of an object.

Geometric Distortion: A transformation or operation which changes the inter-object (or inter-point) relationships in the plane (e.g. in an image).

Invariant: A quantity, in mathematics, is said to be invariant if its value does not change following a given operation.

Invariant Properties: Properties or the set of properties which remain the same (or do not change) after certain set of operations or transforms, are called invariant properties. For example, the area of a triangle is invariant under translation, rotation and reflection, but not under magnification. On the other hand, the interior angles of a triangle are invariant under magnification, and so are the proportionalities of the lengths of its sides.

Image Moments: Image moments are certain particular averages of either binary objects (unweighted) or the image pixel intensities (weighted) used to describe the image contents (or distribution) with respect to its axes.

Moment Generating Function: The moment generating function is the exponential generating function of the moments of the probability distribution. For any random variable, it is characterized and described by the probability distribution function of the random variable.

Orthogonal Image Moments: The image moments for which the kernel or the basis func-

tions are orthogonal and satisfy the orthogonality condition.

Pochhammer Symbol: For $(a)_0 = 1$, and $k = 1, 2, 3, \dots$, the Pochhammer symbol is defined as:

$$(a)_k = a(a+1)\dots(a+k-1) = \frac{\Gamma(a+k)}{\Gamma(a)}$$

Hypergeometric Series: A hypergeometric series, in the most general sense, is a power series in which the ratio of successive coefficients indexed by n is a rational function of n .

Orthogonality Condition: For a set of discrete orthogonal polynomials $\{v_n(x)\}$, $n, x = 0, 1, \dots, N$, with weight $w(x)$ and norm $\rho(n)$ the orthogonality condition is defined as:

$$\sum_{x=0}^N w(x)v_m(x)v_n(x) = \rho(n)d_{mn}$$

Tchebichef Moments: The moments that use Tchebichef polynomials as the kernel or the basis function.

Krawtchouk Moments: The moments that use Krawtchouk polynomials as the kernel or the basis function.

Hahn Moments: The moments that use Hahn polynomials as the kernel or the basis function.

Difference of Gaussian: The difference of Gaussians is a grayscale image enhancement algorithm and is equivalent to a band-pass filter to discards all but a handful of spatial frequencies present in the image.

Scale Invariant Feature Transform (SIFT): Scale-invariant feature transform (or SIFT) is an algorithm in computer vision to detect and describe local features in images.

Image Normalization: Image normalization refers to eliminating image variations (such as noise, illumination, or occlusion) that are related to conditions of image acquisition and are irrelevant to object identity.

Independent Component Analysis (ICA): A computational method for separating a multivariate signal into additive subcomponents supposing

the mutual statistical independence of the non-Gaussian source signals.

Blind Source/Signal Separation: The process of separating a set of signals from a set of mixed signals, without the aid of information (or with very little information) about the source signals or the mixing process.

Section 2

Video, Audio, Text, and 3D Mesh Watermarking

Chapter 5

From Watermarking to In-Band Enrichment: Theoretical and Applicative Trends

Mihai Mitrea
Institut TELECOM, France

Françoise Prêteux
Institut TELECOM, France

ABSTRACT

Fostered by the emerging Knowledge Society, the enriched media is nowadays a very challenging research topic, be it considered either from academic or from industrial perspectives. In its largest acceptation, enriched media refers to all possible associations established between some original data (video, audio, 3D, ...) and some metadata (textual, audio, video, executable codes, ...). Such a new content may be further exploited for various applications, like interactive HDTV, computer games, or data mining, for instance. This chapter is meant to bring into evidence the role watermarking techniques may play in this new applicative field. Following the watermarking philosophy, the in-band enrichment supposed that the enrichment data are inserted into the very data to be enriched. Thus, three main advantages are ensured: backward compatibility, format coherence, and virtually no network overhead. The discussion is structured on both theoretical aspects (the accurate evaluation of the watermarking capacity in several real-life scenarios) and on applications developed under the framework of the R&D contracts conducted at the ARTEMIS Department, Institut TELECOM.

1. INTRODUCTION

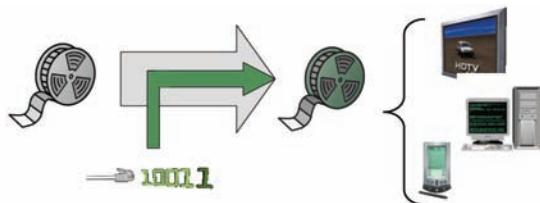
The video enrichment requires some additional (meta)data, of any type and with any syntax, to be associated with an original video content. Although very simple, this principle proves itself very powerful in practice: content customisation (digital

television, e-commerce), interactivity (games, e-learning), adaptation (intelligent broadcasting), indexing/data mining, property right assessment are just some examples of value added services it supports.

The enriched video scientific, technical and economic supports are granted by the efforts of the leading industrial players, of active SMEs, of main state institutions and of research laboratories. For

DOI: 10.4018/978-1-61520-903-3.ch005

Figure 1. In-band enrichment principle: The enrichment data are inserted into the very media to be enriched



instance, Ericsson mentioned the new services associated to the enriched video as an important component of its latest *success story* (Ericsson 2009). At the CeBIT 2008, the products presented by Thomson included enriched video functionality (Thomson 2009). IBM took the enriched video challenge as an opportunity to grant to the disabled persons non-discriminatory access to digital content (IBM 2009). The Louvre Museum in Paris showed a special interest in the new multimedia services: the already obsolete audio guides are replaced by true multimedia companions with tactile screens (Louvre 2009). The SMEs are also part of the core efforts in enriched multimedia (Wipo 2009), (Fre 2009), (Pay 2009), mainly with the large number of patents: their reaction capacity allows them to step into new roles in a continuously evolving market.

The convergence between in-band enrichment and watermarking has been brought into evidence by academic research activities (Barron, Chen & Wornell 2003), (Mitrea, Duta, Zaharia & Prêteux 2006), (Mitrea, Duta, Preda & Prêteux 2006), (IRISA 2009): following the new *in-band enriched multimedia* concept, Figure 1, the additional data are no longer conveyed through a supplementary channel, but inserted into the visual content itself. The insertion should not perceptibly alter the visual quality of the original content. Moreover, this information must be recovered even after severe alterations of the enriched video, be they

the consequence of transmission errors, malicious attacks, or application related operations.

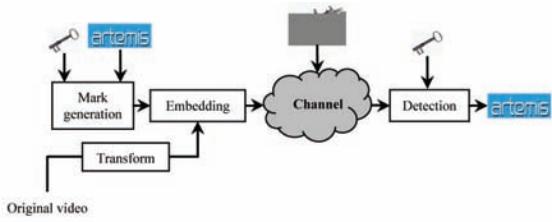
When compared to the traditional solutions, the in-band enrichment features three main advantages: virtually no-cost concerning the terminal and video representation format, a complete backward compatibility guaranteeing the co-existence of successive service generations, and virtually no network overhead. Additionally, note that the in-band enrichment may fully benefit from the theoretical watermarking framework.

Following a study devoted to the capacity of video watermarking (Mitrea & Prêteux 2009), this chapter is meant to be a guide for a user interested in deploying such solutions. In Section 2, the watermarking-inherited theoretical framework for *in-band enrichment* is sketched. Section 3 is devoted to the capacity evaluation for watermarking purposes. The related applicative instantiations are detailed and illustrated with reference values in Section 4. Note that this approach is deliberately left open: should the user be interested in some new applications, he/she can further decline the general framework so as to match his/her own purpose and to find his/her context-dependent theoretical limits. Section 5 brings more light on the impact of the difference between the real-life watermarking and its theoretical models. Section 6 discusses and demonstrates the effectiveness of the results for four enrich media content applications while Section 7 concludes the paper and opens the perspectives for future work.

2. BACKGROUND

Under the watermarking framework (Cox, Miller & Bloom 2003), (Arnold, Schmucker & Wolthusen 2003), (Davoine & Pateux 2004) the *mark* is to be *transparently* (imperceptibly) and *persistently* (robustly) associated with the media content, Figure 2. Note that while in “traditional” watermarking applications the mark is exploited for intellectual property assessment, in *in-band*

Figure 2. The watermarking model



enrichment applications the same mark represents the enrichment information.

In practice, the mark is generally encrypted with a secret key and then inserted into a certain transform (DCT - Discrete Cosine Transform, DWT – Discrete Wavelet Transform, ...) of the original content. Note that in some in-band enrichment applications, the key may be omitted (it may be no need to consider a secret parameter).

The *transparency* means that no visual differences can be identified between the original and the marked content. Such a property can be evaluated either subjectively (*i.e.* by inquiring a large panel of human observers, of different ages and with different professional backgrounds) or objectively (*i.e.* by computing different values supposed to be connected to the human visual system, as the signal to noise ratio, for instance).

The *persistence* (robustness) refers to the possibility of recovering the mark even when the marked content was deteriorated by mundane or malicious attacks (change of file format, compression, geometric attacks,...).

The *data payload* represents the amount of information (in bits) inserted into the original content. The data payload may vary from 1 bit (a simple yes/no decision) to a large quantity of information (*e.g.* a binary logo or even a colour image may be inserted into the original content). In practice, the data payload is upper limited by the trade-off to be reached between robustness and transparency.

From the *theoretical point of view*, watermarking is represented within the framework of the

information theory, Figure 2. The mark is a sample from the information source while the noise is represented by the original content (in its transformed domain) and the attacks. These two noise sources are of different types: the original content is completely known at the insertion but unknown at the detection while the attack is unknown on both insertion and detection sides. Consequently, the proper watermarking model (Cox, Miller & Bloom 2003) is a channel with non-causal side information at the embedder (Shannon 1958), (Costa 1983). Note that the watermarking channel type varies from uncompressed to MPEG-compressed video. In the former case, the DCT/DWT coefficients are real numbers, so the channel is continuous. In the latter case, the MPEG-4 AVC (ISO 2005), (Wiegand, Sullivan, Bjontegaard & Luthra 2003) watermarking peculiarities result in a discrete channel.

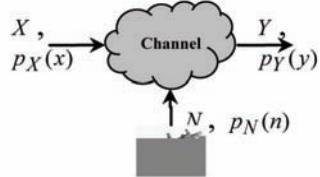
The *watermarking capacity* is the capacity of the equivalent noisy channel.

The nowadays watermarking challenge is to maximise the amount of inserted information while keeping prescribed transparency and robustness constraints (*i.e.* to reach in practice the *watermarking capacity*). Hence, the applicative issue of reaching the watermarking capacity becomes, from the theoretical point of view, an issue of evaluating the capacity of a channel with non-causal side information and of devising transmission methods reaching this limit.

The present chapter focuses on the watermarking capacity evaluation for in-band enrichment applications, *i.e.* on establishing the upper limit for the enrichment information which can be concealed in the very content to be enriched.

Note that this task is not trivial, requiring advanced tools for computing the capacity of both continuous and discrete non-causal side information channels. Or, such a problem does not have yet any generic and reliable solution. For instance, in the discrete case, the famous paper of Gel'fand & Pinsker (Gel'fand & Pinsker 1980) completely solves the problem from the theoretical point of

Figure 3. Classical channel model



view but results in an algorithm with exponential complexity, improper for the watermarking applications (see the numerical example in Section 3.2). On the contrarily, in the continuous case, several low-complexity manners of computing the side-information channel capacity exist but suspicious concerning their accuracy for watermarking arise (see Sections 3.1 and 4.1).

3. CAPACITY EVALUATION

3.1 Continuous Case

According to the results reported in (Costa 1983), an ergodic zero-memory Gaussian (continuous) noise source known at the embedder and unknown at the receiver should not decrease the channel capacity. As in watermarking applications the original content is often considered as being Gaussian distributed, the capacity can be computed by considering a classical channel (without any side information) having a unique noise source, namely the attacks. Assuming the attacks are ergodic (or, at least, stationary), the watermarking channel can be represented as in Figure 3, where X , N and Y denote the (ergodic) zero-memory input, noise and output information sources respectively, while $p_X(x)$, $p_N(n)$ and $p_Y(y)$ stand for the corresponding *pdfs* (*probability density functions*). Be $(x_1; x_2)$, $(n_1; n_2)$ and $(y_1; y_2)$ the interval on which the input, noise and output *pdfs* have non-zero values, respectively.

Shannon defined the capacity of an arbitrarily noise continuous channel by the maximum achievable value for the mutual information (Shannon 1948):

$$C = \max_{p_X(x)} I(X, Y) = \max_{p_X(x)} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} p_{XY}(x, y) \log_2 \frac{p_{XY}(x, y)}{p_X(x)p_Y(y)} dx dy \quad (1)$$

where $p_X(x)$ and $p_Y(y)$ are the same as above and $p_{XY}(x, y)$ stands for the joint input-output *pdf*.

Unfortunately, no generic and reliable computation formula has been yet established in order to analytically maximise $I(X, Y)$ over the space of all possible input *pdf*. Hence, the practice obliges to a large variety of particular cases and/or approximations.

For instance, Shannon derived the formula corresponding to a channels having additive white Gaussian noise:

$$C = W \log_2 \frac{P + N}{N}, \quad (2)$$

where W is the channel bandwidth while P and N stands for the signal (*i.e.* the mark) and noise (*i.e.* the attacks) powers, respectively. As detailed statistical investigations pointed out the watermarking attacks are not Gaussian distributed (Mitrea, Dumitru, Prêteux & Vlad 2007), equation (2) can be considered just as a comparative entity. For a non-Gaussian additive white noise, Shannon derives only some lower and upper boundaries, eq. (3):

$$W \log_2 \frac{P + N_1}{N_1} \leq C \leq W \log_2 \frac{P + N}{N_1}, \quad (3)$$

where W , and N are the same as above and N_1 denotes the noise entropy power. Unfortunately, in cases of practical relevance for watermarking,

these limits lack in accuracy (Mitrea, Dumitru, Duta, Prêteux & Vlad 2008): the relative errors are very large, sometimes approaching 100%. Consequently, two more elaborated approaches to continuous watermarking capacity computation (Dumitru, Mitrea & Prêteux 2007) are further detailed.

The Continuous Blahut–Arimoto Algorithm

The popular Blahut–Arimoto algorithm was first devoted to the discrete and finite case (Blahut 1972), (Arimoto 1972) and further extended (Chang & Davisson 2004), (Vontobel, Kavcic, Arnold & Loeliger 2008) for discrete and infinite case as well as for continuous case (Dauwels 2005), (Dauwels 2006), (Matz & Duhamel 2004).

The flowchart of the discrete Blahut–Arimoto algorithm is represented in Figure 4.

In the first iteration, the searched input $p_X^{(k=0)}(x)$ is randomly chosen (in Figure 4, a Gaussian law was considered); then it is recursively computed by using the following formula:

$$p_X^{(k+1)}(x) = \frac{p_X^{(k)}(x)}{Z^{(k)}} \exp\left(D\left(p(y/x) / p_Y^{(k)}(y)\right)\right) \quad (4)$$

where k stands for the iteration index, $D(\cdot / \cdot)$ is defined by (5) and $Z^{(k)}$ by (6):

$$D\left(p_{Y/X}(y/x) / p_Y^{(k)}(y)\right) = \int_{y_1}^{y_2} p_{Y/X}(y/x) \log_2 \left(\frac{p_{Y/X}(y/x)}{p_Y^{(k)}(y)} \right) dy \quad (5)$$

$$Z^{(k)} = \int_{x_1}^{x_2} p_X^{(k-1)}(x) \exp\left(D\left(p_{Y/X}(y/x) / p_Y^{(k)}(y)\right)\right) dx \quad (6)$$

When the difference between the $M^{(k)}$ and $I^{(k)}$ - cf. (7) and (8) - is lower than a given error ε , it

can be considered that the convergence is reached and that the capacity was computed $C = I^{(k)}$:

$$M^{(k)} = \max_{x \in [x_1, x_2]} D\left(p_{Y/X}(y/x) / p_Y^{(k)}(y)\right), \quad (7)$$

$$I^{(k)} = \int_{x_1}^{x_2} p_X^{(k)}(x) D\left(p_{Y/X}(y/x) / p_Y^{(k)}(y)\right) dx \quad (8)$$

Of course, in practice, an additional exit condition is set by the maximal number of iterations.

Gaussian Mixture-Based Capacity Evaluation (GMC)

A $\hat{p}(x)$ Gaussian mixture (Archambeau, Valle, Assenza & Verleysen 2006) is a linear decomposition of an unknown theoretical $p_X(x)$ pdf on a basis of K Gaussian laws (9):

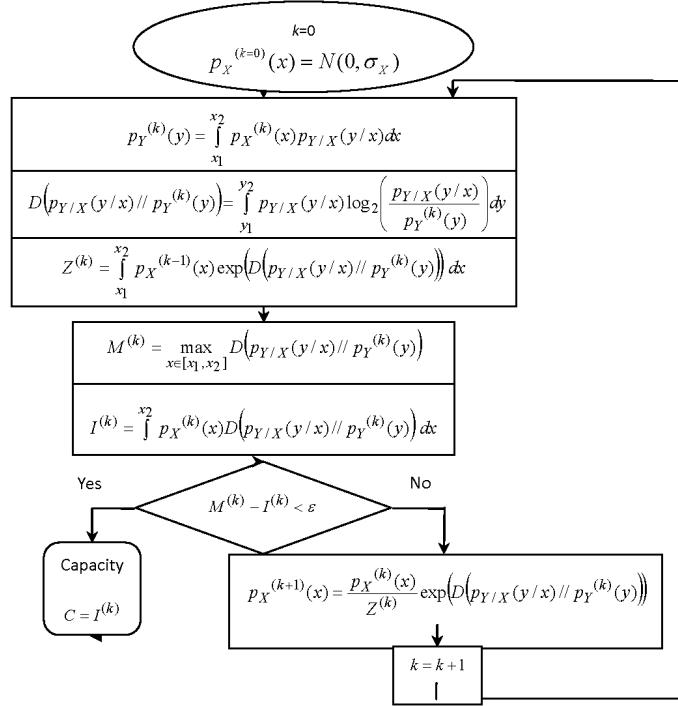
$$\hat{p}(x) = \sum_{k=1}^K P(k) p_k(x),$$

where

$$p_k(x) = \frac{1}{\sqrt{2\pi\sigma_k^2}} \exp\left(-\frac{(x-\mu_k)^2}{2\sigma_k^2}\right). \quad (9)$$

The K number of mixtures is pre-established by the experimenter and $P(k)$, μ_k and σ_k are parameters to be estimated (computed) on the data sample so as to minimise a given error function between the $p_X(x)$ and its $\hat{p}(x)$ approximation. In practice, an EM (expectation maximisation) estimation algorithm considering a maximum likelihood criterion proved its efficiency (Archambeau, Lee & Verleysen 2003): the convergence is stable and quick while the number of Gaussian laws in the mixture is conveniently low (e.g.

Figure 4. The continuous Blahut-Arimoto algorithm



from 5 to 10). For instance, an original statistical approach based on Gaussian mixture estimation made it possible for the first time to model the watermarking attacks with mathematical rigour and to grant sound basis to their stationarity hypothesis (Mitrea, Dumitru, Prêteux & Vlad 2007).

From the computational point of view, the Gaussian mixture representations offer a huge advantage: they allow any arbitrarily (non-analytical) *pdf* to be represented by a set of $3K$ parameters. Should the input *pdf* be represented by a Gaussian mixture, the capacity evaluation is no longer a problem of maximisation over the space of all possible input *pdfs* but a problem of maximisation in a $3K$ dimensional space. This observation is the basis for the *Gaussian Mixture based Capacity* evaluation method (*GMC*) which will be further summarised (Dumitru, Mitrea & Prêteux 2007). This method deals with the case of the ergodic zero-memory additive noise, when

the output *pdf* can be written as a convolution between the input and the noise:

$$Y = X + N \Rightarrow p_Y(y) = p_X(x) \circ p_N(n), \quad (10)$$

where \circ represents the convolution product. By combining (10) and (1), equation (11) can be written:

$$C = \max_{p_X(x)} \int_{x_1}^{x_2} \int_{x_1+n_1}^{x_2+n_2} p_X(x) p_N(y-x) \log_2 \frac{p_N(y-x)}{\int_{n_1}^{n_2} p_N(n) p_X(y-n) dn} dx dy \quad (11)$$

As the noise *pdfs* corresponding to a large variety of watermarking attacks were computed in our previous studies, assuming the input *pdf* represented by Gaussian mixtures with K parameters, (11) allows the capacity to be evaluated by maximising in the space of the $3K$ parameters.

3.2 Discrete Case

While the traditional (uncompressed domain) watermarking framework mainly deals with the continuous channel model, the very attractive and challenging compressed domain watermarking requires an in-depth study on the discrete channel model. Although the theoretical issue is basically the same in the two cases, the solutions are completely different (Mitrea, Dumitru, Duta, Prêteux & Vlad 2008), (Duta 2009).

Be there a discrete time-invariant channel with side information (with random states), and be $X = \{x_1, x_2, \dots, x_n\}$ the set of input symbols with the probabilities $P(X) = \{P(x_1), P(x_2), \dots, P(x_n)\}$, $Y = \{y_1, y_2, \dots, y_m\}$ the set of output symbols with the probabilities $P(Y) = \{P(y_1), P(y_2), \dots, P(y_m)\}$, and $S = \{s_1, s_2, \dots, s_k\}$ the set of states with the probabilities $P(S) = \{P(s_1), P(s_2), \dots, P(s_k)\}$. Such a channel is described by its conditional probability matrix $P(Y/X, S)$, i.e. by a set of k noise matrices of $P(Y/X)$ type. Note: these notations implicitly assume the ergodicity (or, at least, stationarity) of the input and noise sources as well as the time-invariance of the states.

The capacity of such a channel was first studied by Shannon (Shannon 1958), who considers that only the current channel state is known to the encoder before the transmission of each symbol. However, watermarking deals with a more generic case: as the entire video is available to the embedder, the state knowledge is non-causal (the past, present and future states are known when transmitting a symbol). A first expression for the capacity of such a channel is (Gel'fand & Pinsker 1980):

$$C = \max_{\substack{P(U/S) \\ P(X/U,S)}} [I(U, Y) - I(U, S)], \quad (12)$$

where U is an arbitrarily random variable, I is the mutual information, defined in the usual way and $P(Y, X, U, S) = P(Y/X, S)P(X/U, S)P(U/S)P(S)$. In such a way, the input is somewhat reflected by the U variable. Actually, as the function $I(U, Y) - I(U, S)$ is concave in $P(X/U, S)$, the capacity is found for $P(X/U, S) \in \{0, 1\}$, thus making X a deterministic function of U and S . The cardinality of U follows the rule $\text{card}(U) \leq \text{card}(X) + \text{card}(S)$.

In order to compute the capacity, all possible combinations for $P(X/U, S) \in \{0, 1\}$ have to be tested, resulting in $\text{card}(X)^{\text{card}(U) \cdot \text{card}(S)}$ maximisations. With no evidence towards the reduction of the U cardinality, the maximum value is considered for $\text{card}(U)$. Taking all these issues into consideration, this approach is only feasible for simple channels. As for example, for a 5 symbol input alphabet ($\text{card}(X) = 5$) and for 9 states ($\text{card}(S) = 9$), $N = 5^{149} \approx 1.175 \cdot 10^{88}$ maximisations would be needed for the capacity computation!

A second approach (Dupuis, Yu & Willems 2004) tries to elucidate this problem by removing the $P(X/U, S)$ term from the capacity computation. In this respect, an approach similar to the Shannon's is followed: the channel input alphabet is expanded by using a new random variable $T = \{t_1, t_2, \dots, t_l\}$, with each $t_i : S \rightarrow X$ a function mapping the values of S to X . The new channel noise is defined as $P(Y/T, S) = P(Y/X = t(S), S)$. The capacity is now given as

$$C = \max_{P(T/S)} [I(T, Y) - I(T, S)], \quad (13)$$

thus reducing its computation to a single maximisation that can be made with a derivation of the Blahut-Arimoto algorithm.

In order to perform this computation, the quantity to be maximised is re-written as

$$I(T, Y) - I(T, S) = \sum_{i,j,g} P(s_i) q(t_g / s_i) P(y_j / t_g, s_i) \log_2 \frac{Q(t_g / y_j)}{q(t_g / s_i)} \quad (14)$$

The $Q(t / y) = P(T / Y)$ and $q(T / S) = P(T / S)$ are considered as independent variables and the maximisation is made by alternatively optimising the quantity according to each of the two. The optimum quantities at each step are computed as

$$q^{(v+1)}(t_g / s_i) = \frac{\prod_j Q^{(v)}(t_g / y_j)^{P(y_j / t_g, s_i)}}{\sum_h \prod_j Q^{(v)}(t_h / y_j)^{P(y_j / t_h, s_i)}}, \quad (15)$$

$$Q^{(v+1)}(t_g / y_j) = \frac{\sum_i P(s_i) q^{(v)}(t_g / s_i) P(y_j / t_g, s_i)}{\sum_{h,i} P(s_i) q^{(v)}(t_h / s_i) P(y_j / t_h, s_i)} \quad (16)$$

Using this new approach, the gain in computation speed is traded for an extremely high memory requirement. The T cardinality is $\text{card}(T) = \text{card}(X)^{\text{card}(S)}$, the maximisation matrix having $\text{card}(S) \cdot (\text{card}(X))^{\text{card}(S)}$ elements. Resuming the previous example, this would mean $M = 9 \cdot 5^9 = 17578125$ floating point elements in the maximisation matrix. This high memory requirement, although not as prohibitive as the complexity of the Gel'fand and Pinsker algorithm, limits the complexity of the channel that can be evaluated with the computational resources available nowadays.

4. QUANTITATIVE RESULTS

This section illustrates the watermarking capacity computation with some key figures (Mitrea & Prêteux 2009), (Duta, Mitrea & Prêteux 2008) see Tables 1 and 2 and Figure 5.

The experimental corpus is composed of 10 video sequences, belonging to different movies, each of them about 25 minutes long ($L = 35000$ frames in each video sequence). Their content is heterogeneous, combining indoor and outdoor scenes, instable and arbitrary lighting conditions, still and high motion scenes. They are coded at a low quality (the worst case scenario in capacity computation): a 64 Kbit/s rate, and frame sizes of 192 x 80 pixels. Note that the same content have been considered in the two situations; however, the continuous case corresponds to the mark insertion before the MPEG-4 AVC compression. More details about the strategies for inserting the mark in the MPEG-4 AVC stream can be found in (Duta, Mitrea, Prêteux & Belhaj 2008).

4.1 Continuous Case

Be there the case in which the mark is inserted into the DWT coefficients decreasingly ordered and be there the following attacks: Gaussian filtering, sharpening, rotations, Stirmark. In order to compute the capacity, the following parameter instantiations have been considered:

- Capacity evaluation using the Shannon formulae, see (2) & (3)
 - The signal bandwidth W is half the sample rate:

$$F_{\text{rate}} = 2W = 25s^{-1}, W = 12.5Hz \text{ or} \\ W = 0.5frames^{-1}.$$

- The signal power P is evaluated starting from the transparency requirements, as follows. First, in watermarking, it may be considered that the mark is a zero mean signal (otherwise it can be eliminated by simple filtering operations). Secondly, from the transparency point of view, the mark disturbs the original signal;

hence, in order for it not to be perceived, it should be much lower than the original video content (e.g. between 25 and 35 dB lower). Hence, the signal power is first estimated, and then the mark power is computed so as to ensure such an SNR (30dB in Table 1, 25dB and 35dB in Table 2).

- The noise power N is connected to the robustness constraints. It is estimated as the second order moment (the sum of the variance and the square of the mean value) of the attacks.
- N_1 (the noise entropy power) is the power of a white noise, which has the same bandwidth and entropy as the analysed noise:

$$N_1 = \frac{\exp(2H(N))}{2\pi e}$$

where $H(N)$ is the entropy of the continuous information source modelling the noise.

- Capacity evaluation using the continuous Blahut-Arimoto algorithm
 - The input $p_x(x)$ has zero mean and the variance σ_x^2 computed so as to ensure a prescribed transparency of 25dB, 30dB or 35 dB (see the comments above). The $(x_1; x_2)$ interval is considered according to the Tchebycheff Inequality $(-6\sigma_x; 6\sigma_x)$. In the first iteration ($k = 0$), $p_x(x)$ is a Gaussian law.
 - The conditional $p_{Y/X}(y)$ and output $p_Y(y)$ pdfs are derived from the input and noise pdfs, assuming an additive channel. As already mentioned, the noise $p_N(n)$ is computed in a previous study (Mitrea, Dumitru, Prêteux & Vlad 2007) and, for additive noise,

$p_{Y/X}(y) = p_N(y - x)$; moreover, the output pdf takes values in the $(x_1 + n_1; x_2 + n_2)$ interval, where $n_1 = \mu_1 - 6\sigma_N$ and $n_2 = \mu_2 + 6\sigma_N$.

- The algorithm exits either when the error is lower than $\varepsilon = 10^{-4}$ or when $N = 10^5$ iterations are achieved.
- Capacity evaluation using the GMC algorithm
 - The input law $p_x(x)$ is represented by a mixture with of 5 Gaussian laws, with the same mean values and variances as above.
 - The noise pdfs $p_N(n)$ are the same as above.

Tables 1 and 2 represents a synopsis of the results, for all the four methods of capacity computation, for several real-life attacks, for three transparency levels (namely, 25dB, 30dB, and 35dB) and to three types of DWTs. Note that all the results correspond to a single DWT coefficient, namely the largest. Capacity values for the rest of coefficients and for the DCT domain have also been computed and are available by contacting the authors.

When inspecting Tables 1 and 2, several conclusions can be drawn. First of all, the Blahut-Arimoto and GMC methods lead to results in very good concordance: the mean relative errors, computed for all investigated cases, are about 10%. Moreover, these values belong to the corresponding limits, with singular exceptions. Note also that the popular Gaussian noise scenario is, in fact, completely meaningless for real-life applications: it results in severe underestimation of the capacity. For instance, for the StirMark attack and for the (9,7) DWT, when an SNR of 30 dB is considered, the Gaussian noise would lead to a capacity up to 15 times lower than the real case (0.02 bit/coeffcient/frame instead of 0.32 bit/coeffcient/frame in the case of the Blahut-Arimoto computation or of 0.38 bit/coeffcient/frame in case of GMC).

Table 1. Capacity value (bit/frame/rank) for rank $r = 1$ and $SNR = 30dB$

Type	Attack C	Gaussian filtering	Sharpening	Rotation +2°	Rotation -2°	Rotation +5°	StirMark
DWT (2,2)	Gaussian noise	0.09	0.03	0.01	0.01	0.01	0.02
	Limits	(0.42 ; 1.39)	(0.07 ; 0.63)	(0.01 ; 0.94)	(0.01 ; 0.98)	(0.01 ; 1.31)	(0.05 ; 0.60)
	Blahut-Arimoto	0.39	0.33	0.30	0.30	0.30	0.37
	GMC	0.47	0.38	0.39	0.37	0.36	0.42
DWT (4,4)	Gaussian noise	0.09	0.01	0.01	0.01	0.01	0.02
	Limits	(0.48 ; 1.48)	(0.06 ; 0.68)	(0.01 ; 0.92)	(0.01 ; 0.96)	(0.01 ; 1.28)	(0.05 ; 0.60)
	Blahut-Arimoto	0.39	0.33	0.30	0.30	0.30	0.32
	GMC	0.47	0.37	0.39	0.36	0.36	0.38
DWT (9,7)	Gaussian noise	0.14	0.06	0.01	0.01	0.01	0.03
	Limits	(0.72 ; 1.60)	(0.12 ; 0.61)	(0.01 ; 0.90)	(0.01 ; 0.90)	(0.01 ; 1.26)	(0.07 ; 0.57)
	Blahut-Arimoto	0.41	0.37	0.31	0.31	0.30	0.32
	GMC	0.58	0.44	0.36	0.37	0.36	0.38

 Table 2. Capacity evaluation (bit/frame/rank) for rank $r = 1$ and for two SNR levels ($SNR = 25dB$ and $SNR = 35dB$)

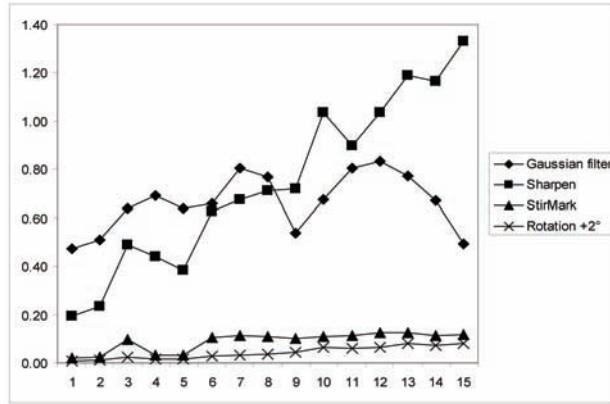
Type	Attack C	SNR = 25dB			SNR = 35dB		
		Gaussian filtering	Sharpening	StirMark	Gaussian filtering	Sharpening	StirMark
DWT (2,2)	Gaussian noise	0.09	0.03	0.02	0.09	0.03	0.02
	Limits	(0.42 ; 1.40)	(0.07 ; 0.64)	(0.05 ; 0.61)	(0.05 ; 1.31)	(0.01 ; 0.60)	(0.01 ; 0.58)
	Blahut-Arimoto	0.44	0.46	0.43	0.06	0.06	0.06
	GMC	0.53	0.52	0.53	0.07	0.07	0.07
DWT (4,4)	Gaussian noise	0.09	0.03	0.02	0.09	0.01	0.02
	Limits	(0.50 ; 1.48)	(0.08 ; 0.70)	(0.05 ; 0.60)	(0.06 ; 1.40)	(0.01 ; 0.64)	(0.01 ; 0.58)
	Blahut-Arimoto	0.43	0.45	0.41	0.08	0.07	0.02
	GMC	0.53	0.51	0.52	0.10	0.09	0.03
DWT (9,7)	Gaussian noise	0.15	0.05	0.02	0.14	0.06	0.03
	Limits	(0.72 ; 1.60)	(0.19 ; 0.61)	(0.07 ; 0.60)	(0.12 ; 1.47)	(0.01 ; 0.56)	(0.01 ; 0.54)
	Blahut-Arimoto	0.74	0.48	0.47	0.18	0.08	0.04
	GMC	0.85	0.56	0.57	0.22	0.10	0.05

4.2 Discrete Case

From the insertion point of view, a state channel corresponds to a technique where the insertion rule is changed according to the host coefficient

value. Hence, the number of states would be equal to the number of possible coefficient values, and, evaluating the capacity according to the procedures previously described would not be directly feasible.

Figure 5. The capacity values versus the spatial frequency for the four considered attacks



Consequently, in order to compute capacity values for MPEG-4 AVC, the following assumptions have been made:

- from the statistical point of view, the inserted data and the original content are altered by the attacks in the same way;
- the transparency restricts the data symbols to the -2, -1, 0, 1, and 2 values; this is a consequence of the reference study on the MPEG-4 AVC watermarking transparency (Duta, Mitrea, Prêteux & Belhaj 2008);
- the insertion technique replaces the original coefficients by the enrichment data symbols.

Under these assumptions, the capacity can be computed by the Dupuis formula, (13)-(16).

The coefficients to be investigated are selected according to their spatial frequencies, Figure 5; note that the coefficient indexes in Figure 5 correspond to the traditional MPEG zigzag order. The values represent the insertion capacity in bits per coefficient per macroblock (AVC block of 16x16 pixels). Note that in a video with 192×80 frame size, about only 50 such blocks can be altered in an *I* frame (Duta, Mitrea, Prêteux & Belhaj 2008).

From the compressed domain watermarking point of view, Figure 5 can be first considered as

a proof of concepts. Note that, at least at a first glance, *compressed domain watermarking* is from the theoretical point of view a contradiction in terms. On the one hand, compression eliminates all visual redundancy. On the other hand, watermarking exploits this redundancy in order to hide the mark. Hence, in an ideally compressed stream, there will be no more room for the mark insertion. However, our study brings into evidence that in the best compression standard nowadays in use (MPEG-4 AVC), the mark insertion is still possible. For instance, even when performing a StirMark attack, about 1.5 bit may be inserted in each macroblock in a frame *I*. As the transparency allows us to modify up to 50 macroblocks per frame, this means that about 75 bits can be inserted into a frame *I* while resisting the StirMark attack.

5. WATERMARKING CAPACITY COMPUTATION BETWEEN THEORY AND PRACTICE

Note that all the numerical results reported in this chapter are obtained out of applying information theory concepts to video watermarking; hence, questions may arise about how close the real life applications are from the general theoretical models¹.

Table 3. The viability of the in-band enrichment concept

Application/ Requirements	Attack	Indexing 25 bits/s	Subtitles 125 bits/s	MPEG games 1200 bits/s	Hyper video 2500 bits/s	iDTV 10000 bits/s
Uncompressed domain (9,7) DWT	Gaussian	Yes	Yes	Yes	Yes	No
	Sharpening	Yes	Yes	Yes	Yes	No
	StirMark	Yes	No	Yes	Maybe	No
Compressed domain MPEG-4 AVC	Filtering	Yes	Yes	Yes	No	No
	Sharpening	Yes	Yes	Yes	No	No
	StirMark	Yes	Yes	Maybe	No	No

The watermarking practice imposes the mutual independence among and between the mark to be inserted, the document to be protected and the malicious attacks: hence, it can be accepted that the information source, the noise source known at the embedder and the arbitrarily noise source are mutually independent. As the information source can be completely controlled by the experimenter (*i.e.* the way in which the mark is processed prior to the insertion), the rest of this section will discuss the statistical properties of the two noise sources.

When considering the continuous case, one key assumption is that the original video content can be modelled in the domain where the mark is inserted by a white Gaussian noise. The author previous studies (Mitrea, Prêteux, Vlad & Fetita 2004), (Mitrea, Zaharia, Prêteux & Vlad 2004) pointed out to what extent this popular assumption holds and established the restriction in selecting DCT or DWT coefficients obeying to the Gaussian *i.i.d.* model. The *i.i.d.* behaviour may be strengthen by shuffling the coefficients prior to the mark insertion (Miller, Doerr & Cox 2004). A second assumption refers to the additive behaviour of the attacks: this hypothesis was always considered in the literature (Cox, Miller & Bloom, 2003) and statistically confirmed (Mitrea, Dumitru, Prêteux & Vlad 2007). Finally, note that stationarity of the attacks can also be accepted on mathematical basis (Mitrea, Dumitru, Prêteux & Vlad 2007). To conclude with, for uncompressed video, the ac-

curacy of the capacity evaluation solely depends on the accuracy in the attack modelling.

The discrete case is more restrictive. In addition to the pitfalls in the computation method already discussed, no sound support for the compressed video and attack stationarity have yet been obtained. Consequently, a certain degree of variability of the results with the processed video sequence may be expected. However, note that when processing the 10 video sequences in our corpus, this variability was lower than 10%.

6. IN-BAND ENRICHMENT APPLICATIONS

This section discusses the pertinence of the *in-band enrichment* by facing it to five representative applications of the enrich media (Mitrea, Duta, Zaharia & Prêteux 2006): video indexing, the subtitles, video games, the hyper-video (clickable video) and the interactive Digital Television (iDTV); the results are synoptically displayed in Table 3.

The aim of *video indexing* is to describe the visual content with another type of information (generally, textual information) which can be very easily exploited for large database management. For instance, an MPEG-7 motion descriptor would require about 52 bits (Zaharia & Prêteux 2004) to describe the movement in a single film shot (an uninterrupted sequence filmed by one

Figure 6. Two scenarios for video data enriched with interactivity information; notice the interactivity information: the score, the ball and pinball control (a), and the memory game fragments selected by the mouse (b)



camera – generally, 2 to 10 seconds of video). From the uncompressed watermarking point of view, this means to insert a mark of about 50 bits in 50 to 250 frames. As for such an application we do not expect malicious attacks (nobody would be interested in removing such a mark), these requirements can be met by existing watermarking techniques. However, from the compressed domain watermarking, this means to insert the same 50 bits in 2 to 80 *I* frames: this is not possible with the nowadays watermarking methods but the capacity computation shows that one day such a method will be designed.

Inserting *subtitles* into a video is possible, in both compressed and uncompressed domain: such an application would require about 125 bit/s, which can be inserted even when assuming malicious attacks will be performed.

Another challenging issue is represented by the *MPEG video games* (Zaharia, Preda & Prêteux 2006). The challenge is to insert all the interactivity information in an original video. We considered two such interactive applications.

The first one is a video sequence enriched with a pinball game, Figure 6.a. The user can watch the movie into a very small round window which enlarges according to the points he/she scores. Such an application would require about 6 kilobytes of extra data which can be inserted in any video sequence in uncompressed domain (even in the worst case scenario, it would require only 80s of video). However, for compressed domain watermarking, longer video sequences (*i.e.* longer duration for the game) would be required. A similar behaviour is achieved for the second application, the memory game example in Figure 6.b. This example corresponds to the case in which the video to be watched is obturated by a commercial clip. This advertising progressively disappears as the player advances in the game.

The *clickable video* (hypervideo) is a particular type of video, in which specific regions of the frames (Figure 7) can be pointed (clicked) with a pointing device thus triggering an action (opening a www address, launching a JAVA application, *etc.*). With this aim, the original video should be

Figure 7. Clickable video



enriched with about 100 bits per frame. Table 3 lets us assume that such an application would be possible one day, but only in the uncompressed domain.

When considering the exploding *iDTV*, the in-band enrichment no longer works, at least not when malicious transformations are applied to the enriched content. However, for the content of high quality and when no alterations affect the enriched media, even such an ambitious application can be solved!

7. CONCLUSION

This chapter establishes the applicative perimeter for the *in-band enrichment*. In this respect, the theoretical support is granted by a study on the watermarking capacity, carried out for both uncompressed and compressed domains. Note that the capacity evaluation procedure, which is general and can be applied for any type of insertion domain, comes across with reference values corresponding to the DWT coefficient hierarchy and to the MPEG-4 AVC. These values prove that the in-band enrichment can serve a large variety of applications, from video indexing to hyper video and *iDTV*.

The research trends in the field are connected to the capacity computation for discrete side-information channels and to the design of optimal insertion rules. From the applicative point of view, the deployment of the in-band enrichment can be

facilitated by the emergence of the international standards.

REFERENCES

- Archambeau, C., Lee, J., & Verleysen, M. (2003). Convergence problems of the EM algorithm for finite Gaussian mixtures. In *Proc. 11th European Symposium on Artificial Neural Networks*, Bruges, Belgium (pp. 99-106).
- Archambeau, C., Valle, M., Assenza, A., & Verleysen, M. (2006). Assessment of probability density estimation methods: Parzen window and finite Gaussian mixtures. In *Proc. IEEE International Symposium on Circuits and Systems*, Kos, Greece.
- Arimoto, S. (1972). An algorithm for computing the capacity of arbitrary discrete memoryless channels. *IEEE Transactions on Information Theory*, 18(1), 14–20. doi:10.1109/TIT.1972.1054753
- Arnold, M., Schmucker, M., & Wolthusen, S. (2003). *Techniques and Applications of Digital Watermarking and Content Protection*. Boston: Artech House.
- Barron, R., Chen, B., & Wornell, G. (2003). The duality between information embedding and source coding with side information and some applications. *IEEE Transactions on Information Theory*, 49(5), 1159–1180. doi:10.1109/TIT.2003.810639

- Blahut, R. (1972). Computation of channel capacity and rate-distortion functions. *IEEE Transactions on Information Theory*, 18(4), 460–473. doi:10.1109/TIT.1972.1054855
- Chang, C., & Davisson, L. D. (2004). On calculating the capacity of an infinite-input finite (infinet)-output channel. *IEEE Transactions on Information Theory*, 34, 1004–1010. doi:10.1109/18.21223
- Costa, M. (1983). Writing on dirty paper. *IEEE Transactions on Information Theory*, IT-29, 439–441. doi:10.1109/TIT.1983.1056659
- Cox, I., Miller, M., & Bloom, J. (2003). *Digital Watermarking*. London: Academic Press.
- Dauwels, J. (2005). Numerical computation of the capacity of continuous memoryless channels. In *26th Symposium on Information Theory*. Benelux.
- Dauwels, J. (2006). *On graphical models for communications and machine learning: algorithms, bounds and analog implementation*. Unpublished Ph.D. thesis, ETH Zürich.
- Davoine, F., & Pateux, S. (Eds.). (2004). *Tatouage de documents audiovisuels numériques*. Lavoisier.
- Dumitru, O., Mitrea, M., & Prêteux, F. (2007). Accurate watermarking capacity evaluation. In *Proc. SPIE* (Vol. 6763, pp. 676303:1-12).
- Dupuis, F., Yu, W., & Willems, F. (2004). Blahut-Arimoto algorithms for computing channel capacity and rate-distortion with side information. In *Proc. IEEE International Symposium on Information Theory*, (pp. 181).
- Duta, S. (2009). *Robust video watermarking as an information theory application*. Unpublished PhD thesis, Université Paris V, France.
- Duta, S., Mitrea, M., & Prêteux, F. (2008). Capacity evaluation for MPEG-4 AVC watermarking. In *Proc. SPIE*, (Vol. 7000, pp. 70000V:1-10).
- Duta, S., Mitrea, M., Prêteux, F., & Belhaj, M. (2008). MPEG-4 AVC domain watermarking transparency. In *Proc. SPIE*, (Vol. 6982, pp. 69820F:1-10).
- Ericsson. (2009). Retrieved from <http://www.ericsson.com/ericsson/successtories/>
- Fre. (2009). Retrieved from <http://www.fresh-patents.com/System-and-method-for-enriched-multimedia-conference-IBM>.
- (2009). Retrieved from <http://www.research.ibm.com/journal/sj/443/petrie.html>
- Gel'fand, S. I., & Pinsker, M. S. (1980). Coding for channel with random parameters. *Problems of Control and Information Theory*, 9(1), 19–31.
- Irisa. (2009). Retrieved from <http://www.irisa.fr/temics/research/>
- ISO. (2005). ISO/IEC 14496-10 (2005).
- Louvre. (2009). Retrieved from <http://www.bestofmicro.com/actualite/24309-louvre-guide-multimedia.html>
- Matz, G., & Duhamel, P. (2004). Information geometric formulation and interpretation of accelerated Blahut-Arimoto-type algorithms. In *Proc. 2004 IEEE Information Theory Workshop*, San Antonio, TX (pp. 66-70).
- Miller, M., Doerr, G., & Cox, I. (2004). Applying informed coding and embedding to design a robust high-capacity watermark. *IEEE Transactions on Image Processing*, 13(6), 792–807. doi:10.1109/TIP.2003.821551
- Mitrea, M., Dumitru, O., Duta, S., Prêteux, F., & Vlad, A. (2008). A comprataive study on video watermarking capacity. In *Proc. of the IEEE 7th Intl. Conf. Communications 2008*, Bucharest, Romania (pp. 335-339).

- Mitrean, M., Dumitru, O., Prêteux, F., & Vlad, A. (2007). Zero-memory information sources approximating to video watermarking attacks. *Lecture Notes in Computer Science* 4707, (Vol. 3, pp. 445-459).
- Mitrean, M., Duta, S., Preda, M., & Prêteux, F. (2006). In-band enriched video for interactive applications. *WSEAS Trans. on Communications*, 5(8), 1528–1534.
- Mitrean, M., Duta, S., Prêteux, F., & Vlad, A. (2006). Data payload optimality: A Key Issue for Video Watermarking Applications. In *Proc. SPIE*, (Vol. 6315, pp. 630509:1-11).
- Mitrean, M., Duta, S., Zaharia, T., & Prêteux, F. (2006). Ensuring multimedia content adaptability by means of data hiding techniques. In *Proc. SPIE*, (Vol. 6383, pp. 63830:1-8).
- Mitrean, M., & Prêteux, F. (2009). From watermarking to in-band enrichment: future trends. invited paper to SPIE Electronic Imaging. In *Proc. SPIE*, (Vol. 7248, pp. 7248OI:1-10).
- Mitrean, M., Prêteux, F., Vlad, A., & Fetita, C. (2004). The 2D-DCT coefficient statistical behaviour: a comparative analysis on different types of image sequences. *JOAM*, 6(1), 95–102.
- Mitrean, M., Zaharia, T., Prêteux, F., & Vlad, A. (2004). Accurate Data Modelling for Watermarking Applications. In *Proc. of the IEE-IMA Intl. Conf. Mathematics in Signal Processing VI*, Cirencester – UK (pp. 167-170).
- Pay. (2009). Retrieved from <http://www.payper-news.nl/home/products/digi-magazine>
- Shannon, C.E. (1948). A mathematical theory of communications. *Bell Syst. Tech. J.*, 379-423 & 623-656.
- Shannon, C.E. (1958). Channels with side information at the transmitter. *IBM Journal*, 289-293.
- Thomson. (2009). Retrieved from <http://www.thomson.net/GlobalEnglish/Corporate/News/PressReleases/Pages/thomson-showcases-powerful-broadband-home-networking-ecosystem-at-cebit-2008-with-several-new-products.aspx>
- Vontobel, P. O., Kavcic, A., Arnold, D. M., & Loeliger, H.-A. (2008). A generalization of the Blahut–Arimoto algorithm to finite-state channels. *IEEE Transactions on Information Theory*, 54(5), 1887–1918. doi:10.1109/TIT.2008.920243
- Wiegand, T., Sullivan, G. J., Bjontegaard, G., & Luthra, A. (2003). Overview of the H.264/AVC video coding standard. *IEEE Trans. on Circuits and Systems for Video Technology*, 13(7), 560–576. doi:10.1109/TCSVT.2003.815165
- Wipo. (2009). Retrieved from <http://www.wipo.int/pctdb/en/wo.jsp?IA=WO2000067479&DISPLAYSTATUSservices-in-a-telecommunications-network-dt20061228ptan20060294186.php>
- Zaharia, T., Preda, M., & Prêteux, F. (2006). Interactivity, reactivity and programmability: advanced MPEG-4 multimedia applications. *IEEE International Conference on Consumer Electronics*, Las Vegas, NV (pp. 441 – 442).
- Zaharia, T., & Prêteux, F. (2004). Descripteurs visuels dans le standard MPEG-7. In Mostefaoui, A., Prêteux, F., Lecuire, V., & Moureaux, J.-M. (Eds.), *Gestion des données multimédias* (pp. 225–282). Lavoisier.

ENDNOTE

¹ The authors are grateful to the (unknown) reviewer(s) for suggesting them the utility of this section.

Chapter 6

Audio Watermarking: State-of-the-Art

Dejan Drajic
Ericsson d.o.o., Serbia

Nedeljko Cvejic
University of Cambridge, UK

ABSTRACT

In this chapter, the authors recapitulate the background and the state-of-the-art of digital audio watermarking, including descriptions of audio watermarking algorithms and malicious attacks against these algorithms. The areas in which audio watermarking has been implemented and the possible future applications are outlined. The three requirements of the “magic triangle” in audio watermarking are described as well, with characterized by a number of defining properties, including robustness, watermark bit rate and perceptual transparency. The chapter also provides a comprehensive list of attacks used by adversaries to interfere with the embedded watermark and to prevent its detection.

1. INTRODUCTION

Although the number of published articles on watermarking and information hiding increased sharply from 1992, the watermarking algorithms were primarily developed for digital images and video sequences (Bender, Gruhl, Morimoto, & Lu, 1996; Cox, & Miller, 2001), whereas the interest and research in audio watermarking started later (Hartung, & Kutter, 1999; Swanson, Zhu, & Tewfik, 1999). In the past few years, several algorithms for embedding and extraction of watermarks in audio

sequences have been published. It is clear that audio watermarking initially started as a sub-discipline of digital signal processing, focusing mainly on convenient signal processing techniques to embed additional information to audio sequences. This included the investigation of suitable transform domain for watermark embedding and schemes for imperceptible modification of the host audio. Digital watermarking has only recently been provided with a stronger theoretical foundation, becoming a more mature discipline, with a proper foundation in both communication modelling and information theory.

Section 2 presents application areas for the audio watermarking algorithms and in Section 3

DOI: 10.4018/978-1-61520-903-3.ch006

the three most important requirements in audio watermarking are highlighted (Arnold, Wolthusen, & Schmucker, 2003). For example, amount of data that can be embedded transparently into an audio sequence is considerably lower than the amount that can be hidden in images as audio signal has a dimension less than two-dimensional image files.

When the perceptual transparency requirement has been fulfilled, design objective is to increase robustness and achieve a practical watermark bit rate. Section 4 gives a general framework of the audio watermark systems performance in the presence of attacks. Many attacks that are malicious against image watermarking algorithms (e.g. geometrical distortions, spatial scaling etc.) cannot be implemented against audio watermarking schemes, whereas some of the signal modifications are specific for audio watermarking, such as time desynchronisation and echo addition.

A literature survey of audio watermarking algorithms that form the mainstream research is presented in Section 5. The algorithms are categorized by the statistical method used for detection and extraction of watermark bits, with references to specific algorithms using different signal domains for watermark embedding. Section 6 gives an overview of the publications describing for the latest developments in the area of audio watermarking.

2. AUDIO WATERMARKING APPLICATIONS

2.1 Ownership Protection

In the **ownership protection** applications, a watermark containing ownership information is embedded to the multimedia host signal. The watermark, known only to the copyright holder, is expected to be very robust and secure (i.e., to survive common signal processing modifications and intentional attacks), enabling the owner to demonstrate the presence of this watermark in

case of dispute to demonstrate his ownership. Watermark detection must have a very small false alarm probability. On the other hand, ownership protection applications require a small embedding data rate of the system, because the number of embedded bits that can be subsequently extracted does not have to be large, as long as the watermark robustness is preserved.

2.2 Authentication and Tampering Detection

In the content authentication applications, a set of secondary data is embedded in the host multimedia signal and is later used to determine whether the host signal was tampered. The robustness against removing the watermark or making it undetectable is not a concern as there is no such motivation from attacker's point of view. However, forging a valid authentication watermark in an unauthorized or tampered host signal must be prevented. In practical applications it is also desirable to locate (in time or spatial dimension) and to discriminate the unintentional modifications (e.g. distortions incurred due to moderate MPEG compression (Noll, 1993; Wu, 2004)) from content tampering itself. In general, the watermark embedding capacity has to be high to satisfy the need for more additional data than in ownership protection applications. The detection must be performed without the original host signal because either the original is unavailable or its integrity has yet to be established. This kind of watermark detection is usually called a **blind detection**.

2.3 Proof of Ownership

It is even more demanding to use watermarks not only in the identification of the copyright ownership, but as an actual **proof of ownership**. The problem arises when adversary uses editing software to replace the original copyright notice with his own one and then claims to own the copyright himself. In the case of early watermark systems,

the problem was that the watermark detector was readily available to adversaries. As elaborated in (Cox, 2003), anybody that can detect a watermark can probably remove it as well. Therefore, because an adversary can easily obtain a detector, he can remove owner's watermark and replace it with his own. To achieve the level of the security necessary for proof of ownership, it is indispensable to restrict the availability of the detector. When an adversary does not have the detector, the removal of a watermark can be made extremely difficult. However, even if owner's watermark cannot be removed, an adversary might try to undermine the owner. As described in (Cox, 2003), an adversary, using his own watermarking system, might be able to make it appear as if his watermark data was present in the owner's original host signal. This problem can be solved using a slight alteration of the problem statement.

Instead of a direct proof of ownership by embedding e.g. "Dave owns this image" watermark signature in the host image, algorithm will instead try to prove that the adversary's image is derived from the original watermarked image. Such an algorithm provides indirect evidence that it is more probable that the real owner owns the disputed image, because he is the one who has the version from which the other two were created.

2.4 Fingerprinting

Additional data embedded by watermark in the fingerprinting applications are used to trace the originator or recipients of a particular copy of multimedia file (Wu, 2004; Trappe, 2003). For example, watermarks carrying different serial or identity (ID) numbers are embedded in different copies of music CDs or DVDs before distributing them to a large number of recipients. The algorithms implemented in fingerprinting applications must show high robustness against intentional attacks and signal processing modifications such as lossy compression or filtering. Fingerprinting also requires good anti-collusion properties of the

algorithms, i.e. it is not possible to embed more than one ID number to the host multimedia file; otherwise the detector is not able to distinguish which copy is present. The embedding capacity required by fingerprinting applications is in the range of the capacity needed in copyright protection applications, with a few bits per second.

2.5 Broadcast Monitoring

A variety of applications for audio watermarking are in the field of broadcasting (Termont, 2000; Termont, 1999). Watermarking is an obvious alternative method of coding identification information for an active broadcast monitoring. It has the advantage of being embedded within the multimedia host signal itself rather than exploiting a particular segment of the broadcast signal. Thus, it is compatible with the already installed base of broadcast equipment, including digital and analogue communication channels. The primary drawback is that embedding process is more complex than a simple placing data into file headers. There is also a concern, especially on the part of content creators, that the watermark would introduce distortions and degrade the visual or audio quality of multimedia. A number of broadcast monitoring watermark-based applications are already available on commercial basis. These include program type identification, advertising research, broadcast coverage research, etc.

2.6 Copy Control and Access Control

In the copy control application, the embedded watermark represents a certain copy control or access control policy. A watermark detector is usually integrated in a recording or playback system, like in the proposed DVD copy control algorithm or during the development Secure Digital Music Initiative (SDMI). After a watermark has been detected and content decoded, the copy control or access control policy is enforced by directing particular hardware or software operations such

as enabling or disabling the record module. These applications require watermarking algorithms resistant against intentional attacks and signal processing modifications, able to perform a blind watermark detection and capable of embedding a non-trivial number of bits in the host signal.

3. AUDIO WATERMARKING REQUIREMENTS

Watermarking algorithms can be characterized by a number of defining properties (Cox et al., 2001). In this section, three of them will be highlighted, that are the most important for audio watermarking algorithms. The relative importance of a particular property is application-dependent and in many cases even the interpretation of a watermark property varies with the application. The three requirements make three corners of the “magic triangle” in watermarking, which cannot be fulfilled simultaneously.

3.1 Perceptual Transparency

In most of the applications, the watermark-embedding algorithm has to insert additional data without affecting the perceptual quality of the audio host signal (Zwicker, & Fastl, 1999). **Fidelity** of the watermarking algorithm is usually defined as perceptual similarity between the original and watermarked audio sequence. However, quality of the watermarked audio is usually degraded, either intentionally by an adversary or unintentionally in the transmission process, before a person perceives it. In that case, it is more adequate to define fidelity of a watermarking algorithm as perceptual similarity between watermarked audio and host audio at the point at which they are presented to a consumer (Cox et al., 2001, Lin et al., 2008).

In perceptual audio coding, the quality of codecs often is evaluated by comparing an original signal, called reference, with its coded version. This general principle is applied to the quality

evaluation of the watermarking systems as well. Instead of evaluating the coded version (as is the case in codec quality assessment) the watermarked version is analyzed. There are three objective measurement methods usually utilized for quality evaluation of the watermarked audio tracks. Those quality measurement systems are “Perceptual Audio Quality Measure” (PAQM) (Beerends, & Stemerdink, 1992), the system “Perceptual Evaluation of Audio Quality” (PEAQ) (ITU-R, 1998) and selected parameters of the “Noise to Mask Ratio” (NMR) (Brandenburg, & Sporer, 1992) measurement system.

In addition to objective measurements listening tests are usually performed as well. A number of audio sequences, that represent a broad range of music genres, are used as test signals; usual duration of test clips is 10-20 s. In the first part of the test, participants listen to the original and the watermarked audio sequences and are asked to report dissimilarities between the two signals, using a 5-point impairment scale: (5: imperceptible, 4: perceptible but not annoying, 3: slightly annoying, 2: annoying 1: very annoying). Results of the test should show the lowest and the highest value from the impairment scale and average MOS for given audio excerpt. In the second part, test participants are randomly presented with unwatermarked and watermarked audio clips and were asked to determine which one the watermarked one. Values near to 50% show that the two audio clips (original audio sequence and watermarked audio signal) cannot be discriminated.

3.2 Watermark Robustness

Robustness of the algorithm is defined as ability of the watermark detector to extract the embedded watermark after common signal processing manipulations. Detailed overview of robustness tests is given in Section 5. Applications usually require robustness in the presence of a predefined set of signal processing modifications, so that watermark can be reliably extracted at the detection

side. For example, in radio broadcast monitoring, embedded watermark need only to survive distortions caused by the transmission process including dynamic compression and low pass filtering, as watermark detection is done directly from the broadcast signal. On the other hand, in some watermarking applications robustness is completely undesirable and those algorithms are labelled **fragile audio watermarking** algorithms.

The ultimate goal of any watermarking system is reliable watermark extraction. In general, extraction reliability for a specific watermarking scheme relies on features of the original data, on the embedding distortion and on the attack distortion. Watermark extraction reliability is usually analysed for different levels of attack distortion and fixed data features and embedding distortion. Different reliability measures are used for **watermark decoding** and **watermark detection**.

In the performance evaluation of the watermark decoding, digital watermarking is considered as a communication problem. A watermark message is embedded into host signal and must be reliably decodable from the received signal. The decoding reliability is usually described by the word error probability (WER) or by the bit-error probability (BER).

Watermark detection is defined as the decision whether the received data is watermarked (hypothesis H_1) or not watermarked (hypothesis H_0). In general, both hypotheses cannot be separated perfectly. Thus, we define the probability p_{fp} (false positive) as the case of accepting H_1 when H_0 is true and the probability p_{fn} of accepting H_0 when H_1 is true (false negative). In many applications, the hypothesis test must be designed to ensure a limited false positive probability, e.g. $p_{fp} < 10^{-12}$ was proposed for watermark detection in the context of DVD copy protection (Cox et al., 2001). Another option for evaluation of watermark detection is the investigation of the total detection error probability p_e , which measures both possible error types.

3.3 Watermark Bit Rate

One of the most important properties of an audio watermarking system is **watermarked bit rate**, usually determined by specific demands of the application the system is designed for. Bit rate of the embedded watermark is number of embedded bits within a unit of time and is usually given in **bits per second** (bps).

In some applications, e.g. hiding speech in audio or compressed audio stream in audio, algorithms have to be able to embed watermarks with bit rate that is a significant fraction of the host audio bit rate, up to 150 kbps. It is a well-known fact in the audio compression community that only a few bits per sample are needed to represent music with quality near to compact disc quality music (Johnston, 1988). This implies that for uncompressed music, a significant level of noise can be injected into the signal without it being perceptible to the end user. Contrary to the compression methods, where this fact is utilized to decrease the file size of the audio clip, in information hiding it is used to maximize the bit rate of the inserted watermark inside the perceptual requirements of the HAS. High capacity hiding algorithms are usually not robust to signal processing modifications of the watermarked audio. However, authors in (Chou, Ramchandran, & Ortega, 2001) described system with watermark bit rate of 100 kbps, which does not cause distortion of the host audio sequence and is able to perfectly extract the hidden bits at a signal-to noise ratio of 15 dB.

Some audio watermarking applications, as copy control, require insertion of serial number or author ID, with average bit rate of up to 0.5 bps (Cox et al., 2001). On other hand, such applications demand a very high level of robustness and usually have to survive all the modifications listed in Section 5.

For broadcast monitoring watermark bit rate is higher, caused by necessity of embedding of ID signature of a commercial within the first second

at the start of the broadcast clip, with average bit rate up to 15 bps (Cox et al., 2001).

4. ATTACKS AGAINST AUDIO WATERMARKING ALGORITHMS

Subjective quality of the watermarked signal and robustness of the embedded watermark to various modifications are general requirements for all watermarking systems. Since the requirements of robustness, inaudibility and high capacity (“magic triangle”) cannot be fulfilled simultaneously, various variations and design criteria are significant for certain application of audio watermarking. The most important requirement addresses the inaudibility of inserted watermark; if the quality of audio signal cannot be preserved method will not be accepted neither by industry nor users. When the perceptual transparency requirement has been fulfilled, design objective is to maximize robustness inside the limits imposed by perceptual requirements, obtaining at the same time a practical watermark bit rate.

Common signal processing manipulations are frequently applied to the watermarked audio. They significantly modify frequency content and dynamics of the host signal and therefore distort the embedded watermark. Furthermore, third parties may attempt to modify the watermarked signal in order to prevent detection of the embedded data.

An example of a signal manipulation is preparation of audio material to be transmitted at a radio station. The audio sequence is first normalized and compressed to fit the loudness level of the broadcast transmission. Equalization is used as well, to optimise the quality of received audio. A denoiser (dehisser) reduces unwanted parts of the audio information and filters are used to cut off any frequency that cannot be transmitted. If a watermark is used for tracking of broadcasted commercials it has to be robust against all the attacks described above, or the extraction will be impossible. Another case is the Internet distribu-

tion, e.g. a company wants to embed watermarks as copyright protection. Thus, the watermark has to be robust against all operations usually applied to the material. In this case the most common attack will be lossy MPEG or AAC compression, usually at high compression rates.

To evaluate robustness of audio watermarking algorithms, attacks can be grouped by the manner in which signal manipulations distort the embedded watermark. Based on the attack models, following group of attacks are usually identified (Steinebach, et al., 2001):

- **Dynamics:** these modifications change the loudness profile of the watermarked audio, amplification and decreasing being the most basic attacks. Limiting, expansion and compression are more complicated, as they consist of non-linear changes depending on the input audio signal. There are even several frequency dependent compression algorithms, which only affect a part of the frequency range.

Examples:

1. Amplitude compression with compression rates dependent on the amplitude A: (8.91:1 for $A > -29\text{dB}$, 1.73:1 for $-46\text{dB} < A < -29\text{dB}$ and 1:1.61 for $A < -46\text{dB}$).
2. Denoising, usually utilized to remove noise from audio. A parameter is used to set the loudness of signals interpreted as noise, similar to a gate (usually set at -60 or -80 dB)

- **Filtering:** filters cut off or increase a selected part of the spectrum. The basic filters are high-pass and low-pass filters, but equalizers can also be seen as filters. They are used to increase or decrease certain subbands of audio spectrum.

Examples:

1. Highpass filter removes all frequencies lower than a threshold, e.g. 100 Hz

- 2. Low pass filter removes all spectral components higher than a threshold, e.g. 6 kHz.
- 3. 8-band equalizer, signal randomly suppressed or amplified by 6 dB in each band
- **Ambience:** audio effects simulating the presence of a room. The most common effects are reverb and delay that offer various parameters to set the quality of effect
Examples:
 1. *Delay*: a delayed replica of the original signal is added to it in order to simulate wide spaces. E.g. delay time 100 ms, amplitude decay 50%.
- **Conversion:** watermarked audio is often subject to format changes. Mono data can be mixed up in order to be used in stereo environments and stereo signal can be down mixed to mono. Sampling frequencies range from 32 kHz to 96 kHz, while sample resolution goes from 8 to 24 bits per sample.
Examples:
 1. Resampling, e.g. from 44.1 KHz to 11.025 kHz and back to 44.1 kHz.
 2. Sample resolution modification, from 16 bps to 8 bps and back to 16 bps.
- **Lossy compression:** audio compression algorithms based on psychoacoustic effects used to reduce the size of audio files by factor 10 or more.
Examples:
 1. Watermarked audio clips compressed to MPEG-1 files, at a rate of 128 kb/s
 2. Audio sequences were encoded with Advanced Audio Coder at the rate of 96 kb/s
- **Noise:** noise can be result of the most attacks described in this section and most of the hardware components introduce noise into the signal. Adversaries usually attack the watermarked audio by adding AWGN of certain amplitude.

Examples:

- 1. Random number addition to the values of audio samples, constrained by a parameter giving the relative amount of the number compared with the watermarked signal. Up to 0.91% of the original sample value could be added as noise without decreasing the subjective quality of the watermarked signal.

• **Modulation:** modulation effect like vibrato, chorus, amplitude modulation or flanging are usually not implemented in the broadcasting, but as most audio processing software includes such effects, they can be used as attacks to remove watermarks.

Examples:

- 1. *Chorus*: a modulated echo is added to the signal with various delay time, modulation strength ad number of voices. E.g. 4 voices, maximum delay 20 ms, delay rate 1.5 Hz, feedback 10%, voice spread 50 ms, vibrato depth 6 dB, vibrato rate 2 Hz, dry out (unmodified signal) 100% and wet out (effect signal) 5%
- 2. *Flanger*: flanging is usually created by mixing a signal with a lightly delayed copy of itself, where the delay length is continuously changing.
- 3. *Enhancer*: used to increase the power of signal in higher frequencies, thereby increasing the subjective brilliance. Effect is also known as “exciter”.

• **Time stretch and pitch shift:** these attacks either change the length of an audio sequence without changing its pitch or change the pitch of audio content without changing its length. They are used for fine tuning or fitting audio sequences into pre-defined time windows.

Examples:

- 1. *Pitch shifter*: used to change the base frequency without changing the speed of audio signal. This is one of the most

- sophisticated algorithms used in audio editing, with many different algorithms providing different output quality, depending on the characteristics of the original signal. E.g. pitch increased by 5 cents (a 480th of an octave).
2. *Time stretch*: effect similar to the pitch shift, used to increase the length of watermarked audio signal without changing its pitch. E.g. attacked watermarked audio sequence is 2% longer than the original watermarked sequence.
- **Sample permutations:** this group consists of the algorithms not used for audio manipulation in common environments. These attacks represent a specialized way to attack embedded watermarks in time domain.
- Examples:
1. *Zero-cross-inserts*: attack consists of search with the value 0 and addition of, for example, 20 zeros at this position, creating a short pause in the signal.
 2. *Copy samples*: Samples are randomly chosen and repeated in the signal, increasing its total duration. E.g. 20 sample repetitions in half a second.
 3. *Flip samples*: the positions of randomly chosen samples are permuted. E.g. 40 sample permutations in half a second.
 4. *Cut samples*: A sequence of randomly chosen samples is deleted from the signal: to make the modification inaudible a maximum length of the deleted sequence should be lower than 50.

Although a complete benchmark for the audio watermarking has not yet been implemented, there were some attempts to introduce unified testing environment for audio watermarking algorithms. Multiple advantages of unified third-party benchmark are obvious. First, researchers and software programmers would just provide a table of test results that would show summary of performances

of the proposed algorithm. Second, end users would get information whether their basic application requirements are fulfilled. Third, industry can properly estimate the risks associated with the use of a particular solution by having information about level of reliability of the proposed solution.

5. AUDIO WATERMARKING ALGORITHMS

Watermarking algorithms were primarily developed for digital images and video sequences; interest and research in audio watermarking started slightly later. In the past few years, several concepts for embedding and extraction of watermarks in audio sequences have been presented. A large majority of the developed algorithms take advantage of perceptual properties of the human auditory system (HAS) in order to add watermark into a host signal in a perceptually transparent manner. A broad range of embedding techniques goes from simple least significant bit (LSB) scheme to the various spread spectrum methods.

Watermark embedder design consists of adjusting the watermark signal to satisfy the perceptual transparency and simultaneously maximize the power of the watermark signal to provide high robustness. It usually contains a psychoacoustic analysis block that provides the embedding algorithm with frequency masking threshold, maximum allowable phase difference, temporal masking threshold or similar parameters necessary for optimal watermark embedding. Selection of the particular psychoacoustic analysis block depends on the domain used for watermark embedding in a specific algorithm.

After the watermarked signal is generated it is subjected to common audio signal distortions, including dynamic compression, filtering, and perceptual coding. The effect of those distortions on the embedded watermark is usually considered to be in the form of stationary additive Gaussian noise, although many watermark attacks are more

appropriately modelled as fading-like (Kundur, & Hatzinakos, 2001). A well-defined model for the distortion introduced by certain attack is a necessary precondition for design of an optimal watermark detector.

The ultimate goal of any watermarking system is reliable watermark extraction. It is important to make term separation between watermark decoding and watermark detection during the watermark extraction. Communicating a watermark message is the essence of embedding and decoding of a digital watermark while verifying whether the received audio sequence is watermarked or not is watermark detection.

5.1 Least Significant Bit Coding

One of the earliest techniques studied in the information hiding and watermarking area of digital audio (as well as other media types (Fridrich, Goljan, & Du, 2001; Lee, & Chen, 2000; Fridrich, Goljan, & Du, 2002) is LSB coding (Yeh, & Kuo, 1999). A simple approach in watermarking of the audio sequences is to embed watermark data by alternation of the certain bits of the digital audio stream, having the amplitude resolution of 16 bits per sample. It usually does not use any psychoacoustics model to perceptually weight the noise introduced by LSB replacement. However, there are some advanced methods of LSB coding (Lee et al., 2000; Cvejic, & Seppänen, 2002) that introduce a certain level of perceptual shaping.

The watermark encoder usually selects a subset of all available host audio samples chosen by a secret key. The substitution operation on the LSBs is performed on this subset. Extraction process simply retrieves the watermark by reading the value of these bits. Therefore, the decoder needs all the samples of the watermarked audio that were used during the embedding process. The random selection of the samples used for embedding introduces low power additive white Gaussian noise. As noted in Section 3, HAS is very sensitive to the

AWGN and that fact limits the number of LSBs that can be imperceptibly modified.

The main advantage of the method is a very **high watermark channel capacity**; use of only one LSB of the host audio sample gives capacity of 44.1 kbps (all samples used). The obvious disadvantage is extremely **low robustness**, due to fact that random changes of the LSBs destroy the coded watermark (Mobasseri, 1998). In addition, it is very unlikely that embedded watermark would survive digital to analogue and subsequent analogue to digital conversion. As no calculation-demanding transformation of the host signal in the basic version of this method needs to be done, this algorithm has a very small computational complexity. This permits the use on this LSB in real-time applications and a good basis for steganographic applications for audio signals (Chandramouli, & Memon, 2001; Dumitrescu, Wu, & Wang, 2003).

5.2 Watermarking the Phase of the Host Signal

Algorithms that embed watermark into the phase of the host audio do not use masking properties of the HAS, but the fact that the human auditory system has a low sensitivity to relative phase change (Bender et al., 1996). There are two main approaches used in watermarking of the host signal's phase, phase coding (Bender et al., 1996; Ruiz, & Deller, 2000) and phase modulation (Ciloglu, & Karaaslan, 2000; Tilki, & Beex, 1997; Lancini, Mapelli, & Tubaro, 2002).

Phase Coding

The basic phase coding method was presented in (Bender et al., 1996). The basic idea is to split the original audio stream into blocks and embed the whole watermark data sequence into the phase spectrum of the first block. One drawback of the phase coding method is considerably low payload

as only the first block is used for watermark embedding. In addition, the watermark is not dispersed over the entire data set available, but is implicitly localized and can thus be removed easily by the cropping attack. It is a **non-blind watermarking method**, which limits the number of applications it is suitable for.

Phase Modulation

Watermark insertion in this method is performed using independent multiband phase modulation [Kuo, Johnston, Turin, & Quackenbush, 2002; Gang, Akansu, & Ramkumar, 2001]. The original signal is segmented into M blocks containing N samples using overlapping windows:

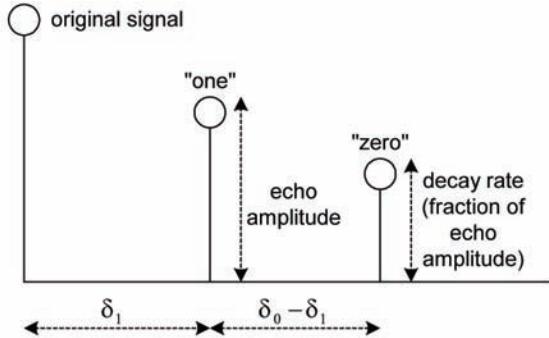
$$win(n) = \sin\left(\frac{\pi(n + 0.5)}{N}\right) \quad 0 \leq n \leq N - 1 \quad (4)$$

Watermark extraction requires perfect synchronization procedure to perform a block alignment for each watermarked block, using the original signal as a reference. The watermark bits from the k-th block are extracted from the phase modulation $\hat{\Phi}_k$ for that block. A matching of the particular segments of the modulated phase to the encoded watermark bits is possible if no significant distortions of the watermarked signal took place.

5.3 Echo Hiding

A number of developed audio watermarking algorithms (Huang, & Yeo, 2002; Ko, Nishimura, & Suzuki, 2002; Foo, Yeo, & Huang, 2001) are based on echo hiding method, described for the first time in (Bender et al., 1996). Echo hiding schemes embed watermarks into a host signal by adding echoes to produce watermarked signal. Echo hiding audio watermarking algorithm is a blind watermarking algorithm, designed especially for audio signals (it is not used in image or video

Figure 1. Parameters of echo embedding watermarking method



watermarking). It is highly robust against standard watermarking attacks and the watermark bit rate of several tens of bps.

The nature of the echo is to add resonance to the host audio, therefore the acute problem of sensitivity of the HAS towards the additive noise is circumvented in this method. After the echo has been added, watermarked signal retains the same statistical and perceptual characteristics. The offset (or delay) between the original and watermarked signal is small enough that the echo is perceived by the HAS as an added resonance. The four major parameters, initial amplitude, decay rate, "one" offset and "zero" offset are given in Figure 1.

Watermark embedding process can be represented as a system that has one of two possible system functions. In the time domain, the system functions are discrete time exponential differing only in the delay between impulses. Processing host signal through any kernel in Figure 1 will result in an encoded signal. The delay between the original signal and the echo is dependent on the kernel being used, δ_1 if the "one" kernel is used and δ_0 if the "zero" kernel is used.

The host signal is divided into smaller portions for encoding more than one bit. Each individual portion can then be considered each as an independent signal and echoed with the desired bit. The final watermarked signal (containing several bits) is composite of all independently encoded

signal portions. A smooth transition between portions encoded with different bits should be adjusted using different methods to prevent abrupt changes in the resonance in the watermarked signal. Information is embedded into a signal by echoing the original signal with one of two delay kernels. Therefore, extraction of the embedded information is to detect the spacing between the echoes. The magnitude of the autocorrelation of the encoded signal's cepstrum:

$$F^{-1} \left\{ \log \left(|F(x)|^2 \right) \right\} \quad (11)$$

where F represents the Fourier Transform and F^{-1} the inverse Fourier Transform can be examined at two locations, corresponding to the delays of the “one” and “zero” kernel, respectively. If the autocepstrum is greater at δ_1 than it is at δ_0 , embedded bit is decoded as “one”. For multiple echo hiding, all peaks present in the autocepstrum are detected. The number of peaks corresponding to the delay locations of the “one” and “zero” kernels are then counted and compared. If there are more peaks at the delay locations for the “one” echo kernel, the watermark bit is decoded as “one”.

Increased robustness of watermark algorithm requires high-energy echoes to be embedded which increases audible distortion. There are several modifications to the basic echo-hiding algorithm. (Xu, Wu, Sun, Xin, 1999) proposed a multi-echo embedding technique to reduce the possibility of echo detection by third parties. The technique has clear constraints regarding the increase of the robustness, as the audio timbre is noticeably changed with the sum of pulse amplitude (Oh, Seok, Hong, & Youn, 2001). (Oh et al., 2001) proposed echo kernel comprising multiple echoes by both positive and negative pulses with different offsets (closely located) in the kernel, of which the frequency response is plain in lower bands and large ripples in high frequency.

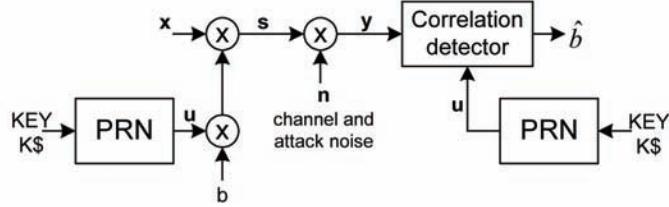
5.4 Spread Spectrum

In a number of the developed algorithms (Bassia, Pitas, & Nikolaidis, 2001; Neubauer, Herre, & Brandenburg, 1998; Cox, Kilian, Leighton, & Shamoon, 1997; Kirovski, & Malvar, 2003; Swanson, Zhu, Tewfik, & Boney, 1998), watermark embedding and extraction are carried out using spread-spectrum (SS) technique. SS sequence can be added to the host audio samples in time domain (Bassia et al., 2001; Cvejic, Keskinarkaus, & Seppänen, 2001), to FFT coefficients (Swanson et al., 1998; Ikeda, Takeda, & Itakura, 1999; Seok, & Hong, 2001), in subband domain (Kirovski, & Malvar, 2001; Li, & Yu, 2000; Tachibana, Shimizu, Kobayashi, & Nakamura, 2002), to cepstral coefficients (Lee, & Ho, 2000; Li, & Yu, 2000) and in compressed domain (Neubauer, & Herre, 2000; Cheng, Yu, & Xiong, 2002). If embedding takes place in a transform domain, it should be located in the coefficients invariant to common watermark attacks as amplitude compression, resampling, low pass filtering, and other common signal processing techniques. The idea is that after the transform, any significant change in the signal would significantly decrease the subjective quality of the watermarked audio. Thus, spread spectrum watermarking is a extremely robust, blind watermarking algorithm, with the watermark bit rate from a few bps to a several tens of bps.

Watermark is spread over a large number of coefficients and distortion is kept below the just noticeable difference level by using occurrence of masking effects of the human auditory system. Change in each coefficient can be small enough to be imperceptible, because correlator detector output still has a high signal to noise ratio, as it despreads the energy present in a large number of coefficients.

A general system for SS-based watermarking is shown in Figure 2. Vector x is considered to be the original host signal already in an appropriate transform domain. The vector y is the received vector, in the transform domain, after channel

Figure 2. General model for SS-based watermarking



distortions. A secret key $K\$$ is used by a pseudo random number generator (Furon, & Duhamel, 2003; Tefas et al., 2003) to produce a **spreading sequence u** with zero mean and whose elements are equal to $+\sigma_u$ or $-\sigma_u$. The sequence u is then added to or subtracted from the signal x according to the variable b , where b assumes the values of +1 or -1 according to the bit (or bits) to be transmitted by the watermarking process (in multiplicative algorithms multiplication operation is performed instead addition (Barni, Bartolini, De Rosa, & Piva, 2003). The signal s is the watermarked audio signal. A simple analysis of SS-based watermarking leads to a simple formula for the probability of error. Thus, if we consider the definitions of inner product and norm:

$$\langle \mathbf{x}, \mathbf{u} \rangle = \sum_{i=0}^{N-1} x_i u_i \text{ and } \|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle} \quad (12)$$

where N is the length of the vectors \mathbf{x} , \mathbf{s} , \mathbf{u} , \mathbf{n} , and \mathbf{y} in Figure 2. Without loss of generality, we assume that we are embedding one bit of information in a vector \mathbf{s} of N transform coefficients. That bit is represented by the variable b , whose value is either +1 or -1. Embedding is performed by

$$\mathbf{s} = \mathbf{x} + b\mathbf{u} \quad (13)$$

The distortion in the embedded signal is defined by $\|\mathbf{s} - \mathbf{x}\|$. It is easy to see that for the embedding equation (13), we have

$$D = \|b\mathbf{u}\| = \|\mathbf{u}\| = \sigma_u \quad (14)$$

The channel is modelled as additive noise $\mathbf{y} = \mathbf{s} + \mathbf{n}$, and watermark extraction is usually performed by calculation of the normalized sufficient statistic (Box, 1978) r :

$$r = \frac{\langle \mathbf{y}, \mathbf{u} \rangle}{\langle \mathbf{u}, \mathbf{u} \rangle} = \frac{\langle b\mathbf{u} + \mathbf{x} + \mathbf{n}, \mathbf{u} \rangle}{\sigma_u^2} = b + x + n \quad (15)$$

and estimating the embedded bit as $\hat{b} = sign(r)$, where $x = \langle \mathbf{x}, \mathbf{u} \rangle / \|\mathbf{u}\|$ and $n = \langle \mathbf{n}, \mathbf{u} \rangle / \|\mathbf{u}\|$.

Simple statistical models for the host audio \mathbf{x} and the attack noise \mathbf{n} are assumed. Both vectors are modelled as uncorrelated white Gaussian random processes (Box, 1978):

$$x_i \approx N(0, \sigma_x^2) \text{ and } n_i \approx N(0, \sigma_n^2) \quad (16)$$

Then, it is easy to show (Box, 1978) that the sufficient statistic r is also Gaussian variable, i.e.:

$$r \approx N(m_r, \sigma_r^2), \quad m_r = E[r] = b\sigma_r^2 = \frac{\sigma_x^2 + \sigma_n^2}{N\sigma_u^2} \quad (17)$$

Specifically, let us elaborate the case when b is equal to 1. In that case, an error occurs when $r < 0$, and therefore, the error probability p is given by

$$p = \Pr\{\hat{b} < 0 \mid b = 1\} = \frac{1}{2} \operatorname{erfc}\left(\frac{m_r}{\sigma_r \sqrt{2}}\right) = \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{\sigma_u^2 N}{2(\sigma_x^2 + \sigma_n^2)}}\right) \quad (18)$$

where $\operatorname{erfc}(*)$ is complementary error function. The equal error probability is obtained under the assumption that $b=-1$. For example, if an error probability lower than 10^{-3} is needed, than we get:

$$\frac{m_r}{\sigma_r} > 3 \Rightarrow N\sigma_u^2 > 9(\sigma_x^2 + \sigma_n^2) \quad (19)$$

or more generally, to achieve an error probability p we need:

$$N\sigma_u^2 > 2\left(\operatorname{erfc}^{-1}(p)\right)^2 (\sigma_x^2 + \sigma_n^2) \quad (20)$$

Equation (20) shows that we can make a trade-off between the length of the spreading sequence N and the energy of the spreading sequence σ_u^2 . It lets us to simply compute either N or σ_u^2 , given the other variables involved.

5.5 Patchwork Method

The patchwork watermarking technique was first presented in (Bender et al., 1996), for embedding watermarks in images. It is a statistical method based on hypothesis testing and relying on large data sets. As a second of CD quality stereo audio contains 88200 samples, patchwork approach is applicable for watermarking of audio sequences as well. The watermark embedding process uses a pseudorandom process to insert a certain statistic into host audio data set, which is extracted with the help of numerical indices (like the mean value) describing the specific distribution. The method is usually applied in a transform domain (Fourier, DCT, wavelet...) in order to spread the watermark in time domain and to increase robustness against signal processing modifications (Sugihara, 2001; Arnold, 2000; Yeo, & Kim, 2003). Patchwork

algorithm does not require the original host signal in the process of watermark detection (blind watermarking detection). Watermark bit rate is 1-10 bps, if a high robustness in the presence of attacks is required.

REFERENCES

- Arnold, M. (2000). Audio watermarking: Features, applications and algorithms. In *Proceeding of the IEEE International Conference on Multimedia and Expo*, (pp. 1013–1016).
- Arnold, M., Wolthusen, S., & Schmucker, M. (2003). *Techniques and applications of digital watermarking and content protection*. Boston: Artech House.
- Barni, M., Bartolini, F., De Rosa, A., & Piva, A. (2003). Optimum decoding and detection of multiplicative watermarks. *IEEE Transactions on Signal Processing*, 51(4), 1118–1123. doi:10.1109/TSP.2003.809371
- Bassia, P., Pitas, I., & Nikolaidis, N. (2001). Robust audio watermarking in the time domain. *IEEE Transactions on Multimedia*, 3(2), 232–241. doi:10.1109/6046.923822
- Beerends, J., & Stemerdink, J. (1992). A perceptual audio quality measurement based on a psychoacoustic sound representation. *Journal of the Audio Engineering Society. Audio Engineering Society*, 40(12), 963–972.
- Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, 35(3), 313–336. doi:10.1147/sj.353.0313
- Box, G. E. P. (1978). *Statistics for experimenters: An introduction to design, data analysis, and model building*. New York: John Wiley & Sons.

- Brandenburg, K., & Sporer, T. (1992). NMR and masking flag: Evaluation of quality using perceptual criteria. In *Proceedings of the International Audio Engineering Society Conference on Audio Test and Measurement*, (pp. 169–179).
- Chandramouli, R., & Memon, N. (2001). Analysis of LSB based image steganography techniques. In *Proceedings of IEEE International Conference on Image Processing*, (pp. 1019–1022).
- Chen, B., & Wornell, B. (1999). Dither modulation: A new approach to digital watermarking and information embedding. In *Proceedings of SPIE: Security and Watermarking of Multimedia Contents*, (pp. 342–353).
- Cheng, S., Yu, H., & Xiong, Z. (2002). Enhanced spread spectrum watermarking of MPEG-2 AAC. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 3728–3731).
- Chou, J., Ramchandran, K., & Ortega, A. (2001). High capacity audio data hiding for noisy channels. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, (pp. 108–111).
- Ciloglu, T., & Karaaslan, S. (2000). An improved all-pass watermarking scheme for speech and audio. In *Proceedings of the IEEE International Conference on Multimedia and Expo*, (pp. 1017–1020).
- Cox, I., Kilian, J., Leighton, F., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673–1687. doi:10.1109/83.650120
- Cox, I., & Miller, M. (2001). Electronic watermarking: The first 50 years. In *Proceedings of the IEEE Workshop on Multimedia Signal Processing*, (pp. 225–230).
- Cox, I., Miller, M., & Bloom, J. (2003). *Digital watermarking*. San Francisco: Morgan Kaufmann.
- Cvejic, N., Keskinarkaus, A., & Seppänen, T. (2001). Audio watermarking using m-sequences and temporal masking. In *Proceedings of the IEEE Workshop on Applications of Signal Processing to Audio and Acoustics*, (pp. 227–230).
- Cvejic, N., & Seppänen, T. (2002). Increasing the capacity of LSB-based audio steganography. In *Proceedings of the IEEE International Workshop on Multimedia Signal Processing*, (pp. 336–338).
- Dumitrescu, S., Wu, W., & Wang, Z. (2003). Detection of LSB steganography via sample pair analysis. *IEEE Transactions on Signal Processing*, 51(7), 1995–2007. doi:10.1109/TSP.2003.812753
- Foo, S. W., Yeo, T. H., & Huang, D. Y. (2001). An adaptive audio watermarking system. In *Proceedings of the IEEE Region 10 International Conference on Electrical and Electronic Technology*, (pp. 509–513).
- Fridrich, J., Goljan, M., & Du, R. (2001). Distortion-free data embedding. *Lecture Notes in Computer Science*, 2137, 27–41. doi:10.1007/3-540-45496-9_3
- Fridrich, J., Goljan, M., & Du, R. (2002). Lossless data embedding—New paradigm in digital watermarking. *Applied Signal Processing*, (2): 185–196.
- Furon, T., & Duhamel, P. (2003). An asymmetric watermarking method. *IEEE Transactions on Signal Processing*, 51(4), 981–995. doi:10.1109/TSP.2003.809376
- Gang, L., Akansu, A., & Ramkumar, M. (2001). MP3 resistant oblivious steganography. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, (pp. 1365–1368).
- Hartung, F., & Kutter, M. (1999). Multimedia watermarking techniques. *Proceedings of the IEEE*, 87(7), 1079–1107. doi:10.1109/5.771066

- Huang, D. Y., & Yeo, Y. H. (2002). Robust and inaudible multi-echo audio watermarking. In *Proceedings of the IEEE Pacific-Rim Conference on Multimedia*, (pp. 615–622).
- Ikeda, M., Takeda, K., & Itakura, F. (1999). Audio data hiding use of bandlimited random sequences. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 2315–2318).
- Johnston, J. (1988). Estimation of perceptual entropy using noise masking criteria. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 2524–2527).
- Kirovski, D., & Malvar, H. (2001). Robust covert communication over a public audio channel using spread spectrum. In *Proceedings of the Information Hiding Workshop*, (pp. 256–269).
- Kirovski, D., & Malvar, H. (2003). Spread-spectrum watermarking of audio signals. *IEEE Transactions on Signal Processing*, 51(4), 1020–1033. doi:10.1109/TSP.2003.809384
- Ko, B. S., Nishimura, R., & Suzuki, Y. (2002). Time-spread echo method for digital audio watermarking using PN sequences. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 2001–2004).
- Kundur, D., & Hatzinakos, D. (2001). Diversity and attack characterization for improved robust watermarking. *IEEE Transactions on Signal Processing*, 49(10), 2383–2396. doi:10.1109/78.950793
- Kuo, S. S., Johnston, J., Turin, W., & Quackenbush, S. (2002). Covert audio watermarking using perceptually tuned signal independent multiband phase modulation. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 1753–1756).
- Lancini, R., Mapelli, F., & Tubaro, S. (2002). Embedding indexing information in audio signal using watermarking technique. *Proceedings of EURASIP-IEEE Region 8 International Symposium on Video/Image Processing and Multimedia Communications*, (pp. 257–261).
- Lee, S. K., & Ho, Y. S. (2000). Digital audio watermarking in the cepstrum domain. *IEEE Transactions on Consumer Electronics*, 46(3), 744–750. doi:10.1109/30.883441
- Lee, Y. K., & Chen, L. H. (2000). High capacity image steganographic model. *IEEE Proceedings on Vision. Image and Signal Processing*, 147(3), 288–294. doi:10.1049/ip-vis:20000341
- Li, X., & Yu, H. (2000a). Transparent and robust audio data hiding in cepstrum domain. In *Proceedings of the IEEE International Conference on Multimedia and Expo*, (pp. 397–400).
- Li, X., & Yu, H. (2000b). Transparent and robust audio data hiding in subband domain. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, (pp. 74–79).
- Lin, Y., & Abdulla, W. H. (2008). Perceptual Evaluation of Audio Watermarking Using Objective Quality Measures. In *Proceedings of the IEEE International Conference on Acoustic, Speech, and Signal Processing*, Las Vegas, NV, (pp. 1745 - 1748).
- Mobasseri, B. (1998). Direct sequence watermarking of digital video using mframes. In *Proceedings of the International Conference on Image Processing*, (pp. 399–403).
- Neubauer, C., & Herre, J. (2000). Audio watermarking of MPEG-2 AAC bit streams. In *Proceedings of the Audio Engineering Society Convention*.
- Neubauer, C., Herre, J., & Brandenburg, K. (1998). Continuous steganographic data transmission using uncompressed audio. In *Proceedings of the Information Hiding Workshop*, (pp. 208–217).

- Noll, P. (1993). Wideband speech and audio coding. *IEEE Communications Magazine*, 31(11), 34–44. doi:10.1109/35.256878
- Oh, H. O., Seok, J. W., Hong, J. W., & Youn, D. H. (2001). New echo embedding technique for robust and imperceptible audio watermarking. In *Proceedings of the IEEE International Conference on Acoustic, Speech and Signal Processing*, (pp. 1341–1344).
- Ruiz, F., & Deller, J. (2000). Digital watermarking of speech signals for the national gallery of the spoken word. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 1499–1502).
- Seok, J. W., & Hong, J. W. (2001). Audio watermarking for copyright protection of digital audio data. *Electronics Letters*, 37(1), 60–61. doi:10.1049/el:20010029
- Steinebach, M., Petitcolas, F., Raynal, F., Dittmann, J., Fontaine, C., Seibel, S., et al. (2001). Stirmark benchmark: Audio watermarking attacks. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, (pp. 49–54).
- Sugihara, R. (2001). Practical capacity of digital watermark as constrained by reliability. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, (pp. 85–89).
- Swanson, M., Zhu, B., & Tewfik, A. (1999). Current state-of-the-art, challenges and future directions for audio watermarking. In *Proceedings of the IEEE International Conference on Multimedia Computing and Systems*, (pp. 19–24).
- Swanson, M., Zhu, B., Tewfik, A., & Boney, L. (1998). Robust audio watermarking using perceptual masking. *Signal Processing*, 66(3), 337–355. doi:10.1016/S0165-1684(98)00014-0
- Tachibana, R., Shimizu, S., Kobayashi, S., & Nakamura, T. (2002). An audio watermarking method using a two-dimensional pseudo-random array. *Signal Processing*, 82(10), 1455–1469. doi:10.1016/S0165-1684(02)00284-0
- Tefas, A., Nikolaidis, A., Nikolaidis, N., Solachidis, V., Tsekridou, S., & Pitas, I. (2003). Performance analysis of correlation-based watermarking schemes employing Markov chaotic sequences. *IEEE Transactions on Signal Processing*, 51(7), 1979–1994. doi:10.1109/TSP.2003.811245
- Termont, P., De Strycker, L., Vandewege, J., Haitsma, J., Kalker, T., Maes, M., et al. (1999). Performance measurements of a real-time digital watermarking system for broadcast monitoring. In *Proc. IEEE International Conference on Multimedia Computing and Systems*, Florence, Italy, (pp. 220–224).
- Termont, P., De Stycker, L., Vandewege, J., Op de Beeck, M., Haitsma, J., Kalker, T., et al. (2000). How to achieve robustness against scaling in a real-time digital watermarking system for broadcast monitoring. In *Proc. IEEE International Conference on Image Processing*, Vancouver, Canada, (pp. 407–410).
- Tilki, J., & Beex, A. (1997). Encoding a hidden auxiliary channel onto a digital audio signal using psychoacoustic masking. In *Proceedings of the IEEE South East Conference*, (pp. 331–333).
- Trappe, W., Wu, M., Wang, Z., & Liu, K. (2003). Anti-collusion fingerprinting for multimedia. *IEEE Transactions on Signal Processing*, 51(4), 1069–1087. doi:10.1109/TSP.2003.809378
- Wu, M., Trappe, W., Wang, Z., & Liu, K. (2004). Collusion-resistant fingerprinting for multimedia. *IEEE Signal Processing Magazine*, 21(2), 15–27. doi:10.1109/MSP.2004.1276103
- Xu, C., Wu, J., Sun, Q., & Xin, K. (1999). Applications of watermarking technology in audio signals. *Journal of the Audio Engineering Society*. *Audio Engineering Society*, 47(10).

- Yeh, C. H., & Kuo, C. J. (1999). Digital watermarking through quasi m-arrays. In *Proceedings of the IEEE Workshop on Signal Processing Systems*, (pp. 456–461).
- Yeo, I. K., & Kim, H. J. (2003). Modified patch-work algorithm: A novel audio watermarking scheme. *IEEE Transactions on Speech and Audio Processing*, 11(4), 381–386. doi:10.1109/TSA.2003.812145
- Zwicker, E., & Fastl, H. (1999). *Psychoacoustics: Facts and models*. Berlin: Springer-Verlag.

6. ADDITIONAL READING

- Deshpande, A., & Prabhu, K. M. M. (2009). A substitution-by-interpolation algorithm for watermarking audio. *Signal Processing*, 89(2), 218–225. doi:10.1016/j.sigpro.2008.07.015
- Erelebi, E., & Bataki, L. (2009). Audio watermarking scheme based on embedding strategy in low frequency components with a binary image. *Digital Signal Processing*, 19(2), 265–277. doi:10.1016/j.dsp.2008.11.007
- Ko, B.-S., Nishimura, R., & Suzuki, Y. (2005). Time-spread echo method for digital audio watermarking. *IEEE Transactions on Multimedia*, 7(2), 212–221. doi:10.1109/TMM.2005.843366
- Lee, H. S., & Lee, W. S. (2005). Audio watermarking through modification of tonal maskers. *ETRI Journal*, 27(5), 608–615. doi:10.4218/etrij.05.0105.0037
- Li, W., Xue, X., & Lu, P. (2006). Localized audio watermarking technique robust against time-scale modification. *IEEE Transactions on Multimedia*, 8(1), 60–69. doi:10.1109/TMM.2005.861291
- Lie, W.-N., & Chang, L.-C. (2006). Robust and high-quality time-domain audio watermarking based on low-frequency amplitude modification. *IEEE Transactions on Multimedia*, 8(1), 46–59. doi:10.1109/TMM.2005.861292
- Liu, Y.-W., Smith, J.O. (2007) Audio watermarking through deterministic plus stochastic signal decomposition. *EURASIP Journal on Information Security*, no. 75961.
- Malik, H., Ansari, R., & Khokhar, A. (2008). Robust audio watermarking using frequency-selective spread spectrum. *IET Information Security*, 2(4), 129–150. doi:10.1049/iet-ifs:20070145
- Wang, H., Nishimura, R., Suzuki, Y., & Mao, L. (2008). Fuzzy self-adaptive digital audio watermarking based on time-spread echo hiding. *Applied Acoustics*, 69(10), 868–874. doi:10.1016/j.apacoust.2007.06.001
- Wang, X.-Y., Niu, P.-P., & Qi, W. (2008). A new adaptive digital audio watermarking based on support vector machine. *Journal of Network and Computer Applications*, 31(4), 735–749. doi:10.1016/j.jnca.2007.10.001
- Wang, X.-Y., & Zhao, H. (2006). A novel synchronization invariant audio watermarking scheme based on DWT and DCT. *IEEE Transactions on Signal Processing*, 54(12), 4835–4840. doi:10.1109/TSP.2006.881258
- Readers interested in the state-of-the-art audio watermarking algorithms are encouraged to read the following articles that cover the latest developments in the area: Wu, S., Huang, J., Huang, D., & Shi, Y. Q. (2005). Efficiently self-synchronized audio watermarking for assured audio data transmission. *IEEE Transactions on Broadcasting*, 51(1), 69–76. doi:10.1109/TBC.2004.838265
- Xiang, S., Kim, H. J., & Huang, J. (2008). Audio watermarking robust against timescale modification and MP3 compression. *Signal Processing*, 88(10), 2372–2387. doi:10.1016/j.sigpro.2008.03.019
- Zaidi, A., Boyer, R., & Duhamel, P. (2006). Audio watermarking under desynchronization and additive noise attacks. *IEEE Transactions on Signal Processing*, 54(2), 570–584. doi:10.1109/TSP.2005.861106

Chapter 7

Watermarking Audio Signals for Copyright Protection Using ICA

B. R. Matam

NCRG, Aston University, UK

David Lowe

NCRG, Aston University, UK

ABSTRACT

The protection or tracking of content transmitted via digital time series data is an important and under-researched area of watermarking. In this chapter a discussion of information hiding in the context of copyright protection of audio signals, an example of time series data is presented. Independent component analysis (ICA) based watermarking methods are used to embed copyright information. The integrity of a hidden message when the cover text in which it is hidden, is attacked by applying signal processing techniques such as filtering and addition of noise to the signal will be investigated. The results of the application of the ICA based method are compared with the results of the application of the discrete wavelet transform (DWT) based approach. This chapter reveals the advantages of using a data dependent transform (for example ICA) based watermarking method for copyright applications when compared with static transform domain (having fixed coefficients, for example DWT) based methods.

INTRODUCTION

Steganography is the science of hiding information in plain sight. The word steganography is derived from Greek meaning covered or hidden writing. Bender et. al. (1996) state ‘embedding information into digital media for the purpose of copyright is a form of steganography’. The process of modifying cover data representing images, audio or video to

contain hidden information is called watermarking (Johnson & Katzenbeisser, 2000). Steganography and watermarking differ primarily in the intent, transmission and use of the hidden message (Cox et. al., (2007)). The message (watermark) is perceptually indistinguishable from the cover digital data but can be detected by systems designed for that purpose. The watermarks can be used to protect the rights of the owner of the digital media and provide a trace of the users of the digital data. Data hiding techniques have been successfully implemented

DOI: 10.4018/978-1-61520-903-3.ch007

for various applications such as copy control, fingerprinting, copyright protection, authentication of multimedia content.

In this chapter we discuss the security of copyright messages embedded into audio signal which represent multimedia content. The embedded message is the digital fingerprint (copyright message) of the owner of the audio signal and the audio signal forms the cover for the hidden message/watermark. The watermark embedding method is chosen such that the watermark is difficult to remove from the cover. The embedding method should also prevent any noticeable distortion of the cover due to the hidden watermark.

Embedding the messages in the spatial domain of the cover is well known (Kirovski & Malvar, 2003). The disadvantages of this type of embedding include easy execution of attacks on the watermarked cover such as removal and distortion of the embedded message. Hence the message that is to be embedded would need to be replicated and spread across the entire length of the cover (represented as *c*hereafter). This method is known as spread spectrum watermarking. More details of this method can be found in (Kirovski & Malvar, 2003 and references within). The embedded message can be protected against certain types and levels of attacks in the transform domain based watermarking methods. Based on the probable types of attack and the application of the hidden message, digital watermarking can be classified as robust (capable of resisting attacks), semi-fragile (distorts against very severe attacks but is not compromised when common signal processing techniques are applied) or fragile (perceptually distorts when the cover digital medium has been compromised even slightly). Since messages used for copyright protection need to be robust, this work focuses on watermarking methods providing robust blind copyright protection of the multimedia content ('blind', since we assume that the unmodified cover is not available at the receiver).

BACKGROUND

Examples of cryptography (data encryption) and steganography (data hiding) can be traced back to a period between 600BC and 400BC (see references within (Petitcolas, 2000)). The difference between the two methods being cryptography (Stallings, 2003) renders messages unintelligible to unauthorized persons who intercept them while steganography conceals the message itself from unauthorized persons (Petitcolas et. al. 1998). In cryptography the attacker knows that information is being transmitted and the security of the encryption method relies on the complexity (time and resources required) of the method used to estimate the key that is required to decipher the message. In steganography, the information is hidden in the sense that it is perceptually and statistically undetectable. The attacker's challenge is to not only identify the transmission of the hidden message but also to detect the location and if possible retrieve the hidden information.

This property of steganography (concealing information which needs to be secured in other data) can provide both anonymity to the embedded information and authentication of the cover work (Cox et. al. 2002). As already mentioned steganography and watermarking differ in the intent and use of the hidden messages. The techniques used to embed/retrieve the hidden information may be the same. Hence security mechanisms based on watermarking techniques become invaluable in applications necessitating copyright protection. With the use of appropriate embedding/detecting techniques the embedded information should be recoverable even if the host signal is compressed, edited or converted from digital to analog format and back (Cox et. al. 2002). As stated in (Craver, et al., 1998) various watermarking techniques for text, video, audio, image and 3D signals have been designed, attacked and countered and enhanced. Though new watermarking algo-

rithms are presented regularly in the literature, the fundamental goal of all the algorithms is to obtain the best trade-off between the three main characteristics of robustness, imperceptibility and rate of information of a watermark. Robustness is the capability of the watermark to resist distortion when the watermarked cover is attacked. The capability of the watermark to remain perceptually invisible in the cover work is referred to as the imperceptibility of the watermark and lastly the ratio of the number of samples of the watermark to the number of samples of the cover represents the rate of information of each watermark. The embedding algorithm is thus designed to provide the required trade-off between the three properties as necessitated by the application and use of the watermark.

Based on the application some of the relevant and most commonly used of watermarking techniques include least significant bit (LSB), patch-work and quantization index modulation (QIM). Many other different watermark embedding methods exist in the literature. These techniques have been used to embed the watermark in a cover work by applying transforms such as the discrete Fourier transform (DFT), the discrete cosine transform (DCT), the discrete wavelet transform (DWT), principal component analysis (PCA), and independent component analysis (ICA). Discussion of the many different embedding techniques and the various transforms is beyond the scope of this chapter. A brief list is presented at the end of the chapter (additional reading) which can be referred to for further information.

Most of the above mentioned transform domain based watermarking methods are mainly applied to multimedia images (2D and 3D). Watermarking approaches derived for time series data are limited. Embedding information into single channel time series data for example audio signals, EEG signals, ECG signals is more difficult and challenging compared with embedding information into images. This is due to the reduced redundancy of the time series data. Hence in this chapter a

watermarking approach designed specifically for one-dimensional time series audio data is provided.

The work presented in (Bounkong et. al. 2004; Toch, et. al. 2003; Matam & Lowe 2006) demonstrated for time series and images, the use of ICA as a frame based approach for information hiding. The advantage of using the principles of ICA for watermarking is: the ICA decomposes the input data (image, audio signal) into statistically independent components. This results in good robustness to the embedded information. When a set of signals are statistically independent, modification of one of the signals in the set (by embedding extra information) does not affect the other signals. This means embedding information into one of the independent components does not affect the other independent components. It was shown in (Bounkong et.al. 2004; Toch & Lowe 2005; Matam & Lowe 2006) that in order to recover the hidden message in the ICA approach it is important to use exactly the same independent components obtained while deriving the independent source signals. This sensitivity of the ICA based watermarking approach leads us to state that the set of independent components may be used as one of the keys in the data hiding method. Murillo-Fuentes (2007) has also discussed how the basis vectors derived from the ICA could be used as one of the secret keys in watermarking applications. It should also be noted that this sensitivity does not exist in transform domain based methods wherein the transform coefficients are known. An example of this is the orthogonal transform of DWT. Hence utilizing the sensitivity of the ICA we will show how the hidden message can be used for copyright protection and how the hidden message in the case of the DWT can be easily attacked.

Audio Watermarking

The human audio system (HAS) is capable of discerning frequencies in the range of 20Hz to 20kHz. High resolution audio systems (music)

sample at 44.1kHz which is almost twice the maximum frequency of the audio frequency range to maintain a high level of fidelity. In watermarking applications this redundant information can be exploited to embed extra information into music signals.

Audio signals are watermarked by embedding inaudible signals which can be used for copyright protection. Since the watermark data is perceptually indistinguishable from the audio signal, it must be of low intensity and the embedding algorithm must ensure that the embedded watermarks are robust to a wide range of signal processing techniques. Audio data undergoes D/A conversions (playing the audio signals on CD players, television) and A/D conversions (recording of audio signals using a microphone). Addition of noise during transmission is a common problem. Similarly compression of the audio data in order to store it in a compact form is another signal processing technique that is commonly applied to the audio data.

The embedded watermark distorts the audio signal. Since audio signals are heard, in order for the embedded watermark to be perceptually indistinguishable from the audio signals, watermarking of audio signals should be based on the understanding of the principles of the HAS. The HAS presents two interesting properties known as spectral masking and temporal masking (Painter, 2000). Sound waves alter the loudness of other sound waves within their spectral vicinity. In other words, if two sounds of similar frequency are heard together, the louder sound will mask the audibility of the second sound. This is known as spectral masking. Temporal masking is the masking of a sound wave that is heard immediately before or after a loud sound. This masking phenomenon of loud intensity sounds can be utilized to embed imperceptible watermarks.

The measurement of imperceptibility or inaudibility of the embedded watermarks can be conducted by listening tests. The imperceptibility of the watermark is measured by playing both the

unwatermarked audio signal and the watermarked audio signal to listeners participating in the test. The participants grade the audibility of the watermark on a 5 point impairment scale.

0. imperceptible
1. perceptible but not annoying
2. slightly annoying
3. annoying
4. very annoying

The imperceptibility is also measured by playing watermarked and unwatermarked audio files randomly to listeners. The participants are asked to determine if any of the audio files are watermarked audio files. If 50% or more of the participants correctly identify the watermarked audio files, then the watermark is said to be perceptible. This means that the distortion to the audio file due to the embedded watermark is high.

The peak signal to noise ratio (PSNR), where the cover work represents the signal and the embedded watermark, the noise signal, provides an easy measure to estimate the distortion to the cover work due to the embedded watermark. It is much simpler to implement compared to the feedback algorithms used to simulate the psychoacoustic model of the HAS. Since the PSNR does not provide a meaningful measure of the distortion of audio signals (as audio signals are heard and not viewed) objective measures to evaluate the quality of audio signals have been designed. These objective measures are the equivalent of PSNR for psychoacoustic distortion. One such measure is the ‘Perceptual Evaluation of Audio Quality (PEAQ)’. More information about objective measures for audio quality assessment can be obtained in (Kabal, 2002 and references within). PEAQ is measured as the degradation of the test signal with respect to a reference signal. In watermarking applications, the quality of the watermarked audio signal is compared with the unwatermarked audio signal. The difference be-

tween the two signals is rated using the 5 point impairment scale discussed above.

The rate of information or the number of watermark bits per cover signal bit that can be embedded is dependent on the type of audio signal used for cover. It is possible to embed more information into rock and pop music signals compared to classical music signals due to the wider range of the spectra of the rock and pop music. Toch & Lowe (2005) have shown that it is possible to embed relatively large amounts of information into pop music signals, 86.13bits/s compared to the 2.8bits/s used to watermark DVD audio.

Independent Component Analysis

Independent component analysis (ICA) (Hyvärinen et.al. 2001) is one of the most popular of blind source separation methods. ICA has been found to be a useful tool in various signal processing and image processing applications such as denoising, separation of signals from a multivariate data set. Let $\mathbf{x} = \{x_1, x_2, x_3, \dots, x_p\}$ represent a p dimensional random variable where $x_i = \sum_j a_{ij} s_j$. The ICA estimates a set of l basis vectors from a set of p linearly mixed random vectors $\mathbf{x} = \mathbf{As}$ where \mathbf{A} represents the mixing matrix and \mathbf{s} the set of source vectors. The main difference between the ICA and other linear projection techniques such as PCA is, the basis vectors estimated by the ICA are statistically independent. The set of basis vectors is known as the separating (also de-mixing) matrix say \mathbf{W} where \mathbf{W} is ideally the inverse of \mathbf{A} . The projection of \mathbf{x} onto \mathbf{W} , \mathbf{u} represents estimates of the sources, \mathbf{s} .

$$\mathbf{u} = \mathbf{Wx}$$

As a steganographic principle, the message is embedded in one, or several of the estimated independent sources. Bounkong et.al. (2004) summarize the advantages of ICA compared to other transforms for watermarking applications.

- Statistical independence of the resulting sources.
- An estimate of one source provides no information on other sources.

Other reasons stated in favor of using the ICA for steganography include: the same approach can be applied across different data modalities and, in the watermarking context, ICA allows the maximization of the information content and minimization of the induced distortion.

Application of ICA to Single Channel Time Series Data

Estimating l independent sources from p observations where $l > p$ is the typical application. Extracting l sources from p observations where $l > p$ (overcomplete bases) has been presented in many works. One of them is Lewicki & Sejnowski (2000). The ICA requires a set of observations and cannot be applied directly for a one-dimensional signal. In the case of a 2D image, the image is divided into blocks and each block is converted to a vector.

For a one-dimensional signal \mathbf{c} two different approaches can be implemented:

1. Equal non-overlapping segmentation of \mathbf{c} similar to the image processing domain, and
2. Delay embedding of \mathbf{c} .

Let N_c represent the length of \mathbf{c} . In the equal non-overlapping method the one-dimensional signal \mathbf{c} is divided into equal segments and each segment represents a single observation. Let N_{nov} represent the length of each segment:

$$x_i = c[(i-1)*N_{\text{nov}} + 1, \dots, i*N_{\text{nov}}],$$

where $i = \{1, p-1\}$.

The disadvantage of this method is that, the linear dependence between each segment is lost as each sample of the one-dimensional signal

represents the value of the random variable at a different instant of time. In order to extract a representation of the dynamics of the underlying sources the observed signals must be dependent on each other. When there is only one observed signal, this can be achieved by constructing delay vectors of the one-dimensional signal, \mathbf{c} . Woon & Lowe (2001) have shown that dynamical embedding of the one-dimensional signal to obtain \mathbf{x} results in a good estimation of the underlying sources.

We employ a delay embedding of \mathbf{c} with a delay of one sample between two successive delay vectors, \mathbf{d}_i and \mathbf{d}_{i+1} , and an embedding window size of p ,

$$\mathbf{d}_i = \mathbf{c}[1, 2, \dots, p],$$

$$\mathbf{d}_i = \mathbf{c}[i, \dots, p+i-1], \text{ where } i=2, \dots, N_c - p + 1.$$

The number of delay vectors $N_{ov} = N_c - p + 1$. Therefore we have,

$$\mathbf{x} = [\mathbf{d}_1; \mathbf{d}_2; \dots; \mathbf{d}_{N_{ov}}].$$

COVER DATA AND THE WATERMARK

The experiments presented in this chapter have been conducted on two different types of music: rock and pop. Each music file is sampled at 44.1kHz and represented using 16 bits. A segment of the music file equal to 0.3s duration is used for each experiment. The choice of 0.3s was made simply as a compromise between insufficient data to reliably estimate source vectors, and appropriately fast computational time. Let us represent each of the one-dimensional music signals as \mathbf{c} . The watermark is embedded into one of the sources estimated from the single channel music file by the application of the ICA method discussed previously.

A watermark used for copyright purposes is usually a low information rate message but it

requires a high level of robustness and must be imperceptible. The watermark employed for the experiments is a binary representation of a character string. A binary watermark is more fragile compared with a watermark derived from samples from a normal distribution. Attacks on the watermarked cover will flip the embedded watermark bit resulting in erroneous estimation of the embedded message. Hence if a method for embedding binary watermarks is robust, then when it is applied to embedding watermarks derived from a normal distribution it should result in better robustness.

METHODOLOGY

In this section we describe the application of the ICA and DWT methods to single channel time series data. An explanation of the selection of the source (ICA) and wavelet coefficients (DWT) used to carry the watermark data is provided. We also explain the procedure used to embed and retrieve the watermark.

Watermark Embedding Technique

The binary watermark which represents the copyright information is embedded in the selected source using quantisation index modulation.

‘QIM’ refers to embedding information by first modulating an index k_i or sequence of indices with the embedded information and then quantising the host signal with the associated quantizer or sequence of quantizers (Chen & Wornell 2001). Quantizers are defined as a class of discontinuous, approximate-identity functions. d defines a quantisation index representing a scalar quantizer.

For a binary watermark (WM), QIM generates the watermarked host data \mathbf{g}_w (\mathbf{g} is a generic term used to represent host data):

$$\mathbf{g}(k_i) = \delta N_e, \text{ if } WM_i = 0,$$

$$\delta N_o, \text{ if } WM_i = 1,$$

where N_e and N_o are respectively even and odd integers and $\mathbf{g}(k_i)$ is quantised to the nearest dN_e or dN_o . In QIM based watermark embedding the parameter d defines the position of the watermark on the trade-off triangle. For the embedded watermark to be robust against an attack the value of d should be large and to comply with the distortion constraint for imperceptibility, the message embedding function, F_m should be close to identity.

Selection of Secret Keys Used to Embed/Estimate the Watermark

Since the coefficients of the wavelet transform applied to \mathbf{c} to obtain its wavelets representation are fixed, the secret keys used to embed the watermark in the DWT-based method are \mathbf{k} and d . In the case of the ICA-based method, the basis vectors used to estimate the independent sources from \mathbf{c} are derived from the constructed input matrix \mathbf{x} . Hence the secret keys used to embed the watermark in the case of the ICA based approach are \mathbf{k} , d and \mathbf{W} (the matrix whose rows represent basis vectors).

The value of d is chosen randomly based on the robustness requirement of the watermark that is embedded. \mathbf{k} is a set of indices used to embed the watermark. The length of the watermark used for copyright purposes is usually much lower compared to the length of the host signal in which it is embedded. Hence the watermark can be embedded in the host signal in different ways. In one approach, the watermark may be replicated such that the total length is equal to the length of the host signal. Multiple copies of the watermark may then be embedded in \mathbf{c} . At the decoder, the multiple versions of the same watermark are recovered. A polling of all the recovered versions may be conducted to deduce a common pattern which represents the most probable estimate of the embedded watermark. This reduces the error in the watermark retrieved at the decoder but increases the distortion to \mathbf{c} . The common method

used to select the elements of \mathbf{k} though, is by using a random number generator.

A random number generator is used to select the values of \mathbf{k} such that no two values are the same. If \mathbf{k} contains indices which are repeated, then the same sample will be used to embed multiple watermark bits resulting in the loss of the embedded watermark at the embedding stage itself. Hence each of the values representing \mathbf{k} should be unique. Since the length of \mathbf{k} is equal to the length of the watermark, the distortion induced in the host signal due to the watermark is reduced but when the watermarked cover is subjected to an attack, the embedded watermark is also affected. The seed of the random number generator used by the watermark embedder is known at the decoder. For watermark retrieval, the decoder generates \mathbf{k} used at the embedder by using the same seed.

Watermark Estimation Technique

The nearest level decoding method is adopted to estimate the two watermarks, the original copyright watermark WM_o and the attacker's watermark WM_A .

$$WM_i = 0, \text{ if } (\mathbf{g}_i/\delta) \leq 0$$

$$1, \text{ if } (\mathbf{g}_i/\delta) \geq 1.$$

EMBEDDING WATERMARKS EXPERIMENT

This experiment was conducted for four watermarks quantised using different quantizer levels. Each watermark was embedded using different rates of information. The rate of information represents the ratio of the number of watermark bits to the number of available samples of the wavelets/independent source selected to embed the watermark. For each of the watermarks the experiment was repeated 5 times selecting a dif-

ferent set of indices \mathbf{k} selected randomly each time to reduce any bias in the results. The watermarked cover was tested against two different attacks, applied separately. Attack 1, a low pass filter of order 7 was applied and attack 2, a random noise signal was added to the watermarked cover. The recovered watermark was evaluated for errors by calculating the Hamming distance between the actual watermark embedded and the recovered watermark. The Hamming distance is represented as the bit error rate (BER) in the figures shown in the results. The results shown are the mean values over 5 iterations. Listening tests were conducted to estimate the distortion of the audio signals due to the embedded watermark. The results presented in this chapter are for rock pop music signals and the distortion levels were imperceptible.

Independent Component Analysis

The experiments were conducted by applying the ICA to observation matrices derived from \mathbf{c} using the dynamical embedding method discussed above. The disadvantage of the non-overlapping segmentation of \mathbf{c} to obtain \mathbf{x} has been mentioned in the section describing the application of the ICA to a one-dimensional signal. The advantage of the dynamical embedding method of constructing the input matrix to the ICA from a one-dimensional cover has also been mentioned in the same section. It shows that the dynamical embedding method of constructing \mathbf{x} is hence advantageous in a signal processing application wherein the underlying dynamics need to be extracted. In a watermarking application, this method though has a few limitations which are discussed in the next paragraph.

Reconstructing the one-dimensional \mathbf{c} from \mathbf{x} requires careful reordering of the samples. In the delay embedding method with a delay of one element, the elements of \mathbf{x} on the anti-diagonal are numerically the same. Hence in order to preserve this symmetry, only one sample across each diagonal can be modified with one bit of the watermark data. This results in a lower data rate

compared to the method using non-overlapping segments as each observation. Also due to the careful reordering used to reconstruct the watermarked cover this method is fragile compared to the non-overlap method.

In the dynamical embedding method of construction of observation signals from \mathbf{c} , the method described in (Woon & Lowe 2001) is used. A brief discussion of the dynamical embedding method is given below.

In order to capture the underlying dynamics of the signal \mathbf{c} , the size of the embedding window E_{win} should be large enough to capture the slowest frequency signal of interest in \mathbf{c} . Let f be the smallest frequency signal of the one-dimensional observation and f_s the sampling frequency of the observation signal (in this case 44.1kHz):

$$E_{\text{win}} = (1/f) * f_s.$$

E_{win} defines the upper limit on the possible number of sources (p) that can be estimated by the ICA. Each of the delay vectors thus obtained forms one observation signal. The set of delay vectors is the input \mathbf{x} to the ICA. The ICA estimates \mathbf{W} and \mathbf{u} from \mathbf{x} . One of the sources containing low frequency spectra, \mathbf{u}_u is used to embed the watermark.

The selection of the source used to embed the watermark is achieved based on the possible types of attack that the watermarked signal, \mathbf{c}_w may undergo. If \mathbf{c}_w is subjected to attacks such as compression and low pass filtering which affect the high frequency components of \mathbf{c}_w , the watermark should be embedded in the low frequency components of the signal. As we believe that music signals will undergo compression for faster transmission and high pass filtering to remove any additive noise, in our experiments the watermark is embedded in one of the sources \mathbf{u}_u containing low frequency spectra. The disadvantage of this is that usually embedding messages in low frequency spectra distorts the cover more significantly for a given embedding rate. However, the ICA based

approach has been shown to have less distortion than equivalent non-ICA based methods for the same rate.

The owner of the cover embeds the copyright message into \mathbf{u}_u using QIM. The secret keys used in the embedding of the watermark in \mathbf{u}_u are the set of indices \mathbf{k}_o and \mathbf{d}_o . The watermarked cover \mathbf{c}_w is obtained by applying the inverse of the separating matrix, the mixing matrix \mathbf{A} to $\mathbf{u} = [\mathbf{u}_1 \mathbf{u}_2 \dots \mathbf{u}_{wm} \dots \mathbf{u}_p]$ (where \mathbf{u}_{wm} represent \mathbf{u}_u modified).

Let h represent an attack on \mathbf{c}_w , in this case filtering/addition of noise. The attacked watermarked cover, \mathbf{c}_h is received at the decoder (recipient of the music file). For the experiments in this chapter we assume that the recipient is a malicious attacker who embeds her own watermark into the cover.

The attacker knows the watermark embedding method including the transform and the embedding technique. The attacker transforms \mathbf{c}_h by applying her knowledge of the transform used and obtains $\mathbf{u}_a = [\mathbf{u}_{1a} \mathbf{u}_{2a} \dots \mathbf{u}_{wma} \dots \mathbf{u}_{pa}]$ and \mathbf{W}_a (her estimate of the separating matrix). Using her secret keys \mathbf{k}_a and \mathbf{d}_a she embeds her watermark into one of the sources which contains low frequencies.

It is well known that the estimated independent components from the ICA are not fixed with respect to scaling and rotation. Hence, in order to bring out the advantages of using the independent components also as one of the secret keys, the selection of the source used to embed both the copyright message and the attacker's watermark is performed using the same procedure.

The attacker reconstructs \mathbf{c}_h further embedded with her watermark by applying the inverse of \mathbf{W}_a to \mathbf{u}_a (with one of the sources watermarked). Let \mathbf{c}_A represent the cover with both the copyright and the attacker's watermarks. \mathbf{c}_A is further filtered/modifies with noise to obtain \mathbf{c}_{Ah} which is processed to obtain an estimate of the copyright message and the attacker's message. The owner of \mathbf{c} and the attacker both estimate their version of independent sources using their unique set of basis vectors \mathbf{W} and \mathbf{W}_a . Using the keys \mathbf{k}_o and \mathbf{d}_o and, \mathbf{k}_a and \mathbf{d}_a , the two watermarks (copyright and

attacker's watermark) are retrieved. The nearest level decoding method is adopted to estimate the two watermarks.

Discrete Wavelet Transform

Embedding a digital watermark in the wavelet transform domain of multimedia images has been presented by many authors (see the additional reading material provided at the end of the chapter for references). The one-dimensional signal \mathbf{c} is transformed to obtain its time-frequency representation using the DWT. A four level wavelet decomposition of the time series data is obtained. The owner's watermark used for copyright purposes is embedded in the fourth level detail coefficients in order to obtain the required trade-off between the three principal characteristics of imperceptibility, robustness and capacity. The secret keys used to embed the copyright message are \mathbf{k}_o and \mathbf{d}_o . The values of d and the data rate in the experiments based on the DWT method are not numerically the same as those used in the experiments based on the ICA method. They are derived based on the length of the number of detail coefficients obtained for the fourth level of wavelet decomposition.

\mathbf{c}_w is obtained by applying the inverse of the wavelet transformation to the wavelet coefficients. As in the experiments based on the ICA, let h represent an attack on \mathbf{c}_w (filtering/addition of noise) which results in an attacked watermarked cover \mathbf{c}_h . The attacker reconstructs the wavelet coefficients from \mathbf{c}_h and embeds her watermark in the fourth level detail coefficients (selecting her own secret keys \mathbf{k}_a and \mathbf{d}_a). Let \mathbf{c}_A represent the cover with both the copyright and the attacker's watermarks which is further filtered/modifies with noise to obtain \mathbf{c}_{Ah} . The attacked doubly-watermarked signal is processed to retrieve the two watermarks.

RESULTS

The results shown in Figures 1, 2 and 3 have been obtained for pop music signals. Figure 1 is the BER obtained for the four watermarks of different quantizer levels embedded by the owner for copyright and overwritten by the attacker for the ICA based method. These results are obtained when the watermarked cover has been tested for an addition of noise attack.

The length of each independent source defines the maximum length of each watermark. Since copyright messages are used to define ownership of the cover, they are of limited length. The length of each of the watermark has hence been derived as a fraction of the maximum length possible. The different rates used in the experiments ranged from 20% of the maximum possible length to 80% of the maximum possible length.

Figure 2 is the result of a similar experiment conducted for the DWT based method. The maximum length of each watermark in this case is limited by the length of the detail coefficients obtained for the fourth level decomposition. The four watermarks are derived as in the ICA method.

It should be noted that in the ICA based method the watermarks used for copyright are recovered without error (both copyright and attacker's set) when the number of quantisation levels is low. The maximum error is 20% when the rate of information is 60% of the available. As the value of the number of quantisation levels increases the error in the watermarks recovered increases. This is the effect of the trade-off between robustness and information rate. The larger the rate of information, the less the robustness of the embedded message. The error in the case of the copyright message is higher than that of the attacker's message. This is because when the copyright message is embedded using a small value of d and the attacker embeds her own watermark, the watermark bits are shifted away from the quantizer levels used to embed the watermark.

In the DWT based method all the watermarks used for copyright are recovered with increasing error (Figure 2). There is a 10% error even when only 20% of the available samples are watermarked. The error increases as the value of d decreases. The relationship between d and robustness has been discussed earlier and the results in

Figure 1. Bit error rate for the two watermarks (of different data rates) embedded using the ICA based method

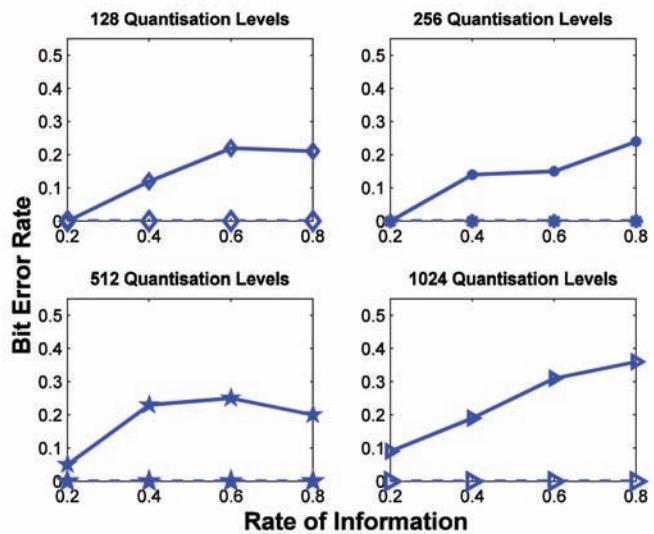


Figure 2. Bit error rate for the two watermarks (of different data rates) embedded using the DWT based method. It should be noted that the BER in the case of the ICA based watermark embedding method is less when compared with the BER for the DWT based watermarking method.

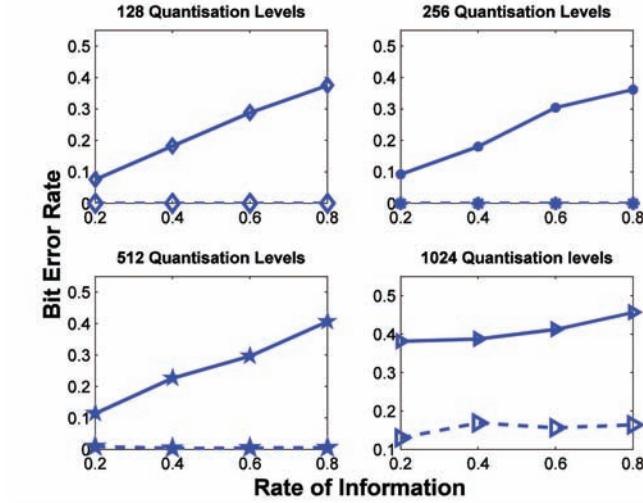
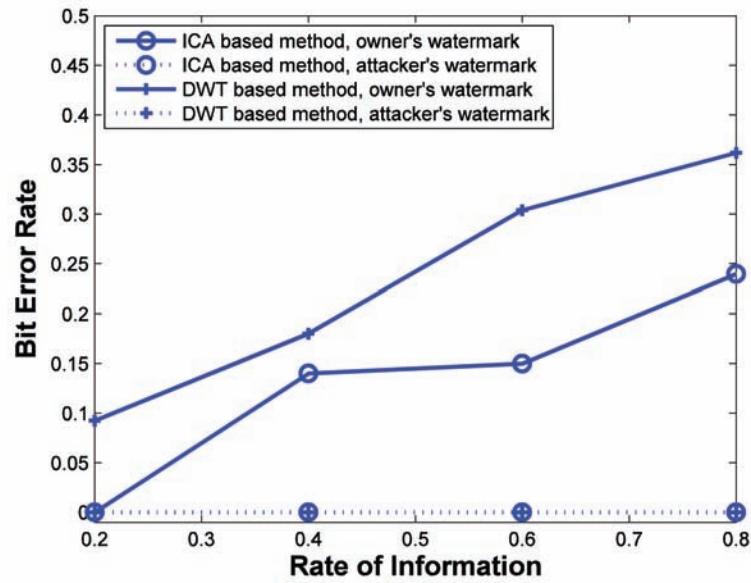


Figure 3. Bit error rate for the two watermarks (copyright and attacker's) embedded using the ICA and DWT based method for noise attack



Figures 1 and 2 are the evidence. It should also be noted that while the attacker's watermarks are recovered with no error for reducing value of d, the copyright messages are distorted to a larger

extent for the same d. This higher distortion of the copyright message shows that the attacker's watermark affects the copyright message similar

to that as h , a signal processing attack and it also varies with changes in d .

Secondly, when the transform coefficients are static as in the DWT and assuming that the attacker has complete knowledge of the watermarking system, the transform used, and the embedding technique, the probability of the indices representing \mathbf{k}_a containing similar values as that of \mathbf{k}_o exists. Let N_{wm} represent the length of the watermark and N_h the length of the host signal (wavelets in the DWT based method). As mentioned in Johnson & Katzenbeisser (2000), for $N_{wm} \ll N_h$ the probability p_c that \mathbf{k}_o and \mathbf{k}_a contain at least one common value is given by

$$p_c \approx 1 - \exp(N_{wm} [N_{wm} - 1]/2N_h).$$

As the length of N_{wm} increases the probability of \mathbf{k}_o and \mathbf{k}_a containing similar values increases, that is the value of p_c increases to one.

In the case of the ICA-based method, assuming that the attacker has complete knowledge of the segmentation procedure, the transform used and the embedding method, she estimates a set of independent sources and the basis vectors, \mathbf{W}_a from the cover containing the copyright watermark. It has been shown in (Toch & Lowe 2005; Matam & Lowe 2006; Matam & Lowe 2009) that the basis vectors derived by the ICA are sensitive to changes in the input data. Though the probability of the attacker selecting the source embedded with the copyright message to embed her own watermark exists, by careful selection of the value of d , and the use of \mathbf{W} as one of the secret keys, the copyright message can be retrieved.

Figure 3 is the result of embedding a copyright message which is overwritten by the attacker's message. The results are shown for the ICA-based approach and the DWT-based approach. The number of quantizer levels that are used to embed the watermarks in both the methods are maintained equal. The watermarked cover is attacked by the addition of random noise. In the ICA-based approach the watermarks (copyright

and attacker's) are embedded into sources containing low frequency spectra. In the DWT based approach the watermarks are embedded into the detail coefficients obtained for the fourth level decomposition of \mathbf{c} . As mentioned in Mehul & Priti (2003) noise affects low frequency signals. This can be noticed from the results in Figure 3.

The ICA-based method performs better than the DWT-based approach as the spectra of the detail coefficients used to embed the watermarks contain lower frequencies compared with the source used to embed the watermarks. It should be noted that while both the watermarks are equally distorted in the case of the ICA-based approach, the copyright message is distorted to a lower extent when compared with the attacker's in the case of the DWT-based method.

CONCLUSION

In this chapter digital watermarking for copyright protection of multimedia content in the form of time series (audio signals) has been investigated using the two transform based methods of ICA and DWT. The experiments were conducted on music signals of three different types. Embedding information in time series data is more complicated when compared to embedding information in image data. This is because time series data has less redundancy which can be modified to hide information compared with images which have more inherent redundancy that can be used to embed extra information. We have illustrated one small but difficult example: that of retrieving the original watermark when the watermarked cover is re-watermarked. From the results obtained for the two different types of attacks it was shown that in the case of the DWT based method, the copyright message will be overwritten by the attacker's and will be affected independent of the type of attack whereas in the ICA-based approach the value of the quantisation index plays an important role in the retrieval of the copyright message. By

careful selection of the number of quantisation levels the embedded copyright message can be recovered from the cover work even when the cover is additionally corrupted by the copyright of an attacker. It was shown that the ICA-based watermarking approach is better suited to prevent loss of copyright.

REFERENCES

- Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, 35(3&4), 313–336. doi:10.1147/sj.353.0313
- Bounkong, S., Toch, B., Saad, D., & Lowe, D. (2004). ICA for Watermarking. *Journal of Machine Learning Research*, 4(7-8), 1471–1498. doi:10.1162/jmlr.2003.4.7-8.1471
- Chen, B., & Wornell, G. W. (2001). Quantization Index Modulation: a Class of Provably Good Methods for Digital Watermarking and Information Embedding. *IEEE Transactions on Information Theory*, 47(4), 1423–1443. doi:10.1109/18.923725
- Cox, I. J., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). *Digital Watermarking and Steganography*. San Francisco: Morgan Kaufmann Publishers.
- Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). *Digital Watermarking*. San Francisco: Morgan Kaufmann Publishers.
- Craver, S., Memon, N., Yeo, B., & Yeung, M. M. (1998). Resolving Rightful Ownerships With Invisible Watermarking Techniques: Limitations, Attacks and Implications. *IEEE Journal on Selected Areas in Communications*, 16(4), 573–586. doi:10.1109/49.668979
- He, X. & Scordilis, M. S. (2008). Efficiently synchronized spread-spectrum audio watermarking with improved psychoacoustic model. *Research letters in Signal Processing*, 2008 (1), 1-5.
- Hyvärinen, A., Karhunen, J., & Oja, E. (2001). *Independent Component Analysis*. New York: Wiley-Interscience. doi:10.1002/0471221317
- Johnson, N. F., & Katzenbeisser, S. (2000). A survey of steganographic techniques. In Katzenbeisser, S., & Petitcolas, F.A.P. (Eds.), *Information Hiding techniques for steganography and digital watermarking*. Boston: Artech House.
- Kabal, P. (2002). *An Examination and Interpretation of ITU-R BS. 1387: perceptual evaluation of audio quality*. Technical report, Department of Electrical and Computer Engineering, Mc Gill University. Retrieved from <http://www.tsp.ece.mcgill.ca>
- Kirovski, D., & Malvar, H. S. (2003, April). Spread-Spectrum Watermarking of Audio Signals. *IEEE Transactions on Signal Processing*, 51(4). doi:10.1109/TSP.2003.809384
- Lewicki, M., & Sejnowski, T. J. (2000). Learning overcomplete representations. *Neural Computation*, 12, 337–365. doi:10.1162/089976600300015826
- Matam, B. R., & Lowe, D. (2006). Steganography, BioPatterns and Independent Components. In *Proc. 7th Int. Conf. Mathematics in Signal Processing*, (pp. 206-209).
- Matam, B. R., & Lowe, D. (2009). Exploiting sensitivity of nonorthogonal joint diagonalisation as a security mechanism in steganography. In *Proceedings of 16th International Conference on Digital Signal Processing*.
- Mehul, R., & Priti, R. (2003). Discrete Wavelet Transform Based Multiple Watermarking Scheme. In *Proc. IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific*, Bangalore, India.

- Murillo-Fuentes, J. J. (2007). Independent component analysis in the blind watermarking of digital images. *Neurocomputing*, 70(16-18), 2881–2890. doi:10.1016/j.neucom.2006.06.011
- Painter, T., & Spanias, A. (2000). Perceptual Coding of Digital Audio. *Proceedings of the IEEE*, 88(4). doi:10.1109/5.842996
- Petitcolas, F. A. P. (2000). Introduction to information hiding. In Katzenbeisser, S., & Petitcolas, F. A. P. (Eds.), *Information Hiding techniques for steganography and digital watermarking*.
- Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1998). Attacks on Copyright Marking Systems. In Information Hiding, (pp. 218-238).
- Stallings, W. (2003). *Cryptography and Network Security Principles and Practice*. Upper Saddle River, NJ: Pearson Education International.
- Toch, B., & Lowe, D. (2005). Watermarking of medical signals. In *Proc. 2nd Int. Conf. on Computational Intelligence in Medicine and Healthcare*, Lisbon, Portugal, (pp. 231- 236).
- Toch, B., Lowe, D., & Saad, D. (2003). Watermarking of audio signals using Independent Component Analysis. In *3rd International Conference on WEB Delivering of Music (WEDELMUSIC'03)*, (pp. 71-74).
- Woon, W. L., & Lowe, D. (2001). Nonlinear Signal Processing for Noise Reduction of Unaveraged Single Channel MEG Data. In *Proc. Int. Conf. Artificial Neural Networks*, (pp. 650 -657).
- Hsieh, M., Tseng, D., & Huang, Y. (2001). Hiding Digital Watermarks Using Multiresolution Wavelet Transform. *IEEE Trans. Industrial Electronics*, 48(5), 875–882. doi:10.1109/41.954550
- Jin, C., Su, T., & Pan, L. (2007). Multiple Digital Watermarking Scheme Based on ICA. Proc IEEE 8th Int. Workshop on Image Analysis for Multimedia Interactive Services. 70-73.
- Johnson, N. F., Duric, Z., & Jajodia, S. (2000). *Steganography and Watermarking - Attacks and Countermeasures*. Information Hiding. Kluwer Academic Publishers.
- Nievergelt, Y. (1999). *Wavelets Made Easy*. Birkhauser.
- Ogden, R. T. (1997). *Essential Wavelets for Statistical Applications and Data Analysis*. Birkhauser.
- Painter, T., & Spanias, A. (2000). Perceptual coding of digital audio. *Proceedings of the IEEE*, 88, 451–513. doi:10.1109/5.842996
- Proakis, J. G., & Manolakis, D. G. (1999). *Digital Signal Processing*. Prentice-Hall India.
- Wang, Y., Doherty, J. F., & Van Dyck, R. E. (2002). A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images. *IEEE Transactions on Image Processing*, 11(2), 77–88. doi:10.1109/83.982816
- Wong, P. H. W., Chang, A., & Au, O. C. (2004). A Sequential Multiple Watermarks Embedding Technique. Proc. Int. Conf. on Acoustics, Speech and Signal Processing. 5. 393-396.

ADDITIONAL READING

- Delaigle, J. F., Devleeschouwer, C., Macq, B., & Langendijk, I. (2002). Human Visual System Features Enabling Watermarking. Proc. IEEE Int. Conf. Multimedia and Expo. 2. 489 – 492.

Chapter 8

Deterring Text Document Piracy with Text Watermarking

Rakesh Kumar Mishra

Feroze Gandhi Institute of Engineering and Technology, India

ABSTRACT

Protecting copyright of a digital content is gaining momentum and has been suitably complemented by technological innovations. Literature piracy, though not being given much attention, constitutes a major bulk. Unlike audio and video, text piracy is not complemented by IT solutions except for certain proprietary initiatives. This pursuit embarks on review of technological advancements for Text Copyright Protection along with issues and challenges for their implementation. Appraisal comprises of watermark embedding algorithms and distribution infrastructure. A brief discussion over the document structure, watermark composition and type, classification of algorithms and future direction is also being accomplished. To make approach holistic couple of systems were also studied.

INTRODUCTION

Communication network has expanded itself to new dimensions and now is available even to mobile users. The exponential growth of networks and its users has transformed Internet into a principal source of information dissemination. Transformation of the network from wired to wireless has made information distribution process a multi-fold complex activity. Insecure spaces appearing on account of the complexity are usually exploited by plagiarist

to make unauthorized accesses and detain data illegally. Plagiarism is a multimillion dollar illegal business and has affected every form of digital contents. Proactive measures against filthy attempts and protecting genuine ownership of authors are the foremost challenges to be ensconced by collaborative researches around the world.

Digital Rights Management (DRM) techniques are now surfacing strongly against plagiarism including Digital Watermarking. In watermarking a proprietary signal is incorporated into host at scaled down strength. Hiding proprietary mark within creations is differentiated from steganogra-

DOI: 10.4018/978-1-61520-903-3.ch008

phy and cryptography on the basis of relevance of received data to illegal recipient. A dummy host is visible to the interceptor in case of Steganography while cryptography scrambles data using key, hence forcing restriction over those who are key deficient recipient. Watermarking of literary resource is most ignored area (Fetscherin & Schmid, 2003) despite of known fact that text constitutes the largest share of Internet download traffic (Hurtung & Kutter, 1999). Text document image dissemination is a common phenomenon with growing number of “Open Archives and Digital Libraries”. These literary assets need to be secured against any misappropriation and right infringement. Watermarking techniques for images are very effective but can not be applied to text document images due to the inherent attributes and the mildest change to host becomes strongly evident. The only left option is to use available for data hiding.

Marking text document image can be classified into three dominant categories. Format marking on one side is of low capacity but on another hand is truly transparent. Space Coding is a variant of Format Marking where data hidden in form of varying spaces is semitransparent. Pixel flipping although ensures high density but is sensitive to noise. With all favours and odds there is a continuous research going on globally for a versatile technique for marking document images which capable of persisting across all media, formats and channel quality.

Next generation watermarking techniques for text document should be made compliant with some minimum standards. Presently, initiatives differ from one another severely and most of these are highly dependent of the language or the script being used. Another concerning factor is that none of the algorithm guarantee a reasonable data hiding capacity and its viability across formats and scripts. Key distribution infrastructure for deciphering the extracted watermark is still an undeclared infrastructure. After all sort of discussions and claims, the issues related to the file format for marked

document has not been decided yet; specifically the metadata content for the marked documents and the compression technique to be deployed for transmission. All-in-all a holistic approach for designing the coder, extractor, watermark and distribution infrastructure is required.

DIGITAL RIGHTS MANAGEMENT

Digital Rights Management (DRM) is a universal concern. The digital data once decomposed into binaries have same level of vulnerability as that of unsecured content. Legal framework has already been put into action, but once media converts to binary form all the proprietary marks can be eliminated with little effort, obviously using computers. Hence the answer to question “*to whom does this binary belong?*” remains a major encumbrance in citation of rulings against plagiarist.

DRM is a scaffold carved from paraphernalia spanning from standalone solutions to protocols designed as per regulation for upholding the rights of an Author. DRM implemented for digital documents is referred as Enterprise DRM i.e. E-DRM. The Association of American Publishers defines DRM as “*the technologies, tools and processes that protect intellectual property during digital content commerce*”. This is the most comprehensive definition encompassing all form of digital content including Image, Video, Text and Audio. Another definition by Einhorn (Fetscherin & Schmid, 2003) appears as “*digital rights management entails the operation of a control system that can monitor, regulate, and price each subsequent use of computer file that contains media contents like photos, video, audio or text.*” this definition describes a holistic characteristic of a DRM which not only helps in protecting the rights of the authors but also thrives for controlling the usage and securing the financial revenue of authors.

Early implementations of DRM trace back to 1996 with the DVD forum applying Content Scrambling System (CSS) over movie DVDs.

Companies working in domain of document editing and distribution standards soon developed their own variants like MS e-Book Reader, Acrobat Reader 6.0 and above. The security setting in these systems restrict recipient from having hardcopy or softcopy of the received file. Objective like Document Tracking, Monitoring, Authentication, Finger printing and labeling are not possible with these system which demands enhanced description of rights imparted to the legatee. To effectively incorporate essence of DRM into next generation of distribution and legal system governments of frontline countries like US, UK France etc have their own version of Digital Millennium Copyright Act (DMCA) that authorizes author to hide signature within the creation and assay to remove marks declared to be illegal.

Methods of Implementing the DRM

Putting DRM into practice commercially individual designer have achieved in different ways. The entire set of industrial practices can be bifurcated into hardware and software solutions.

Hardware Solutions

These solutions are based on the enforcement of security either in form of additional hardware or auxiliary chip. Peripheral hardware is connected externally to the system hardware at specific port to make product active. Hardwired protection mechanism has separate chip mounted over main circuit board as secondary chip. The technologies in the context are:

- **Dongles:** These are sub-units of hardware containing an electronic serial number that must be plugged into the computer system to run the software or the software itself senses it over a dedicated port. The full version of software activates only in the presence of hardware. Dongles are found

mostly in expensive high-end software packages.

- **Crypto-processors:** A dedicated micro-processor for carrying out cryptographic operations, embedded in a packaging with multiple physical security measures, which offers a high degree of tamper resistance. The purpose of a secure crypto-processor is to act as the keystone of a security sub-system, eliminating the need to protect the rest of the sub-system with physical security measures.
- **Bus encryption:** It is an encrypted program instructions on a data bus in a computer that includes a secure crypto-processor for executing the encrypted instructions. Bus encryption is used primarily in electronic systems that require high security, such as Automated teller machines, TV set-top boxes, and secure data communication devices such as digital police radios. Bus encryption distinguished from encrypted data transmission which does not require input of encrypted instructions.

Software Solutions

Within the skeleton of this approach soft-tools are designed and implemented for distributing, managing and maintaining the copies of creations. Some of techniques are as follows:

- **Product Activation:** Approach necessitates each copy of sold or installed software to be registered with the publisher using unique identification key. Unregistered products may not function at all i.e. product may not even startup or activates with deactivated essential functions like printing or backup, or activates a deprecated version. It is designed for restricting a special form of the piracy known as “Casual copying”.

- **Agent Based Restrictions:** Such solution installs a software component which is a terminate-and-stay type. The component keeps track of the user activities and restricts those activities that are threat to the protected content. The restriction, may be disallowing the copying of content for safeguarding the authenticity and integrity. Such solutions sometime lead to opening of trapdoors at user stations that may be exploited by any malicious software.
- **Platform specific Solution:** Data files i.e. the creations of authors like music file are encoded in specific form that requires a particular platform for representation of their contents. The data file's metadata specification contain the information pertaining to users or recipient rights. The behaviour of the host platform is decided by the rights encoded therein.
- **Digital Watermarking:** It an ancient thirteenth century approach being adopted by digital society for securing the content. Herein the recipient's authority is incorporated within the content itself instead of metadata part. It is a variation of the data hiding concept of Object Oriented Paradigm wherein the hidden data is totally inaccessible to rest of the code segment similarly in watermarking watermark remain imperceptible to human senses but traceable by the digital computers. The watermark is extracted digitally for the cause of data protection and rights invocation. (Wong & Memon, 1998)

Limitation in DRM Implementation

Early implementation flaws of DRM surfaced when Sony Rootkit alarmed internationally. The problem with realization was that it has bound itself with OS kernel and left trapdoor open for malicious software to intrude your system. Other implementations like 'iTune Stores' do have

success but failed to enforce the indispensable regulation of Copyright law viz Right of First Sale and Fair Use, another aspect associated was legal facet for interoperability among different players. DMCA has legalized the contamination of host thus erected barricade for undertaking the researches in the arena as any attempt to verify the robustness of embedding system or data invites an unnecessary legal action onto itself.

DRM connote security of content but in mean time it develops into enforcer by restricting the Right of First Sale and Fair Use sanctioned under Copyright Act. DRM confines rights associated with creation to publisher instead of author and enforces the ownership retention with the publishers even after the sale. Hence to make DRM products more effective, forum like US-ACM has laid down certain norms for compliance.

DIGITAL WATERMARKING

Watermarking is a practice of signal grabbing wherein the host content is contaminated with another signal. Tainting is done in such a fashion that the presence of contaminating signal is transparent to the recipient system. Mentioned characteristic of the technique proven to be an effective tool from point of view of DRM realization. It is defined as "*It is a technique of hiding a digital code irremovably, robustly and imperceptibly into a digital host data. Watermarking enables appropriate follow up action in case of suspected infringements of rights*". (Hurtung & Kutter, 1999)

Steganography and cryptography are two peers from security paradigm and are also the candidates for DRM implementation. Steganography uses the cover data to hide actual data; thus the stego-data becomes dominant while conveyed information becomes dormant. Similarly, cryptography transforms the actual data into an unintelligent form using a foreign component referred as *key*. Steganography and cryptography both refrains common user from accessing the content by adopting

pessimistic approach. These could not qualify for DRM as both techniques on the recipient end sends a unintelligent content that needs to be deciphered; contrary in watermarking host appears to natural and intelligent and the restrictions are enforced for its usage instead of accessibility.

Berghel & O’Gorman (1996) identified the issues that digital watermarking must conform to maintain the sanctity of a digital asset it becomes necessary such as

- It should bind tag with the digital content strongly enough so that tag could not be separated. It is recommended that presence of tag should not be known
- The hidden mark must survive all sort of modifications (attacks) applied to the digital content.
- The presence of the mark within the text must be transparent and should not affect the experience of viewing the image.
- It must be possible to segregate the hidden artifact from digital assets in limited space-time complexity.

Watermarking system is composed of three basic components namely the *embedding process*, *extractor* and the *watermark*. *Embedding Process* is entrusted with the responsibility of hiding a watermark robustly and imperceptibly into host. Watermarking technology defines two kind of embedding techniques: Coefficient based Technique and System based Technique. In coefficient based approaches either the pixel value is modulated or the transform coefficient values are modified. During embedding process unmarked host passes through perceptual analyzer block which defines possible sites for data hiding. These sites constitute the perceptual mask and hides artifact segments by spreading them across perceptual mask. *Embedding Process* may optionally be provided with key to further improve the robustness to embedding process. When a key is used the modulation is affected by key value.

Extractor on contrary does simply the reverse of the embedding process. An *extractor* receives a marked image and prepares for extraction. In preprocessing phase unnecessary contribution from the distribution and production channels are removed. Then the preprocessed signal is transformed into domain where the watermark is inserted and projected into signal subspace. This stage may optionally involve a key provided *Embedding Process* has used the key. Projected signals then analyzed for watermark presence and if detected watermark is decoded and produced or matched for claiming right over content. (Martin & Kutter, 2001), (Wong & Memon, 1998), (Perez-Gonzalez, & Hernandez, 1999)

It is necessary that there exists synchronization between two processes. Synchronization is performed with three different approaches: Invariant domains, Template and Self-reference. In invariant domain primarily frequency or wavelet domain transformation are used as these have better resistance towards certain specific kind of geometric translations. In templates the watermark is hidden as per specific distribution pattern. These predefine constellation of features act as the reference point where the signal is modulated. Templates are widely implemented within the commercial products. In self-reference approach the watermark by itself reveals its coordinates. A watermark could be anything from an image, a text string or a random binary sequence. It is small content which basically be used for proclaiming the rights. (Martin & Kutter, 2001)

WATERMARK COMPOSITION AND CLASSIFICATION

A watermark may be defined as “*a digital code irremovably, robustly and imperceptibly embedded in host data and typically contains information about origin status and / or destination of data. Watermarking enables appropriate follow up action in case of suspected infringements of rights*”.

Watermark is inserted into a host to establish the sanctity and integrity. Watermarking is performed to enforce discretionary access control which decides access to object of file system based on the identity and need-to-know of user(s) or groups to whom the object is transferred.

A watermark with a wide objectivity needs to be self explanatory and elaborative to serve the cause of its origin. A watermark is expected to contain the information regarding the owner and recipient of the content. Hence, a watermark may subcategorize into sections and each section contains information pertaining to its domain. The information that can be encoded into each domain will be:

- Identification of the author that uniquely identifies the author over the World Wide Web.
- Name of the author / publisher / recipient.
- Type of the host i.e. which kind of host the watermark is inserted to protect.
- Authorities – the rights that an author / publisher / recipient possess over the content
- Copy count – a decrementing counters that control the copy creation / number concurrent users and other operation of the sort.
- Cost – the price of the document.

Watermark Information and Constraints

Watermarks can be classified into eight different categories based on different designing techniques described below.

Content Information

Watermark needs to be designed in accordance to information it is required to carry regarding the permissions and rights being owned or delegated for each party. Other information like the third party infrastructure or tool requirement may also be incorporated. The level of disclosure must be

in compliance with the host capacity and type of embedding to be performed. The most desired design constraint is expressive and compact watermark. Either of desired attribute has inverse impact on its counterpart.

Content Type

Copyright information can be represented effectively by several mean which includes text, image or a binary key. Each mode of expression has their advantages and their effectuation is guided by capacity of host channel. Text is a descriptive mode of right expression where rights are fully expressed using natural language. Hence, the watermark is required to be disintegrated into different frames to cite rights owned by each party viz. the owner, sender and receiver. Image representing Copyright information is a one of the primitive form of ownership declamation. A watermark can be a logo, registered trademark, hologram or any other intelligent or unintelligent image. Image other than logo, registered trademark or hologram may also contain cryptic message that needs to be deciphered. Binary Key is a pseudorandom binary number sequence generated using characteristics or meta-specification of host. Binary sequence acts as hash key for a database defining the rights associate to individual party. This technique produces the smallest watermark that can be used for online digital libraries. (Carver, Yeo & Yang, 1998)

Host Derived

Watermark may be composed from the attributes of host document. Such watermarks may be useful in proving sanctity of document. It is most challenging to represent document attributes effectively and efficiently. Watermark needs to be small enough in comparison to host so that minimum redundant copies can be maintained. For a document host, information like number

of words, size of margin or number of paragraph may used for designing watermark.

Host Structure Directed

Host can be disintegrated into various constituent components as discussed in document structure and composition. Each media component being sublime channel has different level of tolerance and data hiding capacity and cumulatively defines the capacity of a host. Thus a watermark can be designed by analyzing the capacity of individual component and spreading the watermark according to the capacity of individual sub-channel.

Colouring

A watermark may be designed in various forms and format. Image watermark can be used for carving copyright information wherein the information can be hidden using colour values. Image watermarks can be classified in according to their perceptual appearance. An image watermark can be a monochrome, grayscale or coloured image.

Scrambling

To secure watermark it can be transformed into unintelligent form using any of the standard encryption techniques. Using encryption, even if a watermark is recovered cannot be deciphered ensure two stage security for the asset. Key infrastructure along with any standard cryptographic approach can be used. Since most of the cryptographic algorithms include error correction code, hence it relives extractor from error handling.

Sensitivity

A watermark is a precious artifact and the ultimate tool against piracy. Sensitivity refers to the ability of watermark to survive against different attacks and record the smallest alteration to host. Such watermarks may be hidden or visible. Sensitiv-

ity is directly proportional to binding strength imparted by embedding process and the ability of host to survive against attacks. Higher the sensitive of a watermark it will be more fragile. A low cost asset may be protected using a fragile version while valuable assets must be secured with highest robustness.

Perceptibility

A watermark can be visible or transparent to human visual system. A visible watermark is prominently used for declaring the copyright statement or any other phrase that conveys warning to the recipient. Perceptual watermark are provided with low cost assets but this form of watermarking sometimes may be annoying to users, especially with audio and video media. Visibility also reflects the quality of embedding performed. In such a scenario visibility may not be intelligent. Visible watermarks are counter balanced by hidden information within the host. Hidden or transparent watermarks are useful when owner wants certain restriction on usage, transfer, printing etc. to be enforced over the recipient.

Watermark Objectives

Sencar & Memon (2005), Perez-Gonzalez & Hernandez(1999), Schulzrinne et al, 1995, Martin & Kutter (2001) have discussed the usage of watermark in depth which can be clubbed together into following categories

Ownership Assertion

Ownership assertion is the foremost purpose of watermarking. In order to uphold the ownership a watermark needs to survive all form of tampering. To secure a content proprietary mark, either as image or text, is inserted into host object. In case of meddling with original or another object is created by illicitly inheriting the original copy,

present watermark can be extracted to claim the ownership.

Authentication and Integrity Verification

These are the most vital aspect and must be established beforehand to ensure that a purchaser has acquired an original version. Authentication proves legitimacy of multimedia content and integrity tests the intactness of content. With watermark it is possible to create ‘soft authentication algorithms’ that can measure degree of closeness with original content and may define degree of transformation an object might have suffered. The presence of different watermark other than the required one also indicates a misappropriation.

Asset Information

Watermark hidden within the host may be used to indicate the version of the asset. This is being used to distinguish different variants of same object published over a span of time. Information like time, date and place of creation or publication can also be a means of locating the asset. Watermark can also contain information peculiar to host containing the watermark. Such information may be used to prove the integrity of the concerned object.

Copyright Communication and Content Protection

Watermarking can be used to communicate the ownership, publisher’s rights and the permission to recipient for using the object. In case an asset is published in a public domain it becomes more vulnerable towards illegal copying and detention. To avoid the asset misappropriation visible watermarks are superimposed over the asset or hide within the object with visible warning to deter illegal copying. (Berghel, 1998)

Playback Control and Copy Protection

A watermark can define explicitly the number of times a multimedia object can be played or number of prints that can be taken. This can be utilized for pay-per-usage or test-n-pay business models. Watermark encoded with no-copy policy refrain a user from making copies of a document without procuring fresh version with copy permission.

Forensic Tracking

In this role a watermark record its path of propagation since it left the publisher archives. A watermark contains the reference of all or immediate predecessor host machine where it was residing. This is presently being implemented within certain class of digital cameras which embeds unique identification, date and time of creation of image during the acquisition itself. Wherever such images resides it is possible to trace back them to their producers. Similarly, in network environment hidden mark may contain the user name or IP address or MAC id of the computer to exhibit its binding to station whenever any claim has to be settled. It is sometimes also refers as *fingerprinting* because with each incidence of copying the traces of crime sites are incorporated. (Berghel, 1998)

Classification and Filtering Using Labeling

Labels are the hidden messages that annotates digital object. In medical applications labeling of images can eliminate hazardous diagnosis; similarly a label can be used to highlight a location within an image. Watermarks can be designed to include tags for the content of host. These tags may be used for classifying the content as per as given criterion, extending this to another dimension of content filtering. For example if all the images are watermarked with content tags before being published over network then it is possible to

design a filter that can discard images belonging to specific class.

Remote Triggering

Watermark can be designed as active or passive unit which will be capable of invoking action in case any illicit attempts are made. As an active unit a watermark can invoke a DRM module within the kernel of system. A watermark extractor located for the sign of tampering within watermark and once that has been located DRM module activates. A passive watermark can be a reference to a URL over a web which extractor accesses when tampering is detected. With remote triggering a trapdoor is opened at recipient side which may be exploited by owners or publisher.

DOCUMENT STRUCTURE AND COMPOSITION

Online archives are constituted from digital document and the digitized version of classical and proprietary contents. Digitization of hardcopy contents is done to create a non-perishable copy of the accumulated knowledge. Online Archives are assets maintained prominently by the Libraries, Universities, Research Organizations and Business Houses, to let people know about their achievements and expertise. These archives are the compilation of professional experience, surveys, product promotions and knowledge acquired by the organization during their operations globally.

Digitized Documents are preserved in specific file format. There are several file formats including proprietary formats like MS-WORD, PDF etc. besides these formats open document format is also gaining momentum. Open document format has long to go before getting stabilized and universally acceptable. The format needs to be capable enough to support the proper content presentation over every available editor. Schulzrinne, Paul et. al.,

(1995) discussed about three classes of document representation which are as follows:

- **Structural Form:** In structural form content portion are suitably tagged to express their presentation characteristic. This form of document representation allows a document to be rendered in different ways as per user preference and capabilities of output devices. Structural representation encourages the consistency of presentation and automatic processing. Client software typically browser parse the tags and text and develop the presentation in real time basis. The file in such format occupies the least space. Structural format includes LaTex, SGML (All form of markup languages)
- **Presentational Formats:** Herein the document specifies where and when a character, graphical element or any other constituent will appear on document canvas. Main advantage with such systems is that it abstracts the device details to be used for presentation. Documents in such format are read-only but scaling and font substitution can be performed by proprietary client software. Portable Document Format, Page Description Language, Tex and Troff also belong to this category.
- **Bitmap:** Document pages may be stored as bitmap images and are compressed to make their size affordable. This document presentation technique requires a lot of computation during real time communication in decompressing the content. It is in this format hyper linking is bit tedious as linking become more spatial than content based. (Schulzrinne, Paul, Maxemchuk & Choudhury, 1995)

As far as their usage and valuation is concerned, bitmaps are more secure than any other format because removal of watermarks is not as simple as it can be in other formats. Similarly, document in

structural format have more value than other two formats. Presentation format supports the platform independence by abstracting higher order details.

A document is, for all intents and purposes, a combination of various components spreading coherently across its dimensions. The major constituent components of a document are

- Background with reference to the text document is the page colour which is usually white. The colour and texture of the page is the primary component of the file. The complexity of colour patterns and richness affects the size of the file format.
- Image and Figure in our purview are two distinguished objects. Figure is an object which shares the same canvas as that of the file background whereas, Image is an external object which has its own background canvas different from the document. A Figure may be a monochrome line chart, scientific sketches, schemas and other free hand diagram to explain the context referred within the text. Image is included as exhibit like photos of devices, landscape, experiment samples and results etc. Extracting or identifying a figure from a document is more complex and computation intensive task than image.
- Content is the literature written in a language and with specific font within the document file. Content usually have its own distinguished font (Theimert, Steinebach & Wolf, 2006) (Aabed, Awaideh et al, 2007). A font thus becomes an important component and some time even proprietary. Font along with the subject also becomes asset to be preserved. A literary content is appreciated by the quality and message or findings contained therein. Hence reflect the valuation of the document. The support for every font of each language is a difficult task and thus has to be imported before viewing the document.
- Content Format is referred as how the content is organized within a file. The text within the file is organized into several structural components like header, footer, titles, end notes, footnotes etc. has its specific position and appearance in the document where as column, paragraph, lines word and characters constitutes the content. Characters act as basic underlying entity usually used for watermarking. Character groups separated by intra-line space constitute the words which in turn composes a line. Words and line together form a paragraph. The content so composed may be vertically separated by inter-column spaces forming multiple columns. (Mishra, 2007), (Mishra & Raghuvansh 2009)

Profiling

A profiling is a projection of a two-dimensional array onto a single dimension sub-array. A profile is an integer-valued vector that contains the information about the relative location of text in an image. (Brassil et. al. 1994) Mathematically, can be defined as

A page image is represented by a two-dimensional array with elements as

$$f(x,y) = \{0,1\} \quad x \in [1,W], y \in [1,L] \quad (1)$$

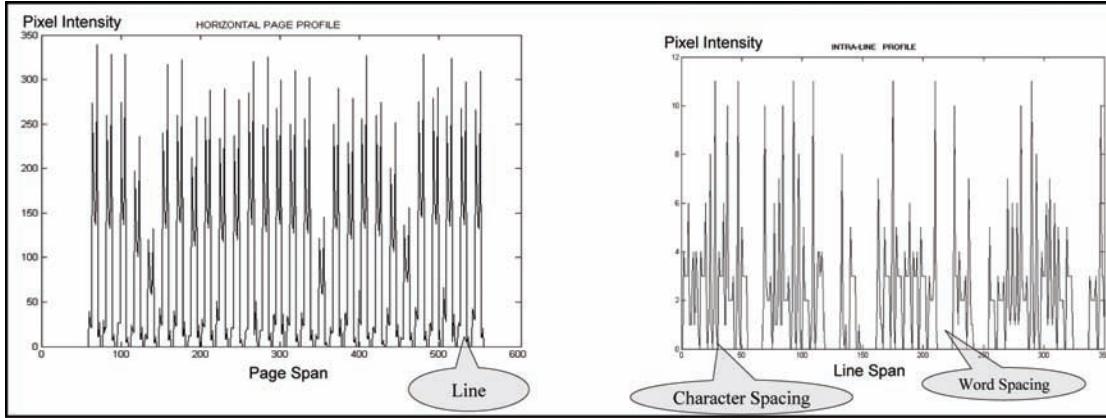
where $f(x,y)$ represents the pixel intensity at position (x,y) , W and L is the width and height of image.

Horizontal profile of the sub-array such that $y \in [t,b]$, bound $[t,b]$ are the dimensions of document sub-image, containing the text line is

$$h(y) = \text{SUM}(f(x,y)) \quad x \in [1,W] \quad (2)$$

Vertical profile of the sub-array such that $x \in [0,W]$, containing the text line is

Figure 1.



$$v(x) = \text{SUM}(f(x,y)) \quad y \in [t, b] \quad (3)$$

The map of the profiles are given below in Figure 1 to illustrate the interpretation of profiles discussed.

Document Spatial Model and Feature Extraction

Considering the description of the document given above here is defined model to extract various features of a document. A document image presumed to contain neatly formatted and equi-spaced constituent components. Images and Figures are not considered and source is free from noise. Let us represent image of a document image as $f(x_{ij}, y_{ij}) \in \{0,1\}$ where $i, j \in N$ & $i, j \neq 0$, $d(x_1, x_2)$ is a distance between components x_1 and x_2 . A line may be defined as

$$L_i = \{\{l_i\} \mid i \in [1, fz] \text{ & } fz \geq 8 \text{ & } l_i = \sum f(x_{ij}, y_{ij}) > 0 \text{ & } j \in [1, w]\} \quad (4)$$

where w is width of text line, fz is font size in pixel. Deriving the document as a set of lines as

$$D = \{ L_i \mid d(L_i, L_{i+1}) \geq t_1 \text{ & } i \in [1, n_l] \} \quad (5)$$

where $n_l \in N$, n_l is total number of line and $n_l > 1$ and t_1 is minimum threshold value for distinguishing the lines. Paragraphs are collection of lines separated apart by a larger threshold of $t_2 > t_1$. Let us define L_{ij} is a j^{th} line of i^{th} paragraph p_i hence

$$p_i = \{ \{L_{ij}\} \mid L_{ij} \approx L_{i(j+1)} \text{ & } j \in [1, n_x] \} \quad (6)$$

where n_x is total number of lines in a paragraph and $n_x << n_l$ and \approx is a relation such that if a, b are two entities then

$$a \approx b = \{ b \mid b \sigma a \text{ & } d(a, b) \geq t_1 \text{ & } d(a, b) < t_2 \} \quad (7)$$

where σ is a successor function. Following from (6) and (7) we have

$$D = \{ p_i \mid p_i \sim p_{(i+1)} \text{ & } i \in [1, n_p] \} \quad (8)$$

where n_p is the number of paragraph in a document page and $n_p > 0$ and \sim is relation such that

$$a \sim b = \{ b \mid b \sigma a \text{ & } d(a, b) = t_2 V d(a, b) = 0 \} \quad (9)$$

Similarly, words and characters may be defined as

$$L_i = \{ \{w_{ij}\} \mid w_{ij} \sigma w_{i(j+1)} \text{ & } d(w_{ij}, w_{i(j+1)}) \geq t_3 \text{ & } j \in [1, n_w] \} \quad (10)$$

$$W_i = \{ \{c_{ij}\} \mid c_{ij} \sigma c_{i,(j+1)} \text{ & } d(c_{ij}, c_{i,(j+1)}) \geq t_4 \text{ &} \\ d(c_{ij}, c_{i,(j+1)}) < t_3 \text{ & } j \in [1, n_c] \} \quad (11)$$

where w_{ij} is the j^{th} word of i^{th} line, t_3 is the threshold defining the inter-word space while t_4 is the threshold for intra-word space, $t_3 >> t_4$, n_w and n_c are the number of words in a line and number of symbol in a word. (Mishra, 2007)

TEXT WATERMARKING ISSUES AND CHALLENGES

Text watermarking hides a foreign message imperceptibly within the host such that actual and modified content remains nearly identical. It is significantly different from steganography where actual data is hidden within dummy coverage. It is still a maturing field and researches are on to improvise more and more robust technique. Like any other domain here also exist certain hindrances that have to be overcome before final implementations. Some of the major issues are discussed in succeeding paragraphs.

Readability

This is a metric related to human vision system. It refers to quality of text obtained after being populated by the foreign components. Since text document contains limited number of features to exploit, therefore a smallest change to content get revealed magnificently. This raises serious quality concerns for the image or document content. It is also sometime referred as the imperceptibility of hidden data. In order to ensure the readability of the document it is necessary that watermark bits are inserted sparsely in a random fashion so as the predictability of hidden data bits become tedious task. Major challenge associated with the approach is ability of watermark has to persist across all form of media and plagiarist attack.

Document Structure

Structure of a text image or document format comprises two major constituents viz. print and space area. Print and Space Areas are the only places for hiding the data. Print area may be colourful but composed of fractals forming the font whereas space area contains background colour and texture. The print area has characters as prime component for data hiding where watermarks bit can be coded.

Other meta-components like word line paragraph etc are also available but as we move-up along abstraction tree the data hiding capacity reduces considerably. Similarly, the spaces like intra or inter word spaces have the largest potential for data hiding in comparison to line word or paragraph spacing. Both components viz. space and print areas do not provide adequate capacity for message hiding. The capacity to hide watermark also greatly influenced by the density of print area because as the number of characters reduces the space area increases which is highly susceptible to the modifications.

Language

It is the logical component of the literature that imparts relevance to the content and identifies the importance of text image or document. Around the globe thousands of languages are in use and almost in every language literary creation do exists. The two main constituents of any language are

Grammar

It is assumed to be a rulebook to express meaningfully using a language. It dictates how to narrate expression and compose the literature. Each language is having its own grammar except for entities like noun, verb etc. nothing is common between any two languages. Further, there is no minimal grammar that is applicable to all the languages. Watermarking using the grammar mainly

restructures the text line or sentence keeping the actual meaning intact. For example ***I have the book*** and ***I have the ‘book’*** have different meaning based on the context used. All such alteration has to be done in a predefined manner such that during the deciphering phase the actual content can be retrieved without errors.

Characters Set

These are the elements for constitution of words for a statement in any language. Each language has its own unique character set being represented distinctly. The fonts representing these characters are the main spots for the data hiding. The strokes and appearance of characters in a font are the prime components that are modulated for data hiding. The strokes and appearance of characters actually defines the channel capacity for example a plain English text has a lower capacity in comparison to Arabic that has a larger set of features to hide watermark. Accurately assessing the font features is main challenge in a language for example Arabic where additional strokes, that do not impart any additional meaning or are optional, can be added to make text artistic. A data hiding technique relying over characters set for watermarking has to consider these modifications to the characters written using font, as these have impact over the readability and presentation of message.

Watermarking Information

This is a copyright message which an author or publisher includes within the host. It can be a text message stating rights a legatee have with content copy or URL refereeing to a specific web page or a logo image. Watermarking Information is assumed to be comprehensive enough to enable the owner to claim his/her right over the document. What will be the minimum information a watermark should contain still remained unanswered. Another perspective may be how an owner(s) wants to use

their watermark for entire spectrum of applications including authentication, tracking and labeling.

Copyright regulation varies from country to country though caters to same objectives but their priorities for copyright protections are different. In proprietary system owner defines their own mechanism for ensuring sanctity of asset but that varies slightly from national copyright agenda of their host nation. Other general aspect like usage rights needs to be included within a watermark. The information size and the security issues associated with watermark affect its ultimate size. With restricted capacity of host this posses a major restriction for an embedding process.

Channel Capacity

This refers to the amount of data that can be hidden within the text document. A channel within a document may be graphical unit or a textual unit. In case of block-wise coding a block is a channel and in text mode characters, words lines paragraphs etc are the channel which can be exploited for hiding the artifact. The attribute a channel includes Colour Space, Text density, Page Layout, Page composition etc. As the Colour Space or any other attribute becomes sparse the net capacity of the channel also gets affected significantly.

Asynchronous mode of detection is more suitable for a document distribution system instead of a synchronized one. In order to comply with asynchronous detection, only a fraction of available capacity is used and a significant amount of space is left untainted for the extractor. These unused spaces are used by extractor to locate for the modified areas within host and recognize the bit embedded, otherwise it requires an original copy to extract the information.

Persistence

This is a characteristic that defines the robustness against all form of media transformation. A literary document may exist in different form of media

from digital to hardcopy, from secured literature to open access libraries. It is desired that a hidden artifact should be carried effectively against all odds from host to destination.

The import and export of document from one format to another is a common phenomenon this posses major challenge because if any sort of modification is done to the document in one format may not necessarily copy to the other. For example if the font feature is modified to encode the watermark, during the export either the font reference is passed between the applications or their equivalent fonts are automatically picked up. As a result in both scenarios the changes carried out do not migrate to the other application. The exported document is free from the watermark. It is mandatory that the artifact should remain within the source and this requires support for copyright protection in one or other form in every text authoring tool.

Another situation may be that a watermarked document is printed and scanned back to digital form. In this circumstance noise will be included within the host due to faulty printer or low quality scanner. This noise will be adding extra components within the text document and the extractor should ignore these false sites during the extraction process and recompose the watermark. Watermark so extract should be of good quality that can be used for legal purpose.

Watermarking Techniques

Document Content has remained the most precious information that a data hiding algorithm exploits. Each language has its own script and formatting and these two features are mostly modified for data hiding. Adding fixed number of pixel in a specific direction of strokes or changing the space distribution along the page or a line are the common approaches. As a consequence of this each implementation becomes unique and sometimes do not share a single aspect of decision making for hiding watermark. For example Chinese and

English characters both have different font appearance and scripting style. In English, the horizontal strokes are least contrary Chinese characters have horizontal and diagonal strokes that appear in equal proportion to vertical strokes. Another striking difference is that Chinese character set also includes compound characters; these have originated by the combination of simple character in a particular ordering whereas English do not have any such provisions. Similarly, Arabic is an artistic language and has several elements that are included but have no impact on the readability of document like Diacritics whereas in Indian sub-continent languages like Hindi and other dialects have half characters which are unique feature these languages.

To enable a watermarking algorithm to be effective against all sort of variations in content appearance, it is required that algorithm marks the content independent of its features. A unified approach needs to be developed that can cope up with all form of scripting fonts and formatting.

Pricing and Complexity

These are two different correlated aspects where first is purely financial and other is technological. The binding factor between them is that these influence each other. Pricing of a solution is an issue that decides its acceptability to wide range of audiences. To keep prices under control DRM implementation may come in various versions to cater the different level of accessibility restriction to over the asset. The objective of pricing factor is to keep the cost low in comparison to procuring illegal copy and removing the watermark from therein. There are fewer publishers than the readers thus user of DRM enforcing module are more than DRM encoders, making the decoders available for free like Adobe Acrobat Reader also encourages users to obtain the legal copies.

Next generation of computing is of *Mobile Computing* where the users with portable devices are accessing the resources. As these are resource

constraint devices hence requires the DRM solution to be least complex with reference to time and space requirement. Thus there is a need for a simple but robust system that can efficient across all platforms.

Codification of Regulations

'Right of first sale' and *'Fair Use'* doctrines are the main concern and the problem is how to implement in digitally marked assets. Doctrine of *Right of first sale* allows the purchaser to transfer a particular lawfully procured copy without the permission of the authors. This means that watermark of both author and seller needs to be coded such that latter do not damage the earlier mark. Similarly, it is essential that both watermarks can be retrieved successfully. In perspective of stated problem marked copy can be codified recursively many times, with small channel capacity this remains a problem.

Another policy that must also be supported is the openness of system for review and technological evaluation. This refers as *'Fair Use' Doctrine* which allows the limited use of copyrighted material without requiring permission from the rights holder. This demands a mechanism to distinguish user with filthy intentions from the reviewers and evaluator who will contributing towards the improvisation.

Watermark Standardizations

Standardization needs to be defined in every aspect of watermarking from watermark creation to encoding and from decoding to deciphering the rights. As all the efforts being mutually exclusive and have been in isolation, hence are specialized variants. An integrated approach is required from the beginning of watermarks designs, encoding-decoding algorithms to dissemination infrastructure. (Mintzer, Braudway & Bell, 1998), (Sheppard, Safavi-Naini & Liu, 2003)

Various metrics needs to be established so that the improvements can be quantitatively and qualitatively be measured and benchmarks can be decided. An exclusive format for document representation and interoperability among the proprietary solution is mandatory.

BACKGROUND: WATERMARKING ALGORITHMS AND TECHNIQUES

It is customary to first revisit the development in watermarking of the text documents and assess the various algorithms being implemented. A document is a high contrast image where every boundary is sharp and scanning and printing adds noise. A watermark, not the regular component of the document, may appear as noise and needs to be preserved in all form of dissemination. It was observed that certain implementations are designed specifically for a language, the best document format for hiding watermark is the image and the pixel flipping technique is the most versatile as a watermark embedding is independent of the language and formatting of the document. The pitfall will only be the computational complexity as the next generation of document access will be from limited resource devices like mobile phones or PDA etc.

This section is divided into two parts the first part is the review of various algorithms and approaches while the second part discusses couple of practical implementation of system employing watermarking as their essential component of delivery system.

A Revisit to Past

The approaches deployed by inventors can broadly be classifying into five categories namely Pixel Intensity Modulation, Block-wise Coding Scheme, Font Feature Coding, Character Displacement and Diacritics Coding and Space Modulation. The utilization of host documents capacity for data

hiding is not optimum in all the cases due to the very nature of document itself, high density coding scheme remains a challenge and incorporation of error correction code without sacrificing the payload is another area where all the algorithms needs to improve. The review of past initiatives is as follows

Pixel Intensity Modulation

Bhattacharjya & Ancin (1999) have proposed an algorithm wherein the change in luminance of adjacent cells is made used for data hiding. The technique has its role for very high resolution photo copying system. This technique uses the scanned image of the text document as input and embedded the watermark message.

The technique comprises of following phases

1. Image Segmentation phase primarily segregates the text and non-text portion within the image using luminance tests and morphological filters.
2. Connected Component Labeling and deskewing phase extract the various components of the documents namely the paragraph lines word characters etc. and individually label them. Orientation of the page is corrected with the help of the Hough-transformation.
3. Block Identification and site selection is performed to locate the regions for data embedding. Entire image is transformed into a grid of 3x3 pixels and the grid cells which contain the text components are elected for insertion. Another approach used was the identification of character strokes using morphological operator.
4. Watermark Message encoding and scrambling is performed to enable uniform message spreading over the content.
5. Embedding is performed by pixel luminance value modulation which extracted back by retracing the process using high resolution scan. The bit is said to be one if the

difference between the luminance factor of three adjacent grid cell is positive the bit is one else it is zero.

Oh & Kim (2004) has proposed an algorithm for grayscale document images. Authors have implemented the algorithm with Korean text images and coded the information by modifying the intensities at different location. As a consequence of the embedding process the edge density improves at certain directions and this is simultaneously complimented by reducing the edge density in other direction. The method of creating the conjugates helps in locating the errors during deciphering phase.

Algorithm

1. The space is divided into 16 bins where bin 0,8 represented horizontal strokes and 4,12 represents the vertical stroke direction, rest of the direction are referred as diagonal direction.
2. If the intensities of a pixel is greater than the threshold then it will be included into appropriate bin. Bin so created by accumulating the pixel values are normalized such that the sum of all values is unity.
3. Embedding process keep certain blocks unaltered and called as *mother-blocks*.
4. If the bit to be inserted is zero the contaminated block vary from *mother-block* by *0-style*. A *0-style* is nothing but increasing edge along bin 2, 10 and simultaneously reducing from direction 1,3,9 and 11. Bit 1 varies by *1-style* coding where bin 6, 14 are enhanced while 5,7, 13 and 15 are diffused.
5. Knowing the position of *mother-blocks* and the change in the histogram of coded block reveals the bit hidden.

Block-Wise Coding Scheme

Chen, Pan & Tseng (2000) (CPT) proposed an algorithm that was one of the unique in the sense

that it can be effectively implemented for both the binary images as well as the text documents. Authors embedded the data within the host by flipping the pixel value at the specific location. Weight Matrix and the key matrix are the important component of the embedding process. Weight matrix is random matrix of integers comprising of values between $[1 \dots 2^r]$ where ' r ' is the number of bits to be inserted per block. Key is secret bit map, which act as mask for the actual image. The key and weight matrix is shared among the sender and receiver. This scheme encodes $\log_2(mn + 1)$ bit per block and robustness is solely decided by the secrecy of the Weight and Key bitmap. Scheme works as follows

1. Assumptions:
 - a. F: is host image and is partitioned into the blocks of mxn hence its size is in multiples of mxn . F_i is the i th block of the host image.
 - b. K: is a secret key shared among the sender and receiver and is randomly selected bit map of size mxn .
 - c. r: is the number od bits to be inserted per mxn size block. It follows the invariant $2^r-1 \leq mn$
 - d. B: is critical information of kr bits where k refers to number of mxn blocks of host image F.
 - e. W: a secret weight matrix shared by the sender and receiver. It is an integer matrix of size mxn . It can contain values in the range $[1,2,3,\dots 2^r-1]$ such that each value is atleast appear once.
 - f. The Key and weight matrix are of the same size viz. mxn and the host image comprises of k number of such blocks.
 - g. $b_1 b_2 .. b_r$ binary number for the message to be inserted.
2. Operator used for the manipulation of host block, key image and weight matrix are
 - a. Bitwise XOR operator \oplus is used to perform masking of host image with

reference to key. This will help in obtaining a matrix that reflects the dissimilarity between the key and the host matrix.

- b. Pair-wise Multiplication operator \bowtie is a matrix multiplication operator that multiplies the identically positioned element in two matrices.
- c. Matrix sum operator SUM aggregates the value in a matrix.
3. Invariant is equations which act as pivot for embedding the information as well as deciphering the same. Invariant in this scheme is

$$(\text{SUM}((F_i \oplus K) \bowtie W)) \bmod (2^r) = b_1 b_2 .. b_r$$

4. Algorithm
 - a. Computes $(\text{SUM}((F_i \oplus K) \bowtie W))$
 - b. Create Matrix
 - c. Compute $d = b_1 b_2 .. b_r - (\text{SUM}((F_i \oplus K) \bowtie W)) \bmod (2^r)$
- If $d = 0$ then do nothing
 Else if $d >= 0$ flip pixel of F_i to reduce the sum
 Otherwise locate of twin coordinate that compensate effect.

Wu & Lee (1998) have proposed a block-wise data embedding technique. Host image is fragmented into the smaller blocks of equal size. The size is determined by the size of the key matrix. Key matrix used for masking host image block and at most only one bit of the watermark message is inserted into the block. Main emphasis is to hide the bit at the position where mask bit is high. Unlike CPT it does not require any weight matrix and efficiently filter outs the blank portion of the image whether pure black or pure white. Algorithm-wise it is straight forward and less complex, also it only requires the key matrix

to be shared between the sender and receiver. Algorithm follows as

1. Assumption
 - a. F is host image and F_i is host image block of size $m \times n$. F has exactly k blocks of the image.
 - b. K is the key matrix of size $m \times n$.
 - c. $\&$ is bitwise AND operator and $\text{Sum}(q)$ adds all the elements of the matrix.
 - d. b_i is the bit of watermark message to be inserted.
2. Invariants are the conditions that have to hold true in all cases. These are
 - a. $0 < \text{SUM}(F_i \& K) < \text{SUM}(K)$
 - b. $\text{SUM}(F_i \& K) \bmod 2 = b_i$
3. Algorithm
 - a. Partition F into blocks of size $m \times n$
 - b. Foreach block compute $0 < \text{SUM}(F_i \& K) < \text{SUM}(K)$ if this holds then proceed else leave the block.
 - c. If b_i is the bit to be embedded then
 - i. If $\text{SUM}(F_i \& K) \bmod 2 = b_i$ then do not change the block
 - ii. Else If $\text{SUM}(F_i \& K) = 1$ then pick $[F]_{i,j,k} = 0$ and $[K]_{j,k} = 1$ then flip $[F]_{i,j,k}$
 - iii. Else If $\text{SUM}(F_i \& K) = \text{SUM}(K) - 1$ then pick $[F]_{i,j,k} = 1$ and $[K]_{j,k} = 1$ then flip $[F]_{i,j,k}$
 - iv. else pick $[F]_{i,j,k}$ and $[K]_{j,k} = 1$ then flip $[F]_{i,j,k}$
4. Extraction – Compute $\text{SUM}(F_i \& K) \bmod 2$ to reveal the bit b_i of message, where F_i is the encoded block.

The algorithm suggested by Pan & Tseng (2001) was devised from the drawbacks of CPT method. In CPT method bits were flipped on the basis of the difference between the bits inserted and the aggregate of the weighted values of Xored image and key block. This approach compromises the quality of watermarked image with data hiding capacity; sometime bits are flipped in a region

where adjacent bits are already in reverse colour. To cater this deficiency authors have redesigned the weight matrix which in this case is sequence of even an odd numbers instead of mere random integer matrix. The next enhancement is towards the computation of the distance matrix which computes the distance of nearest pixel with complemented value; flippable bits with smallest distance are the candidates for data hiding.

Major modifications in comparison to the CPT are

1. Invariants in this method modified to
 - a. $\text{SUM}((F_i \& K) \text{XOR } W) \bmod 2 \Rightarrow \text{SUM}((F_i \& K) \text{XOR } W) / 2 \Rightarrow b_1 b_2 .. b_r \pmod{2^{r-1}}$
 - b. $(\text{SUM}((F_i \& K) \text{XOR } W)) \bmod 2 = 1 \Rightarrow$ there is no hidden bit.
where F_i is encoded block
 - c. On receiver side $\text{SUM}((F_i \& K) \text{XOR } W) / 2$ is the hidden bit such that F_i is not completely blank or black and $\text{SUM}((F_i \& K) \text{XOR } W) \bmod 2 = 0$.
2. Data structure modification
 - a. Weight Matrix
 - i. Earlier contains elements in range $[1 - (2^{r-1})]$ here it is $[1 - (2^{r+1}-1)]$ where 'r' is the number bits of the message to be inserted in each block.
 - ii. In each 2×2 sub-block contains atleast one odd number hence it is no more a random integer matrix $[1 - (2^{r-1})]$
 - iii. In case of no bit is to be inserted in a block and its SUM is even then $[F]_{x,y}$ is flipped such that the corresponding weight in weight matrix is odd and distance is minimum.
 - b. Distance matrix is altogether a new data structure introduced which is an integer matrix of the same size as F such that

- i. $[dist(F)]_{ij} = \text{forall}(x,y) \min(\sqrt{(i-x)^2 + (j-y)^2})$
such that $[F]_{ij} \neq [F]_{xy}$
 $[dist(F)]_{ij}$ is the distance from $[F]_{ij}$ to the closest element $[F]_{xy}$
such that the complement of $[F]$
 $_{ij}$ is equal to $[F]_{xy}$.
 - ii. The threshold distance for the flappable pixel is $\leq \sqrt{2}$.
3. Weight difference which previously calculated as $d = b_1 b_2 \dots b_r - (\sum((F_i \ominus K) \otimes W)) \bmod (2^r)$ modified to $d' = (b_1 b_2 \dots b_r) - (\sum((F_i \ominus K) \otimes W)) \bmod (2^{r+1})$.
4. Pixel coordinates that are the candidates for data hiding are evaluated as

$$Sw = \{(j,k) | [W]_{jk} = w \text{ \&\& } (F_i \ominus K)_{jk} = 0 \text{ \&\&} \\ [dist(F)]_{ij} \leq \sqrt{2} \text{ } || [W]_{jk} = 2^{r+1} - w \text{ \&\& } (F_i \ominus K)_{jk} = 1 \\ \text{ \&\& } [dist(F)]_{ij} \leq \sqrt{2}\}$$

5. Algorithm modification

- a. Blank and black host image is ignore
- b. Coordinates of pixels that are candidates for data hiding (4) is evaluated for each weight $w = \{1..2^{r+1} - 1\}$
- c. Difference of weight is computed as stated in (3)
- d. In case block do not qualify for the data hiding and invariant (1b) donot holds then image block pixel having corresponding smallest odd weight with minimum distance is flipped.

Wu & Liu (2004) have proposed a blind data hiding techniques which will be capable of making watermarked copy sufficient evidence against illicit copying. The technique uses a novel method of block-wise pixel flipping. Method comprises of three different stages where in first stage pixel flipability score is computed in second stage data is embedded into the host and in last stage the data embedding density is maintained uniform in each cell.

In the pixel flipability computation stage the flipability score of each pixel is evaluated. The boundary pixels are selected for the image to be flipped. The score value varies between '0' to '1' where '0' indicates no flipping. To assign flipability score the metrics like smoothness and connectivity were used. The smoothness measured by horizontal, vertical and diagonal transition in a local window and the connectivity is measure by number of black and white pixel cluster.

To compute the smoothness following expression were evaluated

$$\text{Horizontal } N_h(i,j) = \sum(\sum(I(p_{i+k, j+l} \neq p_{i+k, j+l+1}) \forall l \in [-1..0]) \forall k \in [-1..1])$$

$$\text{Vertical } N_v(i,j) = \sum(\sum(I(p_{i+l, j+k} \neq p_{i+l+1, j+k}) \forall l \in [-1..0]) \forall k \in [-1..1])$$

$$\text{Diagonal } N_d(i,j) = \sum(I(p_{i+k, j+l} \neq p_{i+k+1, j+l+1}) \forall l, k \in [-1..1])$$

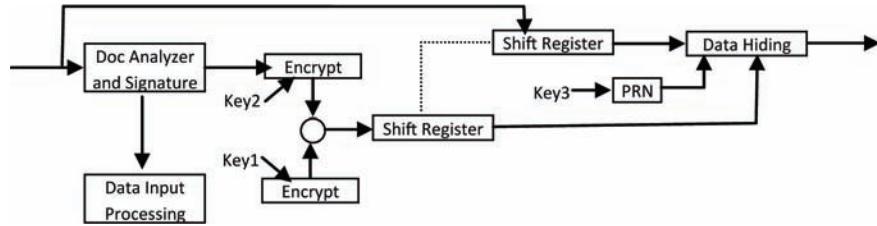
$$\text{Anti-Diagonal } N_{ad}(i,j) = \sum(I(p_{i+k, j+l} \neq p_{i+k-1, j+l+1}) \forall l \in [-1..0], k \in [0..1])$$

where as the connectivity is computed using the diagonal and horizontal pixel states which constitute 90° , 45° (4 way) connectivity. Both 90° and 45° connectivity together constitute the higher 8 way connectivity.

Algorithm:

1. For each local window the connectivity graph is formed may be comprising of 2 or more disjoint trees. The graphs are created for both black pixels as well as the white pixels.
2. The flipability scores is computed for each block through horizontal, vertical, diagonal and anti-diagonal navigation along with increase and decrease black and white cluster count.

Figure 2. [Quadir and Ahmad (2005)]



3. The minimum distance is maintained between two flipable pixels by sliding the window over adjacent cells.
4. As each block has different flipable pixel count and hence have varying data hiding capacity. To normalize the capacity shuffling is performed using a shuffle table and constraints like blank blocks should not receive any weight.
5. The embedding mechanism hides the data in the pixels with higher flipability count. The count of black pixels was maintained to even to indicate that hidden bit is zero and count becomes odd to accommodate bit '1'.

The probability of error reaches to 0.5 the detector starts giving higher false-positive error. To circumvent the problem boundary coding technique was deployed by making registration marks and enforcing restriction on the image size factor.

Quadir & Ahmad (2005) have proposed a complete infrastructure framework for dissemination of document over the network. The prime objective was to design and develop a robust and imperceptible watermarking scheme that can cater to need of copyright protection, integrity preservation, labeling, monitoring etc. The characteristic of the scheme was that under the influence of the attack the host content should also be substantially destroyed. Authors in their proposed document dissemination model include three parties the first is owner who approaches a trusted party for asset registration and receive a registration code. The size of the registration code is decided by the characteristic own by the host channel. Watermark

is obtained by owner conforming to restriction enforced by the registration code. The watermark is embedded and maintained by the third party who will be arbitrating in case of any violation of rights is reported (Figure 2).

In the proposed system the data bits are imperceptibly hidden by manipulating the information within the characters of the text such that overall structure of document does not change significantly. The system component works as

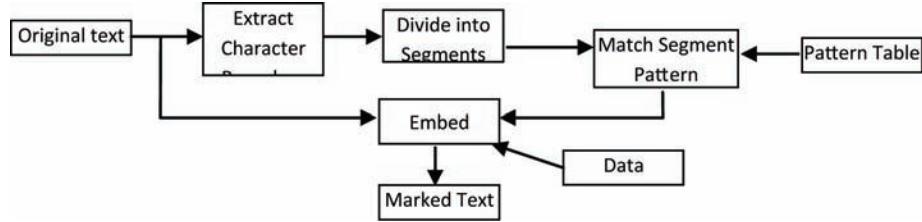
1. Raw text is processed by Document Analyzer and Signature creator and returns watermark size and document signature.
2. Knowing the watermark size a user watermark is created by Data Input Processing.
3. Signature and Watermark of the document the encrypted using two different keys say Key1 and Key2.
4. Encrypted Signature and Watermark are spread over a pseudo noise. Let it be called as processed watermark.
5. Processed watermark then inserted imperceptibly into the document using key Key3.

Embedding process is reversible with the need of original document. The tampering or originality of text can be established even with the smallest trace of the watermark.

Font Feature Coding

Mei, Wong & Memon (2001) propose a feature coding algorithm wherein pixels are set or reset using a congruence table. It is also a feature coding

Figure 3. [Mei, Wong and Memon (2001)]



technique performed in the way of pixel flipping. A set of patterns of 5 pixels are maintained in a lookup table and the data is embedded in a boundary of a character which is 8-way connected. These pattern pairs are dual of each other i.e. a flipping a pixel adjacent to central pixel will convert one pattern to another. The pattern for which pixel is added to convert it into its dual is called as the *A-patterns* (Add-pattern) and the other is called as *D-pattern* (Delete-pattern)

Assumptions taken in the algorithm are

1. Each of the five consecutive boundary pixel do not touch any pixels in boundary segment other than one immediately preceding or following it.
2. Pattern pairs removed from the lookup table are
 - a. Boundary segments that do not preserve length after addition or deletion operation.
 - b. Straight line segments
 - c. Boundary segment with 90° degree corner

Algorithm as follows:

1. Patterns are stored in a lookup table called *pattern table*.
2. Image is scanned in a left-right and top-down manner
3. Connected components are extracted representing character or other symbols in text.

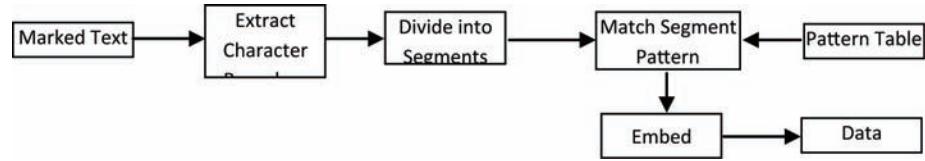
4. for each connected component
 - a. 8-connected boundary is used to obtain the closed outer boundary of the connected component.
 - b. Outer boundary is then traversed in clock-wise direction. To generate 5 pixel segments
 - c. Segments is matched with the pairs in pattern table
 - d. If the segment is valid then
 - i. If the bit to hide is '0' and pattern is *A-pattern* then pixel is flipped otherwise no change is done
 - ii. If the bit is '1' and pattern is *D-pattern* then pixel is flipped otherwise no changes are made.

Schematics for encoding and decoding can be given as in Figures 3 and 4.

The proposal by Theimert, Steinebach & Wolf (2006) addresses the concern of firms which use their own proprietary fonts. Such organization to maintain the sanctity of their communication may watermark their fonts which can be useful in establishing the authenticity of the correspondence as well as stand firmly against frauds at market place. On the other side it can also be implemented by font publishers to retain their rights over their font and restrict plagiarist acts. The proposed scheme embeds the binary message by modifying the curves of adjacent alphabets. The curve in this context also includes the straight lines.

Algorithm as follows:

Figure 4. [Mei, Wong and Memon (2001)]



Assumptions

$w_{init} \Rightarrow$ initial curve width
 $k \Rightarrow$ secret key

Constraints

only 8% of the actual width modification can be done

Identifying groups and curve pair

1. Add to the first group all curves widths which can be coupled with w_{init}

An order pair is created $(w_n, w_n + 8\%)$ where $w_n \in [w_{init}, w_{init} + 8\%]$

2. Start the next group with the closest width not the member of current group
3. Repeat(1) and (2) until all curve widths of the font are member of a group.

An embedding function is defined accordingly as

1. $E: W \times W \times \{0,1\} \times K \Rightarrow W \times W$
2. E is a mapping which redefines the width of two adjacent alphabets such that the change is determined by the selected threshold.
3. $P_k: C \times C \Rightarrow \{0,1\}$
4. where P_k is a parity function based on secret key K and applied over curve space C
5. The embedding process does not change the group borders thus parity function is defined as
6. $P_k(p,b) = \{(w_1, w_2) | (w_1 > w_2 \cdot t_k \text{ iff } b=0) \text{ or } ((w_1 \leq w_2 \cdot t_k \text{ iff } b=1)\}$

Decoding

1. Curve pair table is created
2. The detection function is $P_k(p)$

Amano & Misaki (1999) proposed the feature coding technique. Feature encoding technique is essentially an approach wherein foreign asset is hidden within the characters of the text by modifying specific component of the text. In their implementation particular feature if the text character is either thickened or thinned. The process of thickening or thinning is applied to symmetrically opposite blocks.

Algorithm to embed works as

1. Text area is identified.
2. For each line its position, height and width is computed.
3. The bounding box so constituted is divided into four equal size partitions i.e. two each in horizontal and vertical direction.
4. Diagonally opposite blocks belong to same group.
5. Average of the vertical black pixel runs is computed.
6. If the bit to be embedded is '1' 'make-fat' operation is applied to portions belonging to set 1 (blocks on left diagonal) conversely 'make-thin' operation is applied to portions belonging to set 2 (block on right diagonal).
7. Vice-a-versa of (6) is applied to embed bit '0'.

To decipher the hidden artifact following process is applied

1. Blocking, partitioning and grouping are performed.

2. If the average vertical run of partition 1 is greater than partition 2 and difference is greater than threshold then embedded bit is ‘1’ otherwise ‘0’.

Zhang, Zeng, Phu & Zhu (2006) has proposed a specific technique for watermarking of the Chinese text document images using font-feature coding technique. The large archive Chinese font component are evaluated for 9 attributes namely connectivity number, occlusive number, extremity number, inflexion number, joint number, cross number etc. Using these attributes the characters are converted into its components and subsequently process for mathematical expression. These components are subjected to relationship operators; there are 6 spatial relations defined for any two components namely *lr*, *ud*, *ld*, *lu*, *ru* and *we* respectively called as left-right, up-down, left-down, left-up, right-upper and whole enclosed.

The algorithm hovers around the following definitions

1. Component – A basic component of several strokes and may be a character or part of character.
2. Component Relation – An operation which defines the spatial relation between the components. If A and B are the components following relation define the spatial relationship *A lr B*, *A ud B*, *A lu B*, *A ru B* and *A we B* between A and B
3. Occlusive components – A component is said to be occlusive when it has one or more hollow enclosing regions. The number of hollow occlusive region defined as occlusive number.
4. Minimal Rectangle – of a component is a rectangular region that can envelop a component. It is only one i.e. only one rectangular bounded region encloses a component.

The technique uses the occlusive component for data hiding. All the characters are classified

into four classes namely characters with one, two, three or four occlusive region. The aspect ratio of the occlusive component is maintained for each type. The algorithm works as

Invariants

1. $N(C_i) < N(C_j) \Rightarrow P(C_i) < P(C_j)$
2. $N(C_i) = N(C_j) \&\& (C_i \text{ we } C_j \parallel C_i \text{ lr } C_j \parallel C_i \text{ ud } C_j) \Rightarrow P(C_i) < P(C_j)$

where $N(C_j)$ is the occlusive count of the character C_i and $P(C_j)$ is its priority thus as per (a) the occlusive count defines the priority for embedding similarly (b) defines the relative precedence among the operators for embedding.

3. $R(C') \subseteq R(C)$ where C' is watermark copy of character c
4. $R(c') \subseteq R(c)$ where c' is component of C

this states that enclosed rectangle will remain same after being watermarked.

Algorithm

1. Host H, watermark W and embedding parameters corresponding to individual occlusive number is given say α_i where $i \in [1..4]$.
2. For each character extracted character components are separated. Based on the occlusive priority a watermark bit is inserting by varying the hollow region keeping the ratio of the characters.
3. Similarly during the extraction process watermark document and parameter α_i where $i \in [1..4]$ are given. For each character component if $|T_i - \alpha_i| < \epsilon$ then hidden bit is one else zero.

Character Displacement and Diacritics Coding

Aabed, Awaideh, Elshafei, & Gutub (2007) have proposed an algorithm that exploits the special

attributes of Arabic language viz. the “Harakat” which are optional. The absence of “Harakat” or diacritics do not modify the meaning of the text and is understood to be present when reading. Though the scheme has been developed for the steganography but can be useful for watermarking the Arabic text.

In their survey study on usage of Harakats authors have found that the diacritic “Farah” occurs almost same number of time as rest of the other seven diacritics occur together. Thus “Farah” is used as target hotspot in text for data hiding on one side and rest of on the other side. “Farah” is used to encode bit one and others together for hiding bit zero. The algorithm is

1. For each character in text
 - a. if the bit to be embedded is ‘1’ then
 - i. if diacritic is “Farah” then keep the diacritics.
 - ii. else do for each character without “Farah” remove the diacritics till “Farah” is obtained.
 - b. else // bit is zero
 - i. if diacritic is not “Farah” then keep
 - ii. else do for each character with “Farah” remove the diacritic till one of the other six diacritics are found.

The algorithm was experimented with pseudo random ASCII number.

Gutub & Fattani (2007) have proposed a steganographic technique which also has capability to be implemented for the digital watermarking. The technique uses the structure of Arabic character for hiding the information. Proposed algorithm modifies the font features like punctuations over the text (Points) and addition of extension letters after the character. The extension letter does not alter the meaning of the text and are used for arrangement purpose and formatting. An extension

can only be added in location between connected letters of the Arabic text but are avoided at beginning or end of the word. The motivation for using the extension and *pointed-characters* for hiding data was that in Arabic *pointed characters* are about 15 out of 28 characters. Thus *pointed-character* will be occurring with approximately with same frequency as other character, qualifies to be a good landmark within text to indicate the presence of a specific bit 1 or 0.

Assertion:

1. The embedding process includes the message bit ‘one’ appears only within the *pointed-characters* appearing within the word by adding extension after the character.

Algorithm:

1. The insertion process scans the document from right to left and the binary pattern to be inserted in same direction.
2. If the inserted bit is zero then first *unpointed-characters* is extended all the *pointed-characters* character appearing before are left similar vise-a versa for zero.

Authors have suggested that by adopting the strategy of adding extension say on even lines extensions will be added before the character while on odd it will be added after the character the imperceptibility of hidden message will be improved.

Li & Dong (2008) proposed algorithm utilizes the structural organization of Chinese characters to imperceptibly insert watermark into the text document. This technique makes use of graphical representation of document file format. Algorithm ensures maximum robustness, greater watermarking capacity and better imperceptibility. The process of embedding watermark splits a Chinese character into two components, radical and the character, and embeds the data bit into host text by redefining the space between the characters.

The Chinese language system comprises of three Grapheme, pronunciation and signification. The font strokes for the Chinese characters are plenty and thus make a character suitable of data hiding. Chinese character organization is complex and complete meaning of the character is inferred by cumulating the meanings of right and left components; independently left and right components have valid meaning. For the purpose of watermarking the entire character set is clustered into three sets, the set of radicals, the character set and set of characters and radicals. The two operators are also defined *Left(C)* and *Right(C)* which reveal the left components and right component of the character. Let us denote set by

1. $\phi = \{ x \mid x \text{ is radical}\}$
2. $\Omega = \{c \mid c \text{ is a character of Chinese Language}\}$
3. $\varphi = \{C \mid C \text{ is a set of characters belonging to } \Omega \text{ and character's radical belongs to } \phi\}$

Algorithm works as follows:

1. Transform watermark W into $\{w_i \mid w_i \text{ is group of bits}\}$
2. To separate individual group code 0x44aa was used. The role of the code to act as delimiter and any loss of information during tampering will be assessable.
3. After inclusion of the delimiter code we have $B = \{b_i \mid b_i \in [0,1] \text{ and } i \in [1..n]\}$
4. for each character in host T
 - a. if $C \notin \phi$ goto (4)
 - b. else (5)
5. if $b_i = 0$ then goto (4)
6. Right(C) and Left(C) extract constituting component, adjust the space between and reconstitute C
7. if T is empty the terminate else goto (4)

Process is reversible and distance change between left and right radical from its character identifies one bit. Once B is obtained, the pattern

0x44aa extracted and watermark is reconstituted. It is purely a blind technique.

An, Lu Yi & Xaiolin (2008) have compared the utility of host as image or document format file and from their experimentation over populated host with different attack models. It was concluded that the host data remains understandable even with 30% loss. Taking advantage of this characteristic of human visual system host in image format was recommended. The proposed algorithm work in conjunction with the document file format and embed watermark using graphical interface APIs of the editor.

Host image is used for site selection and it is segregated into constituent components; among all other components characters were found to be the best for data hiding. The algorithm developed includes both the character size modification and the inter-character space modification. Since the character size modification leads to change in the vertical span of a line hence is dropped from the final implementation.

Proposed algorithm includes the restriction enforced above and modifies its approach by grouping the characters into a set of 3. In each group first character remains unaltered and acts as the reference character. The second character of the group encapsulates the data bit by increasing its font spacing and third character compensates the increase by reducing its space.

The algorithm is as follows:

1. Convert copyright information to bmp[]
2. using a key generate two-value random sequence randSeq[]
3. xormap [] = bmp[] \otimes randSeq[]
4. for each $i \in [0 \text{ to } m]$
 - for each $j \in [0 \text{ to } \text{xormap.length - 1}]$
 - if xormap[j] = 0 then
 - increase font spacing for second character on right
 - else
 - decrease font spacing for third character in on left

Similarly, the extractor reverses insertion process and computes the embedded bit by analyzing the difference between character spacing.

Chotikakamthon, (1999) developed algorithm for hiding digital signature within Thai language. It was commented by author that character spacing technique with any language degrades the readability of the text but that was not of too much consideration. Most appreciating part of such watermarking scheme is that it does not modify the sentence construction thus meaning of the text remains the same. Algorithm can be implemented for the other languages like English if the space modification is done with the set thresholds. Experiment was conducted with bitmap document image described using (1). The horizontal and vertical profiles, given by (2) and (3)

The proposed technique is used for the documents where the profile fails to provide clear demarcation for the line and word boundaries or the words are not separated by the exceptionally extended space. Technique has been implemented over a piece of text in English and Thai as well.

The technique works as follows:

1. Text is categorized into character groups called as Blocks using sentence / word level spacing as a group boundary.
2. Character blocks having more than L_D numbers of consecutive spaces are only selected for marking.
3. The data is embedded using

$$s_{nk}(l) = \hat{s}_{ok} + (2d_m - 1) \times \delta_d(l), l \in [1.. L_D]$$

$\delta_d(l)$ is the control mask for the d^{th} watermark bit, d_m is the m^{th} bit to embed. \hat{s}_{ek} is the average space between character at k^{th} block. $s_{nk}(l)$ is the new space.

4. If the spaces are more than twice of L_D than additional bits can be encoded as

$$s_{nk}(l) = \hat{s}_{ok} + \delta_n(l - L_D), l \in [L_D + 1.. L_T]$$

$$s_{nk}(l) = \hat{s}_{ok} + \delta_{d(m+1)}(l - L_T), l \in [L_T + 1.. L_D]$$

The detector reverses the phenomenon; challenge with the approach is the image quality of the output and the management of $\delta_n \delta_{d(m+1)}$ for each document.

Sun, Luo, & Huang (2004) have proposed an algorithm which modifies the feature of compound characters i.e. the characters that formed using more than basic character set of the Chinese language. The technique has its background in the Mathematical expression of the relationship between Chinese characters. Chinese characters exhibit six spatial relationships with their constituent components. The entire procedure can be summarized as – the watermark binary digits are coded by changing the glyphs of right and left components and the space between the characters.

Foundation of the process is based on the following definitions

1. A basic component is composed of several strokes and it may be Chinese character or a part of the Chinese character.
2. A compound component is composed of two or more than two basic components.
3. If A, B are two components then these exhibits six spatial relationship namely lr, ud, ld, lu, ru and we called as left-right, op-down, left-down, left-up, right-up and whole enclosed.
4. The operators exhibit relative precedence as: (), {we, lu, ld, ru}, {lr, ud}
5. For a Chinese character C in H_i , host text, if C is candidate for marking then $C \in \Theta$

Let us further define the sets

1. $\Theta = \{C | C \in \Omega, \exists D, E \in \Omega, F(C) = F(D) \text{ lr } F(E)\}$
2. $\Omega = \{C | C \text{ is a character of Unicode 3.0}\}$

The embedding algorithm works as

1. For each bit of watermark do
 - a. Locate $C \in H_i \cap \Omega$
 - b. If it is embedding position and bit is 1 then

Generate the glyph of C

End if

End for

Decoding procedure works as

1. calculate average width W of all Chinese character in H_i
2. calculate average space S between the two Chinese characters
3. calculate average error of width ΔW of all Chinese character
4. calculate average error of space ΔS
 - a. for each $C \in H_i \cap \Theta$ do
 - i. if $|W - W_c| > \Delta W$ or $|S - S_c| > \Delta S$ then
 1. if $C \text{ is } D$ then {D is following character of C}
 - C is a watermarking embedding position
 - go to following character D

Algorithm is designed specifically for a language.

Space Modulation

Huang & Yan (2001) have proposed algorithm wherein the watermark is inserted by changing inter-word spaces of text lines. Embedding process is characterized by presence of a Sine Wave across different lines. Attributes like frequency, amplitude and initial phase are used for coding information. The technique is relatively more robust than line or word shifting and can be used for both blind and non-blind data hiding. Experiment was done with the justified text.

An binary image is represented using (1) and vertical profile can be evaluated using (3). The spaces are recognized by

$$v(x) = 0, x \in [k, k+c] \quad (12)$$

where c is threshold distinguishing the word spacing from character spacing if there are d words in a line the average space will be

$$S_a = S_t / d-1 \quad d \neq 1 \quad (13)$$

where S_t is the total available in a line. Average space varies across different lines because as the number of word increases the space available decreases and vice-a-versa. When being watermarked the spaces will increase or decrease then change in average space will become \check{S}_a thus average change per word in a text line will be

$$S_{tc} = (\check{S}_a - S_a) / d-1 \quad d \neq 1 \quad (14)$$

If $S_{tc} > 0$ then the lines were expanded else those were shrinked thus the average

$$ES_i = INT(S_{tc} \times (Pxl_i / SUM(Pxl_i))) \quad (15)$$

Due obvious reasons there do exist difference between the s_{tc} and ES_i given by

$$S_d = S_{tc} - SUM(ES_i) \quad i \in [1, d] \quad (16)$$

where Pxl_i is width of i^{th} line in pixels thus after marking, it changes to

$$Pxl_{ni} = Pxl_i - ES_i \quad (17)$$

The interval by which the words will be drifted horizontally is evaluated as

$$Iv_i = Int(Pxl_i / ABS(ES_i)) \quad (18)$$

Above are the steps used by the algorithm to encode / decode the data within text, there are two methods of watermarking being proposed

Non Blind

- Mean is computed using (13) for the lines within workspace

$$a_1 = \text{SUM}(S_{an}) / q - p + 1,$$

$n \in [p, q]$, $0 \leq p < q < N$, N is total number of lines

- For each line a watermark component is determined by sine wave

$$W_n = C_1 a_1 \sin(\omega_1(n - p) + \phi_1)$$

where W_n represent the desire watermark component of the text line with an index of n , C_1 is a constant and its value in experiment remained 0.2, ω_1 and ϕ_1 are radian frequency and initial phase angle.

- W_n is added to S_a as

$$\check{S}_{an} = S_{an} + W_n$$

- Finally, the words in lines are modified using (14) to (18)

Blind coding technique

- A key is selected from the text such that all lines having word count greater than or equal to key can only be watermarked.
- S_w is the set of line so selected.
- $a_2 = \text{SUM}(S_{am}) / (u - v + 1)$
where $m \in [u, v]$, u, v are the indices of the original text lines, m is the index within S_w , S_{am} is the S_a of line m
- for each line in set identified

$$W_m = C_2 a_2 \sin(\omega_2(m - u) + \phi_2)$$

the C_1 is chosen within the range of 0.2-0.3

- watermarked lines are computed as

$$\check{S}_{am} = a_2 + W_m \text{ if } m \in S_w$$

Decoding of the watermark can be generalized as the following equation

$$W_n = Y(n) - X(n)$$

where $Y(n)$ is the discrete random variable representing the space distribution of the coded text while $X(n)$ is same for the plain text. phase information is obtained as

$$r(j) = (\text{SUM} [W(n) A_d \sin(\omega_d n + j)]) / T$$

where T is summation number depending upon number of items in $W(n)$, ω_d is the radian frequency which can be varied, and j is the lag number for a line.

The symmetric nature of the coding can be perceived by the any attack and watermark can be removed but that requires additional effort.

The algorithm proposed by Kim, Moon & Oh (2003) implements watermarking in a text document image. Embedding of artifact is done using the word-shifts in a line. In each line that can be marked words are classified into segments such that two neighbouring segment shares a common word. A word lying at the boundary of two segments act as reference for assessing the displacement, furthermore the inter-segment boundary word do not allow the word shifting of one segment to intrude into adjoining segment. Data hiding is performed within the segments of same class.

The readjustment of inter-word space is performed using statistical attributes of the inter-word spaces.

Assumption

- K be the number of words
- s is the number of words in a segment
- total number of segment classes produced will be $L = K^s$. The value of L as grows larger the complexity of assessing the watermark within the text become rarer, hence robustness improves.

4. There must be atleast two segments per line.
5. Artifact will be saved in the segment of same class.

Segmentation of the line begins with the classification of words into classes by comparing the relative weights of adjacent word(s) e.g. if $l(w_i)$ be the width of the w_i in a line i then $l(w_{i-1}) - l(w_{i+1})$ defines the weight of the word w_i . Words in line are assumed to be in a circular queue. As each word is classified into its respective class there segment is identified by concatenating the class code for a group of words. If word w_i , w_{i+1} , w_{i-2} belongs to class 1,0,1 respectively then together these constitute a segment and segment class will be '101'. All the segment belonging to same class constitute the segment set $S(k)$ where $1 \leq k \leq L$ is the number of segments of a class. By computing the space statistics like mean and variance, for each segment set and inter-word space is adjusted to comply the assumed heuristics. In paper it was considered as

H1: ($s=3$, $L=64$, $K=4$, parameter μ)

If($\mu_1 \leq \mu_2$) bit = 1 else bit = 0

H2: ($s=3$, $L=64$, $K=4$, parameter μ, σ)

If($\mu_1 \leq \mu_2$ and $\sigma_1 \leq \sigma_2$) bit = 00

($\mu_1 \leq \mu_2$ and $\sigma_1 \geq \sigma_2$) bit = 01

($\mu_1 \geq \mu_2$ and $\sigma_1 \leq \sigma_2$) bit = 10

($\mu_1 \geq \mu_2$ and $\sigma_1 \geq \sigma_2$) bit = 11

It is evident, as many parameters are taken for the compliance, larger will be the data hiding capacity. In H1 capacity is 64 bits while in H2 it increases two fold to 128 bits with same number of segments.

Micic, Radenkovic & Nikolic (2005) designed a solution which was directed towards securing the

text documents over the unsecure communication channels. The main purpose was to enable the receiver to authenticate the received message and to ensure the sanctity of the text message. Authors have used the coarse method for extracting the line features and exactly every character is not segregated from line. Data was hidden using the techniques of line and word shifting i.e. a component selected may be shifted slightly up – down or left – right.

In their experimentation authors have used the text document in Word format. The proposed method makes partition of all lines of text in syllables. A syllable may be a word which can not be divided. On the receipt of the document recipient will be decoding the shifts produced in the syllables and authenticating the message.

The embedding is performed as

1. A line is divided into its constituent syllables according to the language
2. Histogram of syllables is computed for the line.
3. Embedding raster is provided for n -th line based on adequate histogram by shifting syllables up or down or left or right. By applying unique key.

In their implementation have shifted only either first, second or third character and kept the position of other character fixed.

Decoding requires the key from sender and work as

1. A line is divided into its constituent syllables according to specific language requirement.
2. Histogram for the line is computed
3. According to embedding rules histogram is reconstructed
4. Comparison of retrieved information and the key is done
5. If the error is found above threshold then document is declared to be modulated or else it is valid.

The algorithm requires synchronization between encoding and decoding process with respect to shifting of lines. With 4 directions of coding there are 24 variants of the process may be designed. As a very small unit of the word is marginally shifted hence imperceptibility was high. Proposed method is completely blind.

Brassil, Low, Maxemchuk & O'Gorman (1994) have discussed in detail the role of marking and its relevance in preserving copyrights of publisher and authors. For various data hiding techniques in their experiment authors used document image as host. The prime tool used for document analysis was horizontal and vertical profiling which is basically the aggregation of pixel intensity along the width and height of the section viz, character, word, line or paragraph of the document. Three techniques that were discussed by the authors were line shifting, word shift and character feature coding.

As per the technique maximum numbers of parallel channels are available when characters are taken as host for hiding and paragraphs have the least channels. Conversely, a paragraph has the maximum signal strength and the word have the least. In line shifting techniques a line is shifted in multiples of a pixel which is around 1/300 inch vertically up or down. In word coding technique a word is shifted left or right by a pixel or so. The character feature coding technique is a bit complex where a specific feature of character is searched and is extended by couple of pixels.

Line and word coding technique requires minimum of two adjacent lines to remain unaltered so as these can be used for reference during the extraction process. This results to the reduction in channel capacity due to wastage. Detection of the drift is done using two different approaches namely the baseline distance method and centeroid detection method. A baseline is a virtual line which running between two lines, line shift can be computed if the distance between baselines above and below the marked text line are unequal. Similarly in case of words the vertical boundary on left and

right of word act as baseline and the difference between the spaces identifies the displacement. Baseline detection method fails when noise level is high. Centeroid method is resilient to this and gives better results even in case of additive noise attacks. Centeroid is a weighted average over pixel intensities along a horizontal or vertical section; it is a relative quantity and remains unaltered due to dislocation of text. Difference between the centeroid of adjoining unaltered lines with altered one if left difference is larger then block is shift right else shift is leftwards. Among the proposed technique authors have experimented with line shift coding due to the reason that photocopy or printing produces more distortion in one direction than in other. Line shift technique can hide bits one-third of total number of lines in a document.

Low, Maxemchuk & Lapone (1995) proposed a variant of line shifting technique wherein the words within the line are shifted either left or right. Since, line marking technique has very low capacity in comparison to word shift or character feature coding hence to improve the capacity of host channel word shifting technique was developed. Due to word shift coding technique each line of sufficiently good length is entitle to carry the watermark bit as a consequence theoretically capacity increases by three folds.

Like line shifting technique in this technique a channel is divided into two segments namely the control and host channels. Control channels are the segment of line which enclose host channel from either side. Control channels act as a reference point to evaluate the disturbance level of the middle or host block. For the detection of the watermark two separate techniques were proposed first was called as Centeroid Method and other was Correlation Detector. Centeroid method unlike that of line shift does not simple compute the difference between the adjacent centeroid. It also takes into account the variances of the distorted unmarked profile.

Brassil, Low, Maxemchuk & O'Gorman (1995) have further improvised their work by including

the word shift along with the line shift algorithm in single implementation. The main reason to include both type of encoding technique was firstly to improve data hiding capacity of the channel and secondly to neutralize the impact of noise in horizontal and vertical direction is totally independent of each other hence the error in watermark detection can be compensated individually and independently.

Embedding process divides channel into two components the control channels and host channel. Thus for line shifting, a group of three lines constitutes a channel and first and third line is regarded as the control sub-channel and middle one is host sub-channel. Similarly, a sufficiently long line is divided into three sub-channels; the length of line must be like that it is possible to have more than two or more words in each block. In their experiment authors have considered all the four kind of noise. Out of the four noises considered salt-and-pepper noise and translation are the additive noises while rests are the multiplicative noises.

During detection process both the original copy and the illicit copy is scanned. Noises are compensated using the original image. Since, host is marked both horizontally and vertically to detect the deflection in host lines difference between the centroid of adjacent pair of lines is measured if the difference between the upper set is smaller than the lower set it is concluded that host line is shifted upwards else downward. Correlation detector is used for the measurement of horizontal drift within the line. A correlation detector quantifies the measure of deflection the marked profile suffers from original profile.

In their initiative, Alattar & Alattar (Retrieved Feb 25 2009) have discussed watermarking technique for text images that has uniform spacing and/or irregular line spacing. The technique was blind i.e. it do not require original document for artifact extraction. Algorithm designed encodes data within host using the space coding approach. Spread spectrum technique is applied to hide the

data within the host. With 18 bit payload algorithm can support 26 thousand different IDs but to ensure robustness against noise and to avoid undue redundancy of watermark error correction code is also included hence there is drastic degradation of payload capacity.

Watermark is inserted within the text by appropriating the total expected displacement to individual word according to their weight. This results into the irregular inter-word space distribution. During the detection of watermark all the spaces computed are aggregated into the sequence of the size equal to the size of spreading sequence. All the spaces above the threshold consider as 1 while others are consider as -1 and thus inserted sequence is obtained. This sequence is then subject to error correction and after that the payload is deciphered to identify the recipient. This is a white paper from Digimarc Corporation, leading company of digital watermarking products.

Early DRM Implementation for Online Archives

This section discusses the renowned implementation to uphold digital right management. The earliest implementation makes use of *Copyright Clearing House* to release copyright to recipients while other two have used the watermarking for DRM. SEPTEMBER, a trial prototype for online distribution of articles uses spatial coding technique while the other exploited the spread spectrum technique.

The Rights Pages (Fox, O'Gorman, & Story, 1992) was an image based electronic library implemented at AT&T Bell Laboratories. This was one of the first implementation for digital libraries wherein the browsing of Journals was enabled using image based hyperlinked web pages. The main objective of implementation was to

- Generate alters to subscriber on the arrival of new journal articles.

- Allows the subscriber to browse the library of articles.
- Allow to process order for printed version of the document.

The virtual library represented by the stacked copies of digitized journals, replicating the physical library. It allows browsing using sequential navigation of pages within a journal as well as article or content specific. The system has the following components

- It obtains Table of content and article pages within a journal in image form.
- Automates data acquisition through OCR and pattern recognition. Data so generated is used for creating tags for the document search.
- Enable matching of user selection for preferences with ASCII tags of the article.
- Generate alters for users matching to their preferences and send URL references for table of content and articles.
- Allows user to place order for print version.

The system was the first of the kind prototype. The copyright issues were handled using location-based restriction. The third party infrastructure was used for managing the copyright related issues.

SEPTEMBER (Choudhary, Kristo et. al. 1995) was an initiative to make the IEEE Journal available online to the subscriber using global network. The first magazine published was IEEE Journal on Selected Areas in Communication. The main objective of the project were

1. To increase reach of journal to wider spectrum of audience.
2. To simplify the access of journal simpler for online readers.
3. To accelerate publication process with rapid dissemination.

The entire system was designed using open access standard and tools. In HTML presentation, document images were used for navigation. Navigation was designed from table of content to individual article and vice-a-versa. The documents are archived in PostScript and Tagged Image File Format and delivered in PDF format. A registered user is being given a complete access to digital library while guests can only be allowed to browse through HTML content. This also include payment infrastructure. A unique digital watermark is added to each article imperceptibly by repositioning of text along both vertical and horizontal direction. Watermark enables tracing of downloaded document copies.

Digimarc Media Bridge (Alattar, AM. retrieved on 25th Feb 2009) was the proprietary innovation done for securing high quality images. This embeds an active content within the host which initiates action when detected. The watermark remains dormant but as analyzer reads the watermark content and invokes the operation for acquiring knowledge pertaining to permissions or rights granted with the object, called as '*smart images*'. Watermark embedded refers to a specific URL within local or global network. Embedder inserts watermark into image using block-wise coding Spread Spectrum technique and each block contains single watermark bit. Similarly, extractor firstly synchronizes to embedder and then extracts the watermark bits. The watermark was paired key of a reference to specific URL, where knowledge is maintained, and index code, referring to permission for the object in database.

CLASSIFICATION OF TEXT WATERMARKING TECHNIQUES

Text watermarking is the most neglected arena of 'watermarking domains'. This was due to the lower market valuation of text documents in comparison to other media format like audio and video. After reviewing watermarking techniques it is apparent

that watermarking of text document is performed in two different domains namely, ‘Document Image Format’ and ‘Document Presentation Format’.

Text Document Image Watermarking

Algorithm belonging to this class hides copyright information into document image. These algorithms implement profiling as common tool for extracting features from document image. Reason behind using image format is that during print operation data file is transformed into image equivalent form. To enable real time data hiding, an algorithm must be capable of inserting watermark into pre-print version of document. These under this class can further be sub divided into following groups

Format Coding

A technique belonging to this class embeds data into host by modifying inter-line space or inter-word space. These techniques detect watermark by computing specific statistical quantity. These are resilient towards printing-and-copying noises. The algorithms belonging to this class are line shift coding and word shift coding.

Line Shift coding technique amends the distance between the two adjacent lines. The line adjusted either upward or downward, to keep track of displacement each drifted line is encapsulated between two stationary lines. Static lines act as the reference to evaluate the displacement using base line detection algorithm or centeroid method. Since to encode each bit three lines are required; these techniques offers a very small data hiding capacity. Such algorithms exhibit a very high robustness by revealing the watermark in the tenth photocopy of a document.

Word shift coding algorithm displaces a group of words by transforming a line into three independent segments. Left and right segment remain static and middle segment is drifted either left or right. The shift normally comprises

of displace of the magnitude of one or two pixel. The shift from the reference point is computed using correlation detector. Word shift algorithm has improved data hiding capacity by three fold. (Brassil, Low, Maxechuk, & O’Gorman, 1994) (Brassil, Low, Maxemchuk, & O’Gorman, 1995) (Low, Maxemchuk & Lapone 1995)

Feature Coding

An algorithm of this category transforms the appearance of character in a predetermined fashion. The information is coded either turning pixel(s) on or off. Certain implementation of this group even deploys pattern recognition and substitution. The complexity of algorithms is relatively higher than Format Coding which owes to the process of site selection. As text is a binary image hence the task of site selection becomes cumbersome. Further, a site must uphold certain invariants to be selected for marking otherwise subsequent site is evaluated; similarly after modification the site must conform to fresh set of invariants. This category is further sub divided into two separate classes namely Font Feature Coding and Pixel Flipping.

Font Feature coding is a technique wherein the embedding process performs data hiding along the boundaries of character. This is performed in three ways firstly by watermarking specific characters, secondly by thickening the boundaries of characters and lastly by enhancing the intensity of characters. For watermarking a character by changing span of its horizontal or vertical component; the upright components have preference hence characters like ‘h’ or ‘b’ is preferred. The data is hidden by extending the vertical span of a character. In second approach the character boundaries are thickened simultaneously in all directions and consequently character becomes bold in appearance. In the third form of coding the color intensity of character(s) is increased to make emergence sharper during printing. (Theimert, Steinebach & Wolf, 2006), (Zhang,

Zeng, Pu & Zhu, 2006) (Oh & Kim, 2004) (Gutub & Fattani, 2007)

Pixel Flipping is also known as block wise watermarking technique. In this approach document image is decomposed into blocks of equal size. Within each block either a pattern is located or invariant is tested if the conditions uphold then pixel(s) is swapped. In pattern based approach pattern database is searched and if block pattern belongs to database its pixel(s) is swapped to form another pattern. Likewise invariant based methods uses a set of conditions to comply and if a block conforms then its pixel are flipped.(Wu & Liu, 2004), (Wu & Lee, 1998),(Pan, & Tseng, 2001), (Bhattacharjya & Ancin, 1999), (Chen, Pan & Tseng, 2000)

Space Coding

Space coding algorithms encode copyright information by modifying intra-line spaces. The two methods that are prominently done are word space coding and character space coding. In either case the distance between the adjacent components is modified to encode the information. The total impact of increasing or decreasing the space is reversely compensated so as there is no effect over the size of line. Word space modification technique is comparatively more transparent than character spacing. The main challenge with character space coding is that if change in space is made above certain threshold value the readability of text degrades. Vertical profiling is used as main tool used for extracting various text components within a line.

Word Space Coding uses inter-word space to hide the watermark. The space between two adjacent words is either increased or decreased to represent the watermark bits. There are several methods to detect such adjustment the prominent one are displacement of words belonging to same classification and representation of watermark as continuous value form a wave form. (Kim Moon & Oh, 2003), (Huang & Yan, 2001)

Character Space coding is performed primarily by language dependent data hiding versions. Language under consideration may have characters that are composed from two or more basic character and increasing the space between these components do not change the meaning of the character. (Chotikakamthron, 1999)

Text Document Watermarking

Watermarking techniques inserts copyright information into text using standard APIs of application program. These techniques automate the process of data hiding within the standard application. The watermark is inserted using any of the methods like space modification, appending certain new character and font feature coding. Among the mentioned approaches font feature coding is the most complex where as the space coding is the simplest. With respect to imperceptibility factor and robustness font feature coding can be ranked at the top followed by space coding method.

Diacritic Coding

Diacritics are the special characters in languages like Arabic which if not present do not hamper the meaning of word. Diacritics are assumed to be present and their pronunciation is derived with reference the context in the literature. Any Arabic text if not properly diacritics can be read by a cleric without any problem. Fully diacritic text, especially in Arabic, is not now in practice hence the presence of diacritic raises suspicion for being marked. Diacritics based coding techniques assigns the bit value to different diacritic and their respective presence in marked document is deciphered to compose watermark. (Aabed et el, 2007), (Gutub, & Fattani, 2007)

Space Coding

Space coding algorithms encode copyright information by modifying intra-word spaces. The

coding is performed after the analysis of character constitution. Mostly the characters that composed from two or more basic character are used for the purpose. Say, in Chinese all complex characters that are satisfying specific spatial relation are used for encoding similarly for Arabic text displacement of diacritics is performed to encode message. Constraint to be maintained are like vertical span of line should not be changed and horizontal span of word must be modified within a limited constraint. This poses a challenge to retain displacement within a threshold so as the readability will not be affected. (Micic, Radenkovic & Nikolic, 2005), (Li & Dong 2008), (An, Lu, Yi & Xaolin, 2004)

Font Feature Coding

In an attempt to define their unique corporate presence companies create their own proprietary font. To protect their font from plagiarist attempts these fonts are watermarked. The watermarking is performed either by the font manufacturer or using standard APIs of application program. Marking of the font is performed over a predefined set of patterns constituting a character. The best approach was to hide the information along the boundaries and curves of the characters. To impart robustness adjacent patterns of adjacent characters may be used and bits are hidden by complementing weight change in adjacent patterns. Another form of feature coding is to change the aspect ratio of different segments of a character. This method of data hiding is relatively easier to implement than earlier version. (Theimert, Steinebach & Wolf, 2006), (An, Lu, Yi & Xaolin, 2008), (Sun, Luo & Huang, 2004)

FUTURE RESEARCH DIRECTIONS

The development of binary image watermarking has remained mainly focused towards insertion and extraction of the secret message. The work till

date has been done with different languages and approaches and still there is ample scope of future research in this field primarily focusing over:

Unified Document Archive Representation

Main objective of the digitization is to converts an analog channel into a digital channel so as the quality of the content remains consistent and the document remain also preserved for life time. During the digitization it is required that a specific format must be used for the archives which will be accessible through any platform.

Open source initiative for document format is currently in a full swing and various standards have come up. The main challenge remains the same which document format to accept and implement. Since, what so ever is the situation, document do exists at some point of time as an image and the image remains independent of the font used in the document, an image of the archive can be viewed with mere browsers thus the image format is the best suited for the document archives.

Keeping the archives in image format is an expensive approach, as the size of image is larger than that of its corresponding text file. A research may be initiated towards a format that remain transparent towards the platform and can be viewed with any of the available essential tools. On the other hand compression algorithm may be worked for the archives so that the size may considerably be reduced.

Watermark Design

There is no research actually being undertaken to define the composition of watermark. Most of the watermarking algorithms implement the watermark as random bit sequence of varying size. The experimental watermarks vary from images to certain ASCII values. Since, a watermark is not merely an object to be inserted within the host but it is also an asset that recites receiver's rights over

the host hence it is mandatory that a watermark be carefully designed. A research needs to be carried out to define the conciseness and expressiveness of the watermarks.

Archive Rights Description

A file irrespective of its nature and content comprise of two components viz. Header and Data. Header contains metadata specification for the data segment of the file. Metadata specification includes listing for file type, data offset, header size, font etc. which is used by the associated application to read and represent the data correctly.

Metadata specification for the header is another area of research because the specification not only defines the content and its layout but also the rights granted to the receiver by the sender. The specification needs to be portable so that archive can be viewed using simplest set of tools available. This feature makes the archive accessible from wide range of applications. Header needs to be comprehensive so that it can augment the need of special provisioning for Rights Management. On the other hand it should not increase the overall size of the document.

To compensate the comprehensiveness of the header a compression algorithm may be devised. This is another area within the archive format definition where a research may proceed. The compression algorithm needs to be lossless and least complex as theses archives have to reside over the networks which have limited resources to share. It worth to mention that the compression is not necessarily be investigated in any of the conventional domains.

Standardization

Digital Rights Management is still juvenile and the researches are going on. The focus of the researches is towards the implementation of data hiding techniques for different document formats and languages. The algorithms vary in approach

from block-wise pixel flipping to character space modification. A great scope is present in converging approaches towards a common guideline as discussed by Mintzer, Braudway & Bell (1998). Development of standard for watermarking algorithm and dissemination infrastructure is essential. The standardization of algorithm and protocol makes the designing of product an easier and less cumbersome task. The prime areas are discussed in following paragraphs

Watermarking algorithm complexity for embedding and extracting processes has direct impact over the performance of the algorithm. Throughput of the system degrades as the complexity increases. Moreover, the data embedding has to be a realtime process because the same rights cannot be granted every user the same hold true for watermark. To enable realtime embedding a fast and simple algorithm is more preferred.

Rights Expression Library specification for different techniques need to be identified. These will be used either by the application or application agent or by the operating system to implement DRM. Library may include the rights description API to define the scope and definition for a Right and Right Management APIs that will be used to assess the Right defined within the asset. The library must be built to cope up the legal issues related with DRM and clearly distinguish innovation from violation.

Key generation, management and dissemination for encoding and decoding of watermarks need special attention. These make the watermark more secure and reliable within the host. It is well known fact that larger the key more secure is the content. This tends to increase the size of the watermark and watermarking process. Beside the key size another challenge lies with the distribution of the key and its authentication.

Communication Protocol level support to enable lossless and efficient transmission of document archive over network and will be analogous to the multimedia multicasting streams. The reason for having separate protocol as the rights related

to literary work are more comprehensive than any other form. With a separate protocol certain rights related issues can be migrated to protocol level. (Zhao,Koch, Luo, 1998)

Operating System level plug-ins or APIs for the support of DRM is essential. An initial initiative resulted into popular problem called *Sony Roottool Kit*. This problem has created an insecure trapdoor open within the client operating system. Like any other security initiative digital watermarking needs a minimum support at Operating System Level so that a tightly knitted DRM can be designed. (Sheppard, Safavi-Naini & Liu, 2003), (Mintzer, Braudway & Bell, 1998)

Portability and Interoperability

DRM implementation needs to exists across all platforms both software and hardware because online archives can be accessible from any platform. This demands the algorithms and data structures to perform against all heterogeneity. Moreover, the integration of the mobile computing network to the conventional network further multiplies the diversity.

Incompatibility among proprietary solutions is a major challenge. A file format that is compatible to one solution may totally become incompatible to other. A middle tier solution is required which will mediate to make these proprietary products interoperable. The middleware must be capable of acquiring, encrypting and embedding watermark. It should also be responsible for secure delivery of content between the stations. Client side component defines the interfacing and protocol defines mechanism for right enforcement. (Zhao,Koch & Luo, 1998)

Benchmarks

There are the metric values that have to persist for every watermarking algorithm and these measure the efficacy of algorithm designed. Evolution of such benchmarks helps in standardizing the

algorithm design and quality. Benchmarks must be established for imperceptibility, false-positive error, watermark composition and content, noise models and robustness.

Imperceptibility is the metric that defines how transparent a watermark is within the host. Ideally the imperceptibility of zero i.e. complete transparency which is impossible thus minimum tolerance thresholds need to be established. The design and size of the host vary from one host to another hence its capability to accommodate watermark may vary drastically. Threshold values for the different classes of host must be computed and help in maintaining uniform embedding of watermark across the host.

Robustness is the metric of watermarking, which measures the tolerance of watermarks against attacks. A value of zero implies the most fragile watermark while higher value defines the robustness of the watermarks. This metric also has impact over embedding process, watermark redundancy and the host capacity. An exploration in the domain will redefine the design of the algorithm and analysis of host.

Adversary Models, noise models and watermark standardization need to be established at the earliest. This will be a significant step towards developing testbeds for next generation of watermarking algorithms to prove their effectiveness and reliability. Watermark standardization will be of great help in deciding the structure of the embedding and extraction process.

Channel Capacity

A text document is a high contrast image, hence becomes highly susceptible to slightest modification. In case the host is in document file format then changes beyond a level hampers the readability. Channel capacity estimation hence is essential for predetermining the tolerance of host and maintaining its readability. In case of document the font face used decides image the channel capacity and the formatting applied. Similarly, in text document

format the composition style decide the capacity. The estimation of capacity is desirous for

- **Estimation of Watermark:** as knowing the capacity and required level of redundancy of embedding the size of the watermark can be estimated. As the size of the watermark becomes available its composition and comprehensiveness can be established or vice-a-versa.
- **Embedding Site Selection:** because during the host channel capacity estimation all the site capable of hosting watermark bits must be identified. The host site capacity and their distribution will be of great help in performing data hiding homogeneously. This improves upon the synchronization desired between the extractor sub-unit and the embedding sub-unit.
- **Structural Composition of Text Document:** the thorough investigation of the constituent components of text document also reveals the structural composition of text document as discussed in section Document Image Structure and Composition. This information will be essential for the embedding algorithm to locate for promising locations.

Trust Model

Document dissemination infrastructure must be developed like any other multimedia distribution infrastructure. The main objective of DRM system is to license the distribution (Quadir & Ahmad 2005), (Sheppard, Safavi-Naini & Liu, 2003) instead of content distribution. Individuals owing the license are authorized to use the digital content and their rights over content are described within the license file. These rules may be related to usage, transfer expiry, copy etc. combining these rules and distribution system a Business Model may be implemented such as Rental, Subscription, Pay-per-use, try-before-use or any other model like

these. Such system designed with the perspective of having more control over consumer than the content. (Zhao,Koch & Luo, 1998)

There are two kind of proposals mentioned in (Quadir & Ahmad, 2005), (Sheppard, Safavi-Naini & Liu, 2003). The proposal by Sheppard, Safavi-Naini & Liu, (2003) is a generalized system, the model is basically an authorization based system and do not address to the need to protect the digital content. The worst risk will be if license is legally procured and illegally distributed and on being recovered it will be difficult to prove the ownership of digital content. System from Quadir & Ahmad, 2005 though being designed specifically for distribution of literary creations over networks but it has too much of user interference. System has left the design of the watermark to hands of user who might be unaware of it design consideration may design a weak watermark.

A lot of research is required for the distribution infrastructure beginning with various units, roles and their integration. The other aspect with the infrastructure is the security of content and transactions.

CONCLUSION

Proprietary systems are in existence for managing the digital rights of a owner(s) but these haven't proven themselves to the expectations. The worst part of all such system was their inability to cooperate across their respective platform for the protection of the rights of owners. The inconsistencies among such solutions include the presentation form of the text document, meta-data specification for literary archives, incorporation of regulation with framework and above all, the client side support. The emergence of open source systems has also started a new tussle regarding the file format and system architecture. This all started with the development of middle tier solution from open source community to provide interoperability among heterogeneous systems. In event of all these

conflicts now it is becoming essential to agree upon standards for digital data files.

The absence of any sort of benchmarking and attack simulation models for the text marking systems act as catalyst to issues and resulted into present differences. Using standardized testbeds and benchmarking tools all the text watermarking solutions can be evaluated for their reliability and sustainability against attack models. Another avenue which remained neglected was the Watermark itself. Most of the experiments assumed watermark to be a simple binary code which uniquely identifies a digital literature. In order to protect digital rights it is mandatory that watermark is made more expressive and concrete so that it can be used as conclusive evidence against intentional or unintentional tampering. The structuring and definition of composition is necessary for making watermark an ultimate tool against plagiarism.

A holistic study of document dissemination infrastructure is required. Number of parties, their roles and authorities must be exclusively defined. The architecture of middle tier to interface all participating entities needs to be decided. Eventually, the support required at protocol level, client end application and at operating system level must be defined. Finally,

“Standardization is inevitable for text watermarking to make it a comprehensive system against breach of copyright.”

REFERENCES

- Aabed, A., Awaideh, S. M., Elshafei, A. M., & Gutub, A. A. (2007). Arabic Diacritics Based Steganography. In *IEEE International Conference on Signal Processing and Communication (ICSPC 2007)*, (pp. 756-759).
- Alattar, A. M. (n.d.). *Bridging Printed Media and Internet via Dimarc's Watermarking Technology*. Retrieved Feb 25, 2009, from https://www.digimarc.com/resources/docs/tech_papers/dmrc_media_bridge.pdf
- Alattar, A. M., & Alattar, O. M. (n.d.). *Watermarking Electronic Text Documents Containing Justified Paragraphs and Irregular Line Spacing*. Retrieved Feb 25, 2009, from https://www.digimarc.com/resources/docs/tech_papers/dmrc_text_watermarking.pdf
- Amano, T., & Misaki, D. (1999, September). A feature calibration method for watermarking of document images. In *Proceedings of the Fifth International Conference on Document Analysis and Recognition (ICDAR '99)*, (pp. 91-94).
- An, L. J., Lu, H., Yi, F. D. & XaoLin, G. (2008). A Text Digital Watermarking for Chinese Word Document. *IEEE Symposium on Computer Science and Computational Technology*, (pp. 348-351).
- Berghel, H. (1998, July). Watermarking Cyberspace. *ACM Communication*, 41(7), 19–24.
- Berghel, H., & O'Gorman, L. (1996, July). Protecting ownership rights through digital watermarking. *IEEE Computer*, 29(7), 101–103.
- Bhattacharjya, A. K., & Ancin, H. (1999). Data Embedding in text for a copier system. In *Proc of International Conference on Image Processing*, 2, 245-249.
- Brassil, J.T, Low, S.H, Maxechuk, N.F & O'Gorman, L. (1994). Electronic Marking and Identification Techniques to Discourage Document Copying. *IEEE Infocom '94*, 3, 1278-1287.
- Brassil, J. T., Low, S. H., Maxemchuk, N. F., & O'Gorman, L. (1995 April), Document Marking and Identification using both Line and Word Shifting. In *Proceedings of IEEE INFOCOM '95. Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, 2, 853-860.

- Chen, Y.-W., Pan, H.-K., & Tseng, Y.-C. (2000). A Secure data hiding Scheme for two color images. In *Proceedings of 5th IEEE symposium on Computer and Communication*, (pp. 750-755).
- Chotikakamthon, N. (1999). Document Image Data Hiding Technique Using Character Spacing Width Sequence Coding. In *Proceedings of IEEE International Conference on Image Processing*, 2, 250–254.
- Choudhury, A. K., Kristol, D. M., Lapone, A., Brassil, J. T., Low, S. H., Maxemchuk, N. F., & O’Gorman, L. (1996, May). SEPTEMBER – Secure Electronic Publishing Trial. *IEEE Communications Magazine*, 34(5), 48–55. doi:10.1109/35.492972
- Craver, S., Yeo, B., & Yeung, M. (1998, July). Technical Trial and Legal Tribulations. *ACM Communication*, 41(7), 45–54. doi:10.1145/278476.278486
- Fetscherin, M., & Schmid, M. (2003) Comparing the usage of Digital Rights Management Systems in Music, Film, and Print Industry. In *Proceedings of the 5th international conference on Electronic commerce*, 50, (pp. 316-325).
- Fox, D., O’Gorman, L., & Story, G. A. (1992, September). The RightPages Image-Based Electronic Library for Altering and Browsing. *IEEE Computer*, 25(9), 17–26.
- Gutub, A. A., & Fattani, M. (2007, May). A Novel Arabic Text Steganography Method Using Letter Points and Extensions. In *WAST International Conference on Computer, Information and Systems Sciences and Engineering*, Vienna, Austria, (pp. 28-31).
- Huang, D. & Yan, H. (2001, December). Interword Distance Changes Represented by Sine Waves for Watermarking Text Images. *IEEE Transaction on Circuits and Systems for video technology*, 11(12), 1237-1245.
- Hurtung, F., & Kutter, M. (1999, July). Multimedia Watermarking Techniques. *Proceedings of the IEEE*, 87(7), 1079–1107. doi:10.1109/5.771066
- Kim, Y., Moon, K., & Oh, I.-S. (2003). A Text Watermarking Algorithm based on Classification and Inter-word Space Statistics. In *Proc of 7th International Conference on Document Analysis and Recognition ’03 (ICDAR ’03)*, (pp. 775-779).
- Li, Q., & Dong, Z. (2008). Novel Text Watermarking Algorithm Based on Chinese Characters Structure. *IEEE Symposium on Computer Science and Computational Technology*, 2, 348-351.
- Low, S. H., Maxemchuk, N. F., & Lapone, A. M. (1995). Document Identification to Discourage Illicit Copying, *IEEE Global Telecommunications Conference, GLOBECOM ’95*, 2, 1203-1208.
- Martin, J. R. H., & Kutter, M. (2001, August). Information Retrieval in Digital Watermarking. *IEEE Communications Magazine*, 39(8), 110–116. doi:10.1109/35.940051
- Mei, Q., Wong, E. K., & Memon, N. (2001). *Data Hiding in Binary Text Documents*. Retrieved on 19th Feb 2009 from http://mike.sfs.poly.edu/memon/publications/pdf/2001_Data_Hiding_in_Binary_Text_Documents.pdf
- Micic, A., Radenkovic, D., & Nikolic, S. (2005, September). Autentification of Text Documents Using Digital Watermarking. In *Proc of 7th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services*, 2, 503-505.
- Mintzer, F., Braudaway, G. W., & Bell, A. E. (1998, July). Opportunities In Watermarking Standards. *ACM Communication*, 41(7), 56–64.
- Mishra, R. (2007, November/December). *Sectional Fingerprinting for Binary Images*. Talk at 42nd Annual Convention of Computer Society of India, “Generation Next”, Bangalore, India.

- Mishra, R. & Raghuvansh, S. (2009, March). Binary Image Mapping for Digital Rights Management. *CSI Communications*, 17-20.
- Oh, I.-S., & Kim, Y.-W. (2004, May). Watermarking text Document images using edge direction histograms. *Pattern Recognition Letters*, 25, 1243–1251. doi:10.1016/j.patrec.2004.04.002
- Pan, H.-K., & Tseng, Y.-C. (2001). Secure and Invisible Data Hiding in 2-Color Images. *Proceedings - IEEE INFOCOM*, 2, 887–895.
- Perez-Gonzalez, F., & Hernandez, J. R. (1999). A Tutorial on Digital Watermarking. In *Proceeding of IEEE 33rd Annual International Carnahan Conference on Security Technology*, 286-292.
- Quadir, A., & Ahmad, I. (2005, October). Digital Text Watermarking: Secure Content Delivery and Data Hiding in Digital Documents. In *Proceeding of 39th Annual International Carnahan Conference on Security Technology*, (CCST'05), (pp. 101- 104).
- Schulzrinne, G., Paul, S., Maxemchuk, N. F., & Choudhury, A. K. (1995, May/June). Copyright Protection for Electronic Publishing Over Computer Networks. *IEEE Network*, 9(3), 12–20. doi:10.1109/65.386048
- Sencar, H. T., & Memon, N. (2005, November). Watermarking and Ownership Problem – A Revisit. In *Proceedings of the 5th ACM workshop on Digital rights management*, (pp. 93-101).
- Sheppard, N. P., Safavi-Naini, R., & Liu, Q. (2003). Digital Rights Mangement for Content Distribution. In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*, 21, 49-58.
- Sun, X., Luo, G., & Huang, H. (2004, November). Component-Based Digital Watermarking of Chinese Texts. In *Proceedings of the 3rd international conference on Information security*, 81, 76-81.
- Theimert, S., Steinebach, M., & Wolf, P. (2006, September). A Digital Watermarking for Vector-Based Fonts. In *Proceedings of the 8th workshop on Multimedia and security*, (pp. 120-123).
- Wong, P. W., & Memon, N. (1998, July). Protecting Digital Media Content. *ACM Communication*, 41(7), 35–43. doi:10.1145/278476.278485
- Wu, M., & Liu, B. (2004, August). Data Hiding in Binary Image for Authentication and Annotation. *IEEE Transactions on Multimedia*, 6(4), 528–538. doi:10.1109/TMM.2004.830814
- Wu, M. Y., & Lee, J. H. (1998, December). A Novel Data Embedding Method for Two-Color Facsimile Images. In *Proc. International Symposium on Multimedia Information Processing*, Taiwan, R.O.C.
- Zhang, W., Zeng, Z., Pu, G., & Zhu, H. (2006). Chinese Text Watermarking Based on Occlusive Components. In 2nd IEEE Information and Communication Technologies, ICTTA ‘06, 1, (pp. 1850-1854).
- Zhao, J., Koch, E., & Luo, C. (1998, July). In business Today and Tomorrow. *ACM Communication*, 41(7), 66–72.

KEY TERMS AND DEFINITIONS

E-DRM: It is a system that can be entrusted for monitoring, regulating, and pricing of each subsequent use of literary resource that may also contains other media contents. This comprises of supporting dissemination technologies, designing tools and processes that can protect intellectual property during digital content commerce.

Digital Watermarking: It is a data hiding technique of hiding a digital code irremovably, robustly and imperceptibly into a digital host data. Watermarking enables appropriate follow up action in case of suspected infringements of rights. The artifact recites the authority a recipient

enjoys over the acquired content and the artifact is referred as Watermark

Right of Fair Use: This doctrine of Copyright Act distinguishes act of tampering done with the malicious intention from that of evaluation purposes. This doctrine allows the researchers and the innovators to test the article against various present and future threats.

Right of First Sale: This doctrine of Copyright Act permits the user who has acquired the digital asset legally to sell the copy. This doctrine is the major challenge for any watermarking system because it demands recursive marking of asset. Marking and persistence of all marks is prime concern.

Pixel Intensity Modulation: A set of watermarking techniques wherein the intensities of the certain pattern or places is modified. As a consequence of the operation, modulated portion within the host becomes dominant. This leads to the colour enhancement of certain sites within the host. These are fully synchronized processes.

Block-wise Coding Scheme: A font and format independent data hiding scheme where the host is compartmentalized into equal sized host. The data is hidden by flipping the pixel values either in each block or block complaint to invariants defined. With these techniques block selection is the most cumbersome task which significantly affects its execution performance.

Font Feature Coding: These techniques primarily modifies the appearance of a character. The modification may be changing the height of specific character or increasing the thickness of character. Algorithms belonging to this category are highly dependent on language used in the document as each language has its own font formats.

Character Displacement: This technique mainly encodes the data by displacing the characters either left or right of its original position. This technique will also lead to changes in spaces around the text part. The displacement is per character basis.

Diacritics Coding and Space Modulation: Diacritics are the special font strokes that add artistic aesthetics to text without changing the meaning of the characters. In diacritics coding is performed among the available diacritics where either the plain text is converted to fully diacritic version or two separate set of diacritics is used to encode the bits. Similarly, a space modulation technique modifies the spacing between the constituent components like syllables, words, lines and paragraphs. Diacritic coding is specifically applicable to Arabic while the space coding can be implemented for any language.

Chapter 9

Blind Watermarking of Three-Dimensional Meshes: Review, Recent Advances and Future Opportunities

Kai Wang

Université de Lyon, CNRS, INSA-Lyon, France

Guillaume Lavoué

Université de Lyon, CNRS, INSA-Lyon, France

Florence Denis

Université de Lyon, CNRS, Université Lyon, France

Atilla Baskurt

Université de Lyon, CNRS, INSA-Lyon, France

ABSTRACT

Digital watermarking of three-dimensional (3-D) meshes has numerous potential applications and has received more and more attention from both academic researchers and industrial practitioners. This chapter focuses on the study of blind mesh watermarking techniques, which do not need the original cover mesh for watermark extraction and thus have a much larger application range than the non-blind techniques. The authors first review the existing methods proposed so far, by classifying them into three groups: fragile schemes, high-capacity schemes and robust schemes. They then present their recent work on quantization-based blind watermarking of semi-regular meshes. Finally, some future working directions are suggested.

INTRODUCTION

Nowadays, 3-D models are more and more used in applications such as medical imaging, digital entertainment and computer-aided design, mainly

due to the processing capability improvement of ordinary PCs and the bandwidth increase of network infrastructure. A 3-D model is often numerically represented as a mesh, which is a collection of polygonal facets targeting to constitute an appropriate piecewise linear approximation of the surface

DOI: 10.4018/978-1-61520-903-3.ch009

Table 1. The increasing number of mesh-watermarking research papers in EI Compendex

Year	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
Paper number	1	2	0	5	7	16	26	27	21	36

of a real 3-D object. Although there exist many other 3-D representations (e.g. implicit surface, NURBS or voxel), polygonal mesh has become the de facto standard of numerical representation of 3-D objects due to its algebraic simplicity and high usability.

Unfortunately, like digital images and audio/video clips, 3-D meshes can be easily duplicated and redistributed by a pirate without any loss of quality. This illegal behavior infringes the intellectual property of mesh owners and could also do harm to the whole underlying commercial chains. Digital watermarking technique appears as an efficient solution to this emerging problem. Actually, since the seminal work of Ohbuchi, Masuda, & Aono (1997), there has been an increasing interest in mesh watermarking research (c.f. Table 1). Besides the robust watermark used for intellectual property protection, fragile and high-capacity mesh watermarks also have many potential applications such as mesh authentication and content enhancement.

Compared with the relative maturity of the research on image, audio and video watermarking, the research on mesh watermarking seems still in its early stage. This situation is mainly due to the fact that a 3-D mesh is normally an irregular structure and that there exist a large number of intractable attacks on watermarked meshes (Wang, Lavoué, Denis, & Baskurt, 2008a). Indeed, existing image watermarking algorithms are rarely applicable on 3-D meshes, and the design of successful blind mesh watermarking schemes, which do not need the original cover mesh for watermark extraction, is particularly difficult. Our objectives in this chapter are threefold: 1) to provide a complete literature review on blind

mesh watermarking research, 2) to present some recent advances in this research field, and 3) to propose several potentially interesting future working directions. Before presenting the technical contents on 3-D mesh watermarking, in the following we will first provide some background knowledge on polygonal meshes.

Background Knowledge on Polygonal Meshes

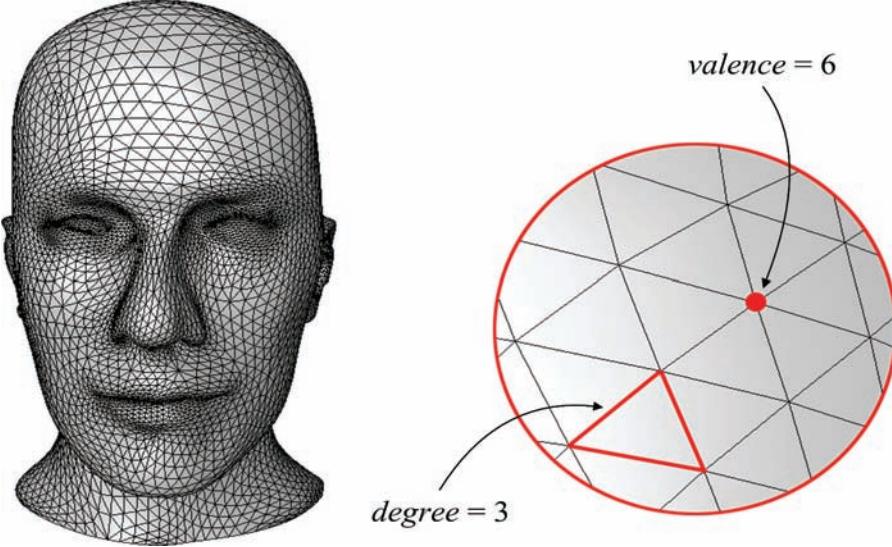
A 3-D mesh has three different combinatorial elements: vertices, edges and facets (typically triangles or quadrangles). The coordinates of the vertices constitute the geometry information of the mesh, while the edges and facets describe the adjacency relationships between vertices and constitute the mesh's connectivity information. Mathematically, a mesh \mathcal{M} containing N vertices and M edges can be modeled as a signal $\mathcal{M} = \{\mathcal{V}, \mathcal{E}\}$, where

$$\mathcal{V} = \left\{ v_i = (x_i, y_i, z_i) \mid i \in \{1, 2, \dots, N\} \right\}, \quad (1)$$

$$\mathcal{E} = \left\{ e_j = (p_1^{(j)}, p_2^{(j)}) \mid j \in \{1, 2, \dots, M\}; p_1^{(j)}, p_2^{(j)} \in \{1, 2, \dots, N\} \right\} \quad (2)$$

More precisely, each vertex v_i is described by its three-dimensional coordinates (x_i, y_i, z_i) ; each element in \mathcal{E} stands for an edge connecting two different vertices indexed by $p_1^{(j)}$ and $p_2^{(j)}$, respectively. Instead of the list of edges \mathcal{E} , the mesh connectivity information can also be completely described by a list of facets $\mathcal{F} = \{f_k \mid k \in \{1, 2, \dots, L\}\}$, where L is the number

Figure 1. The mannequin mesh model (on left) and a close-up of this model illustrating the concepts of vertex valence and facet degree (on right)



of facets of the mesh. Each facet from the list \mathcal{F} is normally represented by a sequence of indices of its component vertices that are sorted in a certain cyclic order around it. A mesh is called triangular if all its facets are triangles; similarly we can define a quadrangular mesh. Figure 1 shows an example of 3-D mesh. As illustrated by the close-up on the right part of this figure, the valence of a vertex is the number of its incident edges and the degree of a facet is the number of its component edges. The 1-ring neighbors of a vertex are the vertices that are directly connected to it by a certain edge.

A mesh is regular if all its vertices have a same valence. A semi-regular mesh is a piecewise regular structure and consists of a patchwork of large regular regions; hence, it owns regular vertices almost everywhere. Otherwise, we say that the mesh is irregular. A mesh is called manifold if the neighborhood of every vertex is homomorphic to a disk or a half-disk. The orientation of a facet can be defined according to the cyclic order of its component vertices. Obviously, there exist two possibilities for this orientation. The orientations of two adjacent facets are called compatible if the two shared vertices are in opposite orders in these

two facets. The entire mesh is called orientable if we can find a combination of the orientations of all its facets such that each pair of adjacent facets in the mesh is compatible.

For more background knowledge on polygonal meshes and particularly their applications in geometry processing, readers could refer to the Siggraph course notes of Botsch et al. (2007).

Three-Dimensional Mesh Watermarking and Its Applications

The basic idea of digital watermarking technique is to hide a piece of imperceptible information in the functional part of a multimedia file. This embedded information can later be extracted and used in a variety of applications. We summarize here three main applications of mesh watermarking techniques.

- **Intellectual property protection.** A robust and imperceptible watermark is embedded in the cover mesh. The watermark conveys a piece of copyright-related information and should be able to survive conventional

- operations and malicious attacks on the watermarked mesh.
- **Content authentication.** A so-called fragile or semi-fragile watermark is embedded in the mesh. This watermark is intentionally designed to be vulnerable to certain kinds of non-tolerable operations, while being robust or invariant to tolerable operations. Based on its extraction result, we can at least tell whether or not the watermarked mesh has undergone non-tolerable operations after watermark embedding and before authentication. A well-designed fragile watermark can also provide some information concerning the location and/or the nature of the endured attack.
- **Content enhancement.** The purpose of this type of watermarks is simply to hide a piece of auxiliary and content-related information in the cover mesh so as to enhance its utility or to provide a supplementary service. This information can be, for example, the model's generation information, some keywords for model retrieval from a database, or the address of a webpage containing some explanations on how to use the model. Instead of robustness or fragility, the main concern here is often the requirement of a high watermarking capacity, which means that a large number of bits (normally around a few thousand) should be hidden in the mesh.

A non-blind watermarking scheme needs the original copy of the protected multimedia file for extracting the embedded watermark. Contrarily, a blind watermark can be correctly extracted without referring to the original cover content. Obviously, blind watermarking schemes have a much larger application range than the non-blind schemes. Indeed, in real-world applications, the original content cannot always be or even should not be present at the extraction phase. For instance, in copy control applications, it is inappropriate to

make the original copy available in the control device that is probably in the hand of a malicious client. It is also meaningless to design a non-blind fragile watermark for content authentication, because the authentication task becomes trivial or even unnecessary if the receiver has the original version. Hence, in this chapter, we focus on the study of blind mesh watermarking techniques.

Organization of the Chapter

The remainder of this chapter is organized as follows. In the next section, we will briefly review the existing blind mesh watermarking methods, by classifying them as robust, fragile or high-capacity schemes. Then, we present our recent work on quantization-based blind watermarking of semi-regular meshes. In our wavelet-based hierarchical watermarking framework, three different watermarks (a robust one, a high-capacity one and a fragile one) can be simultaneously embedded in a same semi-regular mesh for being used in different applications (copyright protection, content enhancement and content authentication). Finally, we suggest several future working directions and draw the conclusions.

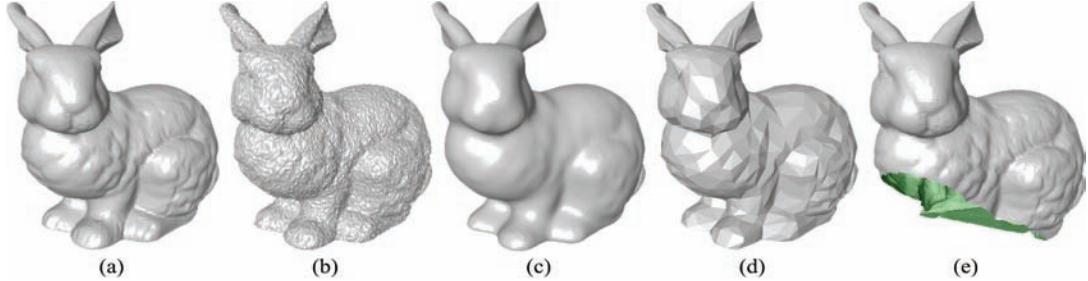
REVIEW ON BLIND MESH WATERMARKING

This section presents the state of the art on blind mesh watermarking. Interested readers could refer to the papers of Rondao-Alface & Macq (2007) and of Wang et al. (2008a) for two recent comprehensive surveys on 3-D mesh watermarking.

Difficulties and Classification

So far, still very few blind mesh watermarking methods have been proposed. This situation is mainly due to two difficulties: 1) the irregular sampling intrinsic to a 3-D mesh and 2) the complexity of the possible attacks on watermarked

Figure 2. The Stanford Bunny model and four attacked versions: (a) the original one; (b) after random noise addition; (c) after smoothing; (d) after simplification; (e) after cropping



models. These two problems will be addressed in the following paragraphs.

In the case of 2-D image watermarking, the cover image can be considered as a matrix, and each pixel as an element of this matrix. This means that all pixels have an intrinsic order in the image, for example the order established by row or column scanning. This order is usually used to synchronize watermark bits. On the contrary, there is no simple, robust and intrinsic ordering for the combinatorial elements of a 3-D mesh, which often constitute the watermark bit carriers (primitives). Some intuitive orders, such as the order of the vertices and facets in the mesh file, or the order of vertices obtained by ranking their projections on an axis of the objective coordinate system, are easy to be altered. Moreover, because of their irregular sampling nature, we still lack an effective spectral analysis tool for 3-D meshes. This situation makes it difficult to devise successful spectral mesh watermarking schemes.

In addition to the above point, robust watermarks also have to face various intractable attacks. The reordering of vertices and facets in the mesh file does not have any impact on the shape of the watermarked model, but it can desynchronize the watermark that relies on this straightforward ordering. The similarity transformations, including translation, rotation, uniform scaling and their combination, are supposed to be common operations through which a robust watermark, or even a fragile or a high-capacity

watermark, should be able to survive. Moreover, original watermarking primitives (e.g. vertices, edges or facets) could disappear after a mesh simplification or remeshing. Such attacks can be easily performed by using some freely available software tools, and they can completely destroy the geometry and the connectivity information of the watermarked mesh while well preserving its global shape. Usually, we distinguish between the geometry attacks, which only modify the positions of the vertices, and the connectivity attacks, which also change the connectivity aspect of the mesh. Typical geometry attacks include noise addition, smoothing and vertex coordinate quantization. Examples of connectivity attacks are surface subdivision, simplification, remeshing and cropping. Figure 2 illustrates the original Stanford Bunny mesh and some attacked versions of this model.

It has been theoretically proven that the requirement of blindness does not cause any performance loss to a watermarking method, at least under certain assumptions (Costa, 1983). However, practically, a blind mesh watermark is normally much less robust than a non-blind one. In the non-blind case, the availability of the original cover mesh makes watermark extraction easier, mainly in sense that it can facilitate the watermark synchronization process, especially under connectivity attacks. Therefore, devising a robust and blind mesh watermarking scheme seems a challenging task. Particularly, for such a scheme, we should

select an appropriate watermarking primitive and establish a robust synchronization mechanism.

In the following, we will present the existing blind mesh watermarking algorithms by classifying them as fragile, high-capacity and robust techniques. In each class, it seems convenient to subdivide the members into two subclasses, depending on whether the watermark is embedded in the spatial domain (by directly modifying the mesh geometry or connectivity) or in a transform domain (by modifying the coefficients obtained after a certain mesh transformation).

Fragile Techniques

A fragile watermarking scheme used for content authentication often has to possess two features: it should be vulnerable to the non-tolerable operations, even with very small amplitudes; and it should be capable of locating, or even identifying the endured attacks. In the case of 3-D meshes, we often require that an authentication watermark should be immune to the so-called content-preserving operations that include vertex/facet reordering and similarity transformation, while being vulnerable to other geometry and connectivity attacks.

Fragile Techniques in Spatial Domain

As mentioned before, the spatial description of a 3-D mesh includes a geometry aspect and a connectivity aspect. We begin with the techniques modifying the geometry.

Fragile Techniques in Spatial Domain Modifying the Geometry

Yeo & Yeung (1999) proposed the first fragile mesh watermarking scheme in the literature. Their basic idea is to search for a new position for each vertex where two predefined hash functions have an identical value, in order to make all vertices valid for authentication. At extraction, one simply examines the validity of each vertex by verify-

ing the equality between the two hash function values, and locates the attacks on invalid vertices. The watermark embedding algorithm depends on the vertex orders that are pre-established in the mesh file, so as to prevent the causality problem. Formally, the causality problem means that the embedding of the posterior watermark bits impacts the synchronization of the anteriorly embedded ones, or directly changes the feature values of the watermarking primitives where the anterior bits are embedded; hence, the extracted bits can be different from the original ones, even in the absence of attacks. In the algorithm of Yeo & Yeung (1999), the first hash function is dependent only on the position of the current vertex that is to be watermarked, but the second one also depends on the positions of its 1-ring neighbors. When considering these neighbors for hash function calculation, the authors only take into account the already watermarked ones, which are in front of the current vertex in the pre-established ordering. Without this precondition, the causality problem occurs, which in this case means that the watermarking of a certain vertex will impact the validities of its 1-ring neighbors that have already been marked at that moment. Therefore, the scheme of Yeo & Yeung (1999) is fragile to vertex reordering.

Lin, Liao, Lu, & Lin (2005) considered vertex reordering as an operation that even a fragile watermark should be able to resist because it is harmless to the mesh shape. Thus, they solved the causality problem and at the same time achieved the invariance to vertex reordering by setting both hash functions in their scheme dependent only on the coordinates of the to-be-watermarked vertex. Chou & Tseng (2006) solved the causality problem by introducing the concept of adjusting vertex. In their algorithm, one of the two hash functions is dependent on the barycenter of the vertex's 1-ring neighbors. However, nearly every watermarked vertex has an adjusting vertex selected from its neighbors. The positions of the adjusting vertices are tuned after the displacement of watermarked

vertices, so as to recover the barycenter of the neighbors of each watermarked vertex to its original value. Another feature is that the displacement upper-bound for watermarked vertices is accurately controlled so that severe distortions are avoided. Wu & Chueng (2006) proposed a fragile scheme by choosing the distance from a vertex to the centroid of its already traversed and watermarked neighbors as authentication primitive. Their watermark is invariant to similarity transformation but vulnerable to vertex/facet reordering because their vertex traversal algorithm is based on the original vertex/facet indices in the mesh file. Recently, Wang, Zheng, Yong, & Gu (2008) pointed out that we can avoid the causality problem by simply making the watermarked vertices not adjacent to each other. Based on this idea, they proposed a fragile scheme similar to that of Chou & Tseng (2006). Meanwhile, compared to the other schemes that use floating-point arithmetic, the algorithm of Wang et al. (2008) is numerically stable since it only uses bit operation and integral arithmetic to carry out watermark embedding and extraction. However, as the other fragile methods that are based on the equality of two hash function values (Yeo & Yeung, 1999; Lin et al. 2005; Chou & Tseng, 2006), this scheme is not immune to similarity transformation.

Fragile Techniques in Spatial Domain Modifying the Connectivity

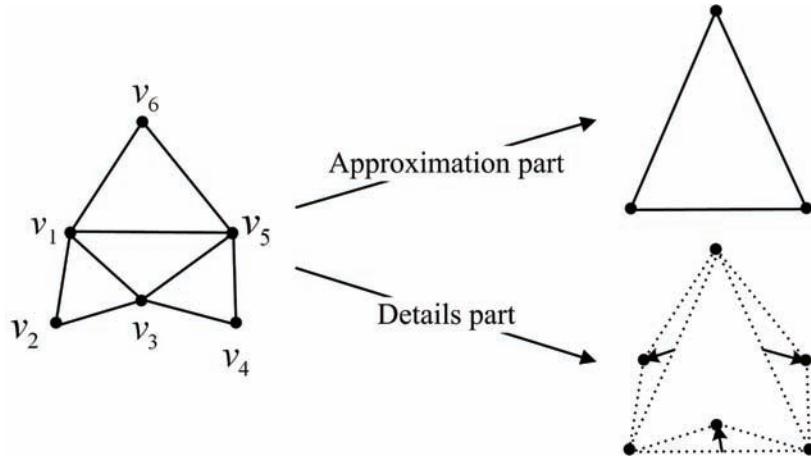
Ohbuchi et al. (1997) presented two visible mesh watermarking algorithms based on connectivity modification. In the first algorithm, the local triangulation density of the cover mesh is changed to embed the watermark. The second algorithm first cuts one band of triangular facets off the mesh and then glues it to the cropped mesh with just one edge. In these two methods, the embedded watermarks do not spread all over the mesh; this fact, along with their visibility to human eyes, stops them from being useful fragile watermarks due to the lack of attack localization capability and security.

Fragile Techniques in Transform Domain

Usually, researchers choose to operate in a kind of spectral domain with the objective to improve imperceptibility, resistance or security of a robust algorithm, mainly by making use of the masking effect of the human visual system and the spreading effect of the embedded watermark in all the spatial/temporal parts of the cover content. However, in the case of 3-D meshes, multiresolution analysis seems more flexible than the other spectral-like transforms, in sense that it is possible to construct all types of watermarks (robust, fragile and high-capacity) in the obtained multiresolution domain.

3-D mesh multiresolution analysis (Dodgson, Floater, & Sabin, 2004) is a useful tool to reach an acceptable trade-off between the mesh complexity and the processing, storage or visualization capacity of the available resource. Such an analysis produces a coarse mesh that represents the basic shape (low frequencies) of the model and a set of details information at different resolution levels (median and high frequencies). During the dual synthesis process, we can obtain a series of reconstructed meshes, all representing a same 3-D object but with different complexities, i.e. resolutions. As mentioned above, the most interesting point of the multiresolution analysis for watermarking is its flexibility: there are different embedding locations that can satisfy different application requirements. For example, embedding in the coarsest representation ensures a good robustness, while embedding in the details parts provides an excellent capacity. Under the same additive embedding intensity, embedding in the mesh low resolution component can be both more robust and more imperceptible because it makes the object globally expand or contract a little, while not introducing annoying distortions. Embedding in high resolution levels may lead to the construction of some effective fragile watermarking schemes that are capable of precisely locating the endured attacks.

Figure 3. Lazy wavelet decomposition of semi-regular triangular meshes



Wavelets are a common tool for carrying out mesh multiresolution analysis. The mathematical formulation of the wavelet analysis and synthesis of 3-D meshes was introduced by Lounsbery, DeRose, & Warren (1997). Figure 3 illustrates the principle of the lazy wavelet decomposition mechanism for semi-regular triangular meshes. In each iteration, a group of four triangles is merged in one and three of the six initial vertices (even vertices, v_2, v_4, v_6 in Figure 3) are conserved in the lower resolution. The wavelet coefficients are calculated as the prediction errors for all the removed vertices (odd vertices, v_1, v_3, v_5 in Figure 3) and they are 3-D vectors associated with each edge of the coarser mesh. A straightforward prediction is used here, which is the midpoint of the two even vertices having been incident to the odd vertex. Such an analysis can be iteratively applied on a dense mesh with subdivision semi-regular connectivity, and the dual synthesis algorithm can accomplish the inverse reconstruction.

Cho, Lee, Lim, & Park (2005) proposed a fragile watermarking scheme for semi-regular meshes based on the wavelet transform. They first apply several wavelet decompositions on the original dense mesh and then consider the facets in the obtained coarse mesh as authentication primitives. The basic idea is to slightly modify the shape of

each facet so that the values of two predefined hash functions on this facet are the same. The inputs of both functions are invariant to similarity transformations. However, it seems that there exist two problems: first, the causality problem occurs because the modification of a certain facet can influence the validities of its neighboring facets that have already been watermarked, and this problem is not discussed by the authors; second, the watermark is embedded in a relatively coarse mesh obtained after several wavelet decompositions, which seems disadvantageous to provide precise attack localization capability. Later in this chapter, we will present a new fragile scheme for semi-regular meshes, which does not suffer from the causality problem and is also capable of precisely locating the endured attacks.

Table 2 summarizes and compares the performances of the existing fragile mesh watermarking algorithms. We can see that not any of them is invariant to both element (vertex/facet) reordering and similarity transformation, while being able to precisely locate the endured attacks.

High-Capacity Techniques

The objective of a high-capacity watermarking method is simply to hide a large amount of

Table 2. Performance comparison of different fragile mesh watermarking schemes

Method	Invariance to element reordering	Invariance to similarity transformation	Attack localization
Yeo & Yeung (1999)	No	No	Yes
Lin et al. (2005)	Yes	No	Yes
Chou & Tseng (2006)	Yes	No	Yes
Wu & Chueng (2006)	No	Yes	Yes
Wang et al. (2008)	Yes	No	Yes
Cho et al. (2005)	Yes	Yes	Not precisely

information within the cover mesh. Sometimes, it is also desired that the embedded watermark should be invariant to certain kinds of operations, such as the element reordering and the similarity transformation.

Most high-capacity methods are based on the modification of individual vertex coordinates. Cayre & Macq (2003) proposed a high-capacity blind data hiding algorithm for triangular meshes. The chosen watermarking primitive is the projection of a vertex on its opposite edge in a triangle. The capacity of their scheme can attain 1 bit/vertex. The synchronization mechanism of this algorithm relies on the choice of the first triangle according to a certain geometric criterion (e.g. one of the triangles intersecting with the most significant principal axis of the mesh) and a further geometric spreading scheme that is guided by a secret key. A higher capacity, which is about 3 bits/vertex, is achieved by Wang & Cheng (2005) by applying a multi-level embedding procedure. This procedure consists of modifying successively the parallel, vertical, and rotary positions of a vertex related to its opposite edge in a triangular facet. Cheng & Wang (2007) further improved the capacity of their scheme by adaptively embedding more bits in rough regions of the cover mesh where the induced distortions are less visible to human eyes.

Some other methods (Cheng & Wang, 2006; Bogomjakov, Gotsman, & Isenburg, 2008) modify the orders of the vertices and facets in the mesh file

to embed high-capacity watermarks. Particularly, Bogomjakov et al. (2008) proposed a fast and sub-optimal variant of the standard permutation steganography (Artz, 2001), which can achieve a capacity of $(\log_2 n!) - n + 1$ bits on a dataset of n elements. For polygonal meshes, such a dataset used for watermark embedding can be the vertex or the facet list. The basic idea of the permutation steganography is that there are $n!$ possible permutations for the n elements in the dataset; therefore, we can hide in maximum a message of $\log_2 n!$ bits by properly setting this permutation. These order-based methods have much higher capacities than the geometry-based methods presented in the last paragraph. In addition, they do not introduce any distortion to the cover mesh and also have the advantage of being invariant to geometry attacks. Their main drawback is that the embedded message can also be easily removed by a simple vertex/facet reordering, without inducing any distortion. Hence, in a practical application, we should carefully choose between geometry-based techniques and order-based techniques, according to the application's robustness requirement, if there is any.

Finally, it is worth pointing out that high-capacity watermarks are often fragile (in sense that they are not robust), and some of them have the potential to be successful fragile watermarks with a precise attack localization capability and the invariance to all the content-preserving operations.

Robust Techniques

A robust technique should at least be able to resist the attacks that cause distortions smaller than a certain threshold beyond which the watermarked mesh is greatly degraded. The main difficulty in devising a robust and blind mesh watermarking scheme is how to achieve the robustness against connectivity attacks without referring to the original cover mesh during watermark extraction.

Robust Techniques in Spatial Domain

Between the geometry and the connectivity of a 3-D mesh, nearly all the existing spatial robust algorithms take the former as primitive. Actually, it is almost impossible for a blind scheme based on mesh connectivity modification to withstand connectivity attacks.

Benedens (1999) presented a robust method based on the mesh's Extended Gaussian Image (EGI). First, the EGI of the cover mesh is established by clustering facets according to their normal directions. Then, in each bin of the EGI, the average normal direction of its component facets is modified to hide one bit. Since these average normal directions roughly describe the shape of the mesh, this scheme possesses a relatively good robustness against surface simplification and remeshing. Instead of EGI, Lee & Kwon (2007) adopted Complex EGI for mesh watermarking. They construct the EGI in the same way as Benedens (1999), but associate each bin with a complex weight, which depends not only on the total surface of the bin's component facets but also on the proximity of these facets. In their algorithm, the bins with bigger complex weights are selected as watermark bit carriers, and this selection is proven effective to reinforce the robustness. Both algorithms need to recover the original mesh pose in 3-D space at the watermark extraction phase, in order to achieve an invariant EGI or Complex EGI. For this purpose, some feature values of the cover mesh have to be transmitted to the watermark

extraction side. This constraint makes these two algorithms semi-blind.

Recently, researchers have attempted to embed watermarks in certain kinds of shape histograms. Zafeiriou, Tefas, & Pitas (2005) first calculate the center and principal axes of the mesh object and afterwards convert the vertex coordinates into the registered spherical coordinate system (r, θ, φ) , then they divide the vertices into several groups associated with different ranges of θ . The histogram of the prediction errors of the vertex radial components is constructed for each group. The prediction is calculated from the vertex 1-ring neighbors by applying a local neighborhood operator. The authors assume that the obtained histograms are of Gaussian distribution, and then embed one bit in each vertex group by modifying the shape of this distribution. The idea is to change the one-side variance of the assumed Gaussian distribution either on the left or on the right so as to indicate the bit '-1' or the bit '+1', respectively. Similarly, Cho, Prost, & Jung (2007) construct the histogram of the distances between vertices and the mesh gravity center, and then divide this histogram in bins associated with different ranges of this distance. They make the hypothesis of a uniform histogram distribution in the obtained bins. One bit is embedded in each bin by slightly modifying the mean value (or the variance) of the distribution in the bin. Both methods are blind and robust against most kinds of attacks except for cropping and anisotropic connectivity changes, mainly because the calculation of the mesh center and principal axes in these two methods is not stable under such attacks. In addition, as in the case of image watermarking, the methods that are based on histogram modification normally have a low security level. Finally, note that the two schemes have different strategies to achieve invariance to similarity transformations, either by carrying out a blind and robust mesh registration at extraction to recover the same canonical pose as that during watermark embedding (Zafeiriou et al., 2005), or by using an invariant watermarking primitive, i.e.

the distribution of the distances from vertices to mesh center (Cho et al., 2007).

To sum up, we can see that in order to resist connectivity attacks in a blind way, the existing spatial methods select certain kinds of connectivity-invariant features as their watermarking primitives. Such features, to some extent, capture the essential property of the mesh shape, and thus are more or less preserved after connectivity changes.

Robust Techniques in Transform Domain

Most successful robust and blind image watermarking algorithms are based on spectral analysis. A better imperceptibility can be obtained due to the spreading effect of the embedded watermark in all the spatial parts of the cover content, and by taking advantage of the masking effect of the human visual system. A better robustness can also be achieved if the watermark is embedded in the low and medium frequency components because these components are perceptually important and thus are less likely to be changed under attacks. However, unfortunately, most of the existing spectral-like transformations for 3-D meshes are either inefficient in terms of computational cost or unstable under attacks. We are only aware of very few blind transform-domain-based mesh watermarking schemes, which are either in the wavelet domain of semi-regular meshes (Uccheddu, Corsini, & Barni, 2004) or in the Fourier-like spectral domain of general meshes (Cayre, Rondao-Alface, Schmitt, Macq, & Maître, 2003; Luo & Bors, 2008; Liu, Prabhakaran, & Guo, 2008; Wang, Luo, Bors, & Denis, 2009; Luo, Wang, Bors, & Lavoué, 2009).

By using the wavelet analysis presented in the subsection titled “Fragile Techniques in Transform Domain”, Uccheddu et al. (2004) described a correlation-based robust and blind one-bit watermarking algorithm for semi-regular meshes. In their method, the cover semi-regular mesh is first normalized to a canonical spatial pose, and

then the watermark signal is embedded through additive modulation of the norms of the wavelet coefficient vectors at a certain appropriate resolution level. In the next section, we will present a robust and blind multi-bit watermarking method for semi-regular meshes, which is also based on the wavelet transform.

In the conventional combinatorial Laplacian spectral analysis of general meshes, we first construct a symmetric Laplacian matrix D of dimension $N \times N$ (N being the number of mesh vertices) purely depending on the mesh connectivity. If the vertices v_i and v_j are connected by an edge, then the elements d_{ij} and d_{ji} of the matrix D are set to be -1; otherwise, they are set to be 0. Each diagonal element d_{ii} is equal to the valence of the vertex v_i . We carry out eigen-decomposition of this matrix and obtain its N eigenvectors and N eigenvalues. Then, the eigenvectors are normalized so as to have unit norms, and are also sorted in an ascending order according to their associated eigenvalues, i.e. their associated frequencies. The N -sized spectral vectors $\tilde{\mathbf{x}} = (\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_N)$, $\tilde{\mathbf{y}} = (\tilde{y}_1, \tilde{y}_2, \dots, \tilde{y}_N)$, $\tilde{\mathbf{z}} = (\tilde{z}_1, \tilde{z}_2, \dots, \tilde{z}_N)$ are calculated respectively as the projections of the three vertex coordinate vectors $\mathbf{x} = (x_1, x_2, \dots, x_N)$, $\mathbf{y} = (y_1, y_2, \dots, y_N)$, $\mathbf{z} = (z_1, z_2, \dots, z_N)$ on the N normalized and sorted eigenvectors. The i -th spectral amplitude can be defined as $c_i = \sqrt{\tilde{x}_i^2 + \tilde{y}_i^2 + \tilde{z}_i^2}$. This mesh spectral analysis was originally derived within the framework of graph theory (Biggs, 1993), and then used by Karni & Gotsman (2000) for mesh geometry compression. It was later introduced by Ohbuchi, Mukaiyama, & Takahashi (2002) for robust mesh watermarking. However, most existing watermarking methods using this spectral analysis are non-blind (Ohbuchi et al., 2002; Abdallah, Ben Hamza, & Bhattacharya, 2007; Lavoué, Denis, & Dupont, 2007) because the obtained spectral coefficients are not robust against connectivity attacks. A re-sampling pre-processing is necessary at extraction to recover the same connectivity configuration as the cover

mesh to ensure a satisfactory robustness, but this step inevitably makes the algorithm non-blind.

Blindness in the Laplacian spectral domain was first exploited by Cayre et al. (2003). Two recently proposed blind methods (Luo & Bors, 2008; Liu et al., 2008) have achieved a better robustness, especially against connectivity attacks. In the method of Luo & Bors (2008), the robustness relies on the stability of the constraints embedded in sets of high-frequency coefficients obtained after the combinatorial spectral analysis. However, this method is not applicable on large meshes having more than 10000 vertices because the calculation of the whole spectrum for such meshes is extremely time-consuming. Lately, Luo et al. (2009) improved this point by introducing a robust registration and segmentation preprocessing before watermark embedding and extraction. In this way, the cover mesh is robustly split into several small patches on which the spectral analysis is much less expensive. Unlike the other spectral schemes, the method of Liu et al. (2008) makes use of a new mesh spectrum decomposition tool, namely the manifold harmonics analysis (Vallet & Lévy, 2007; Vallet & Lévy, 2008). The manifold harmonics spectrum coefficients are quite robust, even after connectivity alterations. In the method of Liu et al. (2008), the low frequency part of the mesh spectrum is split into 5 slots. Then in each slot, one bit is embedded by modifying the relative relationship between the magnitude of a certain selected coefficient and the average magnitude of the other coefficients in the slot. Recently, Wang et al. (2009) proposed a new robust and blind method also based on the manifold harmonics analysis. Watermark bits are embedded in the cover mesh through iterative quantization of its low-frequency spectral amplitudes. Compared with the method of Liu et al. (2008), the method of Wang et al. (2009) has a higher capacity (16 bits versus 5 bits), as well as a better trade-off between the robustness and the induced distortion.

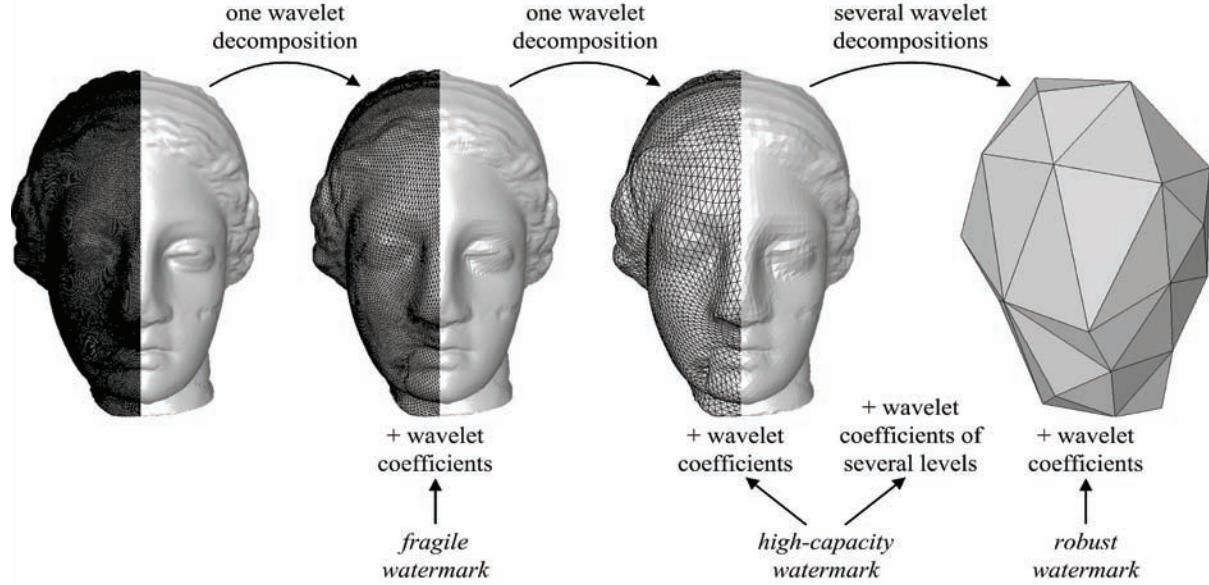
Summary

In this section, we have presented the state of the art in the field of blind mesh watermarking research. It can be seen that several open problems still exist in this research domain. For fragile watermarking, one interesting future work would be the design of a scheme that is capable of precisely locating the endured attacks and meanwhile invariant to all the content-preserving operations. For high-capacity watermarking, it is worthwhile to investigate whether it is possible to combine the ideas of geometry-based and order-based methods to construct new schemes that have the good properties of both kinds of techniques. Finally, the community seems interested in finding new spatial watermarking primitives or new robust spectral-like mesh transformations to construct blind and robust watermarking schemes with better overall performances. We were actually in part following these working direction proposals when conducting our research on blind and multiple watermarking of semi-regular meshes.

HIERARCHICAL WATERMARKING OF SEMI-REGULAR MESHES

This section presents a hierarchical watermarking framework for semi-regular meshes. Three different watermarks (robust, high-capacity and fragile) can be simultaneously embedded in a same semi-regular mesh, serving for different applications (copyright protection, content enhancement and content authentication). Indeed, the above watermarking applications are not mutually exclusive. For instance, we can imagine the following scenario: a manufacturer designs a complex car part represented by a semi-regular mesh, then he may wish to embed in this part a piece of copyright information for intellectual property protection against possible forgery; he

Figure 4. The proposed hierarchical multiple watermarking framework for semi-regular meshes



may also want to insert a fragile watermark in order to ensure that any modification on this part can be easily detected by authorized clients; and finally he may like to embed into the object some description information, such as the part design norm and its applicable car models, so as to facilitate the usage of the mesh object.

Overview of the Hierarchical Framework

The mesh multiresolution analysis based on wavelet transform (c.f. the subsection titled “Fragile Techniques in Transform Domain”) is a very suitable tool for constructing a hierarchical multiple watermarking system: first, there is no interference between different watermarks if they are embedded in the wavelet coefficient vectors (WCVs) of different levels; secondly, and also more importantly, these watermarks can be embedded at different appropriate resolution levels according to their specific objectives. Figure 4 illustrates the proposed hierarchical watermarking framework: the fragile watermark is embedded

in a dense resolution level obtained just after one wavelet decomposition of the original semi-regular mesh, by modifying the orientations and norms of the corresponding WCVs; the robust watermark is embedded by modifying the norms of the WCVs associated with the lowest resolution level; the high-capacity watermark is embedded in one or several intermediate levels by considering groups of WCV norms as watermarking primitives. In practice, the robust watermark is first embedded after a thorough decomposition, and then the high-capacity watermark and the fragile watermark are embedded successively during the reconstruction process. This embedding order effectively prevents the posteriorly inserted watermark from impacting the anteriorly inserted one(s).

All the three embedded watermarks are blind and invariant to content-preserving operations including vertex/facet reordering and similarity transformation. The robust watermark is able to resist all the common geometry attacks on the watermarked mesh, even with relatively strong amplitudes. The fragile watermark is invariant

to content-preserving operations but vulnerable to others attacks such as local and global mesh geometry modifications, since the objective is to check the integrity of the mesh shape. In addition, at extraction, these attacks can be precisely located on the surface of the attacked mesh in a blind way. The payload of the high-capacity watermark increases rapidly with the number of primitives involved in the watermark embedding.

Brief Introduction to Scalar Costa Scheme

The scalar Costa scheme (Eggers, Bauml, Tzschoppe, & Girod, 2003) has been widely used in image, audio and video watermarking to hide bits in scalar quantities, such as image pixels or audio samples. Now, we introduce this scheme to watermarking 3-D semi-regular meshes in the wavelet domain.

Without loss of generality, suppose that we want to hide a sequence of watermark symbols $a_i, i = 1, 2, \dots, N$ in a sequence of scalar quantities $d_i, i = 1, 2, \dots, N$. Each watermark symbol a_i takes its value from alphabet $\mathcal{A} = \{0, 1, \dots, R - 1\}$ and thus conveys $\log_2 R$ bits. In most cases, we set $R = 2$ so that each symbol a_i conveys one bit. In order to carry out the watermark embedding, we first construct a component-wise and pseudo-random codebook $\mathcal{U}_{d_i, t_{d_i}}$ for each d_i as follows:

$$\mathcal{U}_{d_i, t_{d_i}} = \bigcup_{l=0}^{R-1} \left\{ u = zS + l \frac{S}{R} + t_{d_i} S \right\}, \quad (3)$$

where $z \in \mathbb{Z}$ is an integer, S is the quantization step, $l \in \{0, 1, \dots, R - 1\}$ is the watermark symbol represented by the codeword u , and t_{d_i} is the i -th element of a pseudo-random sequence that is generated by using a secret key K . As an example, t_{d_i} can be uniformly distributed in $[-1/2, 1/2]$. The dither signal t_{d_i} is introduced to randomize the values of the codewords u , with the objective

to enhance the watermarking security. In this way, non-authorized watermark extraction and optimal watermark removal can in general be avoided. Note that the codewords in $\mathcal{U}_{d_i, t_{d_i}}$ represent the watermark symbols from $\mathcal{A} = \{0, 1, \dots, R - 1\}$ in a uniform and interleaved manner.

In order to insert a watermark symbol a_i in d_i , we first find in $\mathcal{U}_{d_i, t_{d_i}}$ a codeword u_{d_i} that is the closest to d_i among all the codewords whose represented symbol is equal to a_i . Then, the quantized value \hat{d}_i is calculated as:

$$\hat{d}_i = d_i + \alpha \left(u_{d_i} - d_i \right), \quad (4)$$

where α is called the distortion compensation factor. The value of α partially drives the trade-off between induced distortion, robustness and security of the watermarking system. However, we should always properly select its value so that it can at least ensure the correctness of the watermark symbol embedding. The above watermark symbol embedding procedure actually consists in pushing d_i towards u_{d_i} , at least to within the interval $(u_{d_i} - S / (2R), u_{d_i} + S / (2R))$, which is the decoding area of u_{d_i} under the nearest neighbor criterion.

The watermark extraction algorithm is blind and only requires the knowledge of the secret key K and the values of the parameters R and S . First, the same component-wise and pseudo-random codebook is constructed for each scalar quantity from which we would like to carry out the extraction. Then, we find in the established codebook the nearest codeword to the actual value of the scalar quantity. The extracted watermark symbol is simply the symbol represented by this retrieved codeword.

The Robust Watermark

In our opinion, a robust watermark for semi-regular meshes may not have to be resistant against the

connectivity attacks, since these attacks generally destroy the semi-regular multiresolution connectivity and thus the intrinsic attractiveness of such meshes. Therefore, the objective in this subsection is to construct a blind watermark that is robust against all the common geometry attacks such as noise addition, smoothing and vertex coordinate quantization. The capacity of the proposed robust scheme is 64 bits. According to Kutter & Petitcolas (1999), this 64-bit capacity ensures the embedding of the digital identifiers of the content owner, the content purchaser and the content itself, and therefore is sufficient in most intellectual property protection applications.

In general, the robustness of a blind mesh watermarking scheme depends on 1) the robustness of the watermarking primitive feature values in which the watermark is embedded and 2) the robustness of the watermark synchronization mechanism. Concerning the first point, we choose to embed the robust watermark by modifying the norms of the WCVs associated with the coarsest-level mesh obtained after a thorough wavelet decomposition of the original dense semi-regular mesh. These WCV norms are of relatively low frequency and are supposed to be robust against geometry attacks. Concerning the second point, our proposal is to use a certain robust aspect to synchronize the embedded watermark bits: the edges in the coarsest-level mesh are sorted according to their lengths; this order is experimentally very robust against geometry attacks. The watermark bits are successively embedded through scalar Costa quantization of the norms of the WCVs associated with these sorted edges (c.f. Figure 3). Moreover, in this way, the synchronization primitives (edge lengths) and the watermarking primitives (WCV norms) are separated, so the causality problem is avoided.

Algorithm 1 summarizes the embedding process of the proposed blind and robust watermarking scheme. The embedded watermark is a bit string $w_i \in \{0, 1\}, i = 1, 2, \dots, W$.

Algorithm 1. Blind and robust watermark embedding procedure.

1. Do wavelet analysis of the original semi-regular mesh \mathcal{M}_0 until its coarsest level J ; we denote the obtained irregular coarsest-level mesh by \mathcal{M}_J
2. Do descending sort of all the edges in \mathcal{M}_J according to their lengths, and denote the sorted edges by $e_i^J, 1 \leq i \leq N_J$, where N_J is the edge number of \mathcal{M}_J
3. Calculate the average length \bar{l}^J of the edges and fix the WCV norm quantization step S_{rob} as $\bar{l}^J / \varepsilon_{rob}$, where ε_{rob} is an adjustable parameter to achieve an expected trade-off between robustness and imperceptibility
4. For each edge e_i^J in the descending sort
 - 4.1 Calculate the norm of its associated WCV and denote it by $\|c_i^J\|$
 - 4.2 Construct a codebook $\mathcal{U}_{\|c_i^J\|, t_{\|c_i^J\|}}$ for $\|c_i^J\|$ according to Equation (3) with $R = 2$, $S = S_{rob}$ and a secret key K_{rob} for the generation of the dither signal $t_{\|c_i^J\|}$
 - 4.3 Quantize $\|c_i^J\|$ by using the 2-symbol scalar Costa scheme to embed a watermark bit $w_i \in \{0, 1\}$; the quantized norm $\|\hat{c}_i^J\|$ is obtained according to Equation (4) with the usage of a pre-defined distortion compensation factor α_{rob}
5. End For
6. Do mesh reconstruction until the level where the high-capacity watermark is to be embedded

If the edge number N_J is greater than the watermark bit number W , a redundant embedding is carried out in order to enhance the robustness. It can be observed that this watermarking scheme is theoretically invariant to similarity transformations, because the quantization step S_{rob} is related

to the average length of the edges in \mathcal{M}_j and therefore changes proportionally with the WCV norms, i.e. the quantized values, under similarity transformations.

The watermark extraction process is blind and also quite simple. It is sufficient to carry out a thorough wavelet analysis, reestablish the edge orders, calculate the quantization step, reconstruct the component-wise codebook for each WCV norm and finally find out its represented bit by looking for the nearest codeword in this codebook to the actual value of the WCV norm. If redundant insertion is used during watermark embedding, a simple majority voting is adopted at extraction to deduce the watermark bit values.

The High-Capacity Watermark

In this subsection, we describe a new high-capacity watermarking scheme for semi-regular meshes. The watermark is embedded through permutation alteration of the selected geometric primitives and is invariant to all the content-preserving operations. By using the proposed scheme, we can easily embed thousands of bits in an ordinary semi-regular mesh with a moderate complexity, i.e. vertex number. The embedded information, which may represent for instance a related website address or a 3-D model indexing tag, can be used to enhance the utility of the mesh or to provide an additional service.

For a mesh $\hat{\mathcal{M}}_H$ at a certain level H of the wavelet synthesis procedure carried out after the robust watermark embedding, we index its N_H WCVs according to the lengths of their associated edges, in the same way as in the robust watermarking scheme. This means that the WCV indexed by i is associated with the i -th longest edge in $\hat{\mathcal{M}}_H$.

Then we combine each WCV \mathbf{c}_i^H with another number denoted by $\text{order}_o(i)$. To obtain this number, we first calculate the residue of the norm $\|\mathbf{c}_i^H\|$ divided by a control parameter p as $\text{res}(i) = \|\mathbf{c}_i^H\| \% p$; $\text{order}_o(i)$ is the ascending

order of the value $\text{res}(i)$ among the residues of all the WCVs at the same resolution level. Similar to the quantization step S_{rob} in the robust watermarking scheme, the control parameter p is fixed as $\bar{l}^H / \varepsilon_{hc}$ and is related to the average length \bar{l}^H of the edges in $\hat{\mathcal{M}}_H$. The first five lines of Table 3 show one simple example of this calculation, where $N_H = 4$ and $p = 0.1$. For instance, $\text{res}(1)$ of $\|\mathbf{c}_1^H\|$ is equal to 0.09, which is the largest among all the residues of the four WCVs at level H , thus $\text{order}_o(1)$ is set to be 4.

The obtained numbers $\text{order}_o(1), \text{order}_o(2), \dots, \text{order}_o(N_H - 1), \text{order}_o(N_H)$ (as shown on the fifth line of Table 3) constitute a permutation of the N_H numbers ranging from 1 to N_H . It is well known that N_H different elements have $N_H!$ possible permutations. Accordingly, each possible permutation can potentially represent a watermark of $\lfloor \log_2(N_H !) \rfloor$ bits, where function $\lfloor x \rfloor$ returns the largest integer less than or equal to a real number x . The correspondence between watermarks ($\lfloor \log_2(N_H !) \rfloor$ -bit strings) and order sequences (N_H -number permutations) can be established according to the following rule: for two permutations, the one with a bigger first number (from left) represents a bigger bit string (in terms of its binary value); and if the first numbers are the same, we compare the second, and so forth. Under this rule, the permutation $1, 2, \dots, N_H - 1, N_H$ represents the smallest bit string $0, 0, \dots, 0, 0$; and the permutation $1, 2, \dots, N_H, N_H - 1$ designates the second smallest bit string $0, 0, \dots, 0, 1$. In this way, each possible watermark bit string can be represented by a permutation. Therefore, we can substitute the original permutation by a new one in order to embed a given watermark. This new permutation is established by modifying the WCV norms so as to alternate their norm residues' orders. The new norm of a WCV \mathbf{c}_i^H is determined according to Equation (5), where $\text{order}(i)$ is its expected norm residue order in the new permutation.

Table 3. A simple example of the high-capacity watermark embedding steps

Edges lengths	3.2	2.8	2.5	1.8
Edge / WCV indices (i for \mathbf{e}_i^H and \mathbf{c}_i^H)	1	2	3	4
WCV norms ($\ \mathbf{c}_i^H\ $)	0.19	0.21	0.16	0.25
Residues of $\ \mathbf{c}_i^H\ $ divided by $p = 0.1$ (res(i))	0.09	0.01	0.06	0.05
Original WCV orders (order _o (i))	4	1	3	2
Expected WCV orders (order(i))	1	3	2	4
New residues ($\frac{\text{order}(i).p}{N_H + 1}$)	0.02	0.06	0.04	0.08
New WCV norms ($\ \hat{\mathbf{c}}_i^H\ $)	0.12	0.26	0.14	0.28

$$\|\hat{\mathbf{c}}_i^H\| = \left\lfloor \frac{\|\mathbf{c}_i^H\|}{p} \right\rfloor \cdot p + \frac{\text{order}(i).p}{N_H + 1}. \quad (5)$$

The last three lines of Table 3 give one simple example of this substitutive watermark embedding procedure. It can be seen that only the residue of the WCV norm is substituted, while the difference between the WCV norm and the residue is kept unchanged.

In practice, the N_H edges are divided into several ordered groups of G edges (in each group are embedded $\lfloor \log_2(G!) \rfloor$ bits), in order to make the watermark less fragile and to avoid the calculation precision problem. Thus, the practical capacity of this method is $\lfloor N_H / G \rfloor \cdot \lfloor \log_2(G!) \rfloor$ bits. In order to enhance the watermarking security, it would be possible to deduce the new norms by using the scalar Costa scheme, with the usage of a secret key K_{hc} . Similarly to the robust watermark, the proposed high-capacity watermark is also invariant to similarity transformations.

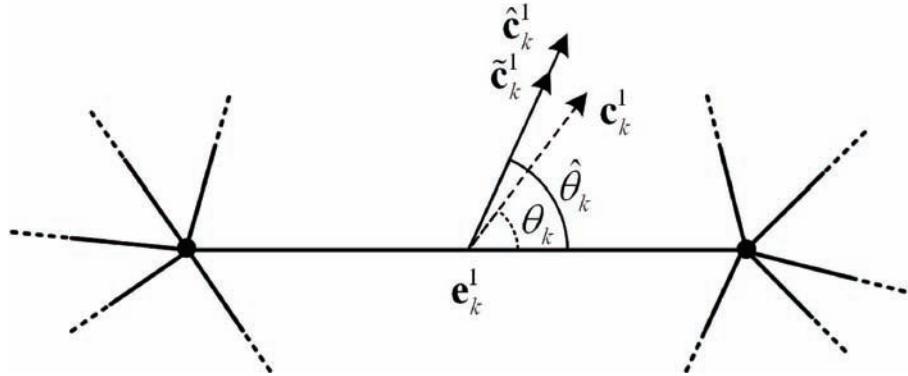
The Fragile Watermark

We recall that the objective of the fragile watermark is to be invariant to all the content-preserving operations while being vulnerable to other local and global geometry attacks. The endured attacks have also to be precisely located on the mesh surface according to the watermark extraction result.

The first step of the watermark embedding is to carry out wavelet synthesis after robust and high-capacity watermark embeddings until the second densest level (level 1). Then, we obtain a relatively dense mesh $\hat{\mathcal{M}}_1$ and a set of N_1 WCVs denoted by $\mathbf{c}_1^1, \mathbf{c}_2^1, \dots, \mathbf{c}_{N_1}^1$. Each WCV $\mathbf{c}_k^1, 1 \leq k \leq N_1$ is associated with an edge \mathbf{e}_k^1 in $\hat{\mathcal{M}}_1$. Note that, differently from the last two subsections, the fragile watermark embedding procedure is independent from these WCV and edge indices so they can be assigned arbitrarily.

The basic idea of the watermark embedding is to find two different watermarking primitives for each edge \mathbf{e}_k^1 in $\hat{\mathcal{M}}_1$ and then slightly modify them so as to embed in both of them a same

Figure 5. The fragile watermarking primitives and the modification of a WCV



watermark symbol $a_k \in \{0, 1, \dots, M_f - 1\}$. The number of eligible symbols M_f has to be big enough to ensure good performances in terms of security and authentication accuracy. Each edge is therefore made valid for authentication by establishing an equality relationship between the two implied symbols. Ideally, the two watermarking primitives have to be modified independently, and the primitives of different edges have also to be modified independently. In this way, the causality problem, either within an individual edge or between different edges, is prevented and the invariance to vertex/facet reordering is attained. We have found two such primitives: the one is the acute angle between c_k^1 and e_k^1 that is denoted by θ_k (c.f. Figure 5); the other is the ratio between the norm of c_k^1 and the length of e_k^1 that is denoted by $r_k = \|c_k^1\| / \|e_k^1\|$. Both primitives are invariant to similarity transformations. θ_k and r_k are then subject to M_f -symbol scalar Costa quantization with two different codebooks, so that the quantized values $\hat{\theta}_k$ and \hat{r}_k represent a same watermark symbol a_k .

As illustrated in Figure 5, the orientation of c_k^1 is modified first by rotating it around the midpoint of e_k^1 in the 2-D plane engendered by c_k^1 and e_k^1 , in order to obtain an intermediate temporary vector \tilde{c}_k^1 that reaches the expected angle value $\hat{\theta}_k$. Then, keeping the orientation of \tilde{c}_k^1 unchanged,

we can modify its norm in order to obtain the watermarked WCV \hat{c}_k^1 that also reaches the expected norm-length ratio value \hat{r}_k . One wavelet synthesis is then applied in order to obtain the watermarked dense mesh $\hat{\mathcal{M}}_0$.

At extraction, the first step is to carry out one wavelet decomposition of the semi-regular mesh to be authenticated. Then two codebooks for θ_k and r_k are reconstructed for each edge e_k^1 in the obtained less dense mesh. Two symbols can then be easily extracted by seeking the nearest codewords in the codebooks to the actual values of θ_k and r_k . If these two symbols are equal, the current edge is marked as valid, otherwise as invalid. The next task is to derive the validity for each vertex in the dense mesh. The validity for an even vertex in the dense mesh (c.f. Figure 3) is determined at first according to the following rule: if any of its incident edges in the less dense mesh is invalid, then it is considered as invalid; otherwise as valid. The validity of an odd vertex in the dense mesh (c.f. Figure 3) is then determined according to the validities of its two neighboring even vertices: if either of these two vertices is invalid, it is considered as invalid; otherwise as valid. Finally, the visualized authentication results are displayed to users.

Experimental Results

In this subsection, we briefly present some experimental results of the proposed hierarchical watermarking system. More results, as well as some algorithms details, can be found in Wang, Lavoué, Denis, & Baskurt (2008b).

Figure 6.(a) and 6.(b) illustrate respectively the original and watermarked Venus models. We can hardly observe any visual difference between the two meshes. In the watermarked Venus that has 163842 vertices and 491520 edges, there are three watermarks embedded. The 64-bit robust watermark is embedded at resolution level 6 (i.e. the coarsest level) that has 120 edges. The high-capacity watermark which conveys a message of 7632 bits is embedded at resolution level 4 that has 1920 edges. The fragile watermark is embedded at resolution level 1. Some of the parameter values are: $\varepsilon_{rob} = 19$, $\alpha_{rob} = 0.80$, $\varepsilon_{hc} = 100$, $G = 40$ and $M_f = 32$. The embedding and extraction times of all the three watermarks are respectively 61.2 and 14.4 seconds on a laptop equipped with a 2GHz processor and 2GB memory. These processing times are considered as acceptable in most mesh watermarking applications except for those that require real-time embedding and extraction. Moreover, the execution time varies for different models and is approximately proportional to the model's complexity, i.e. the number of its comprised vertices.

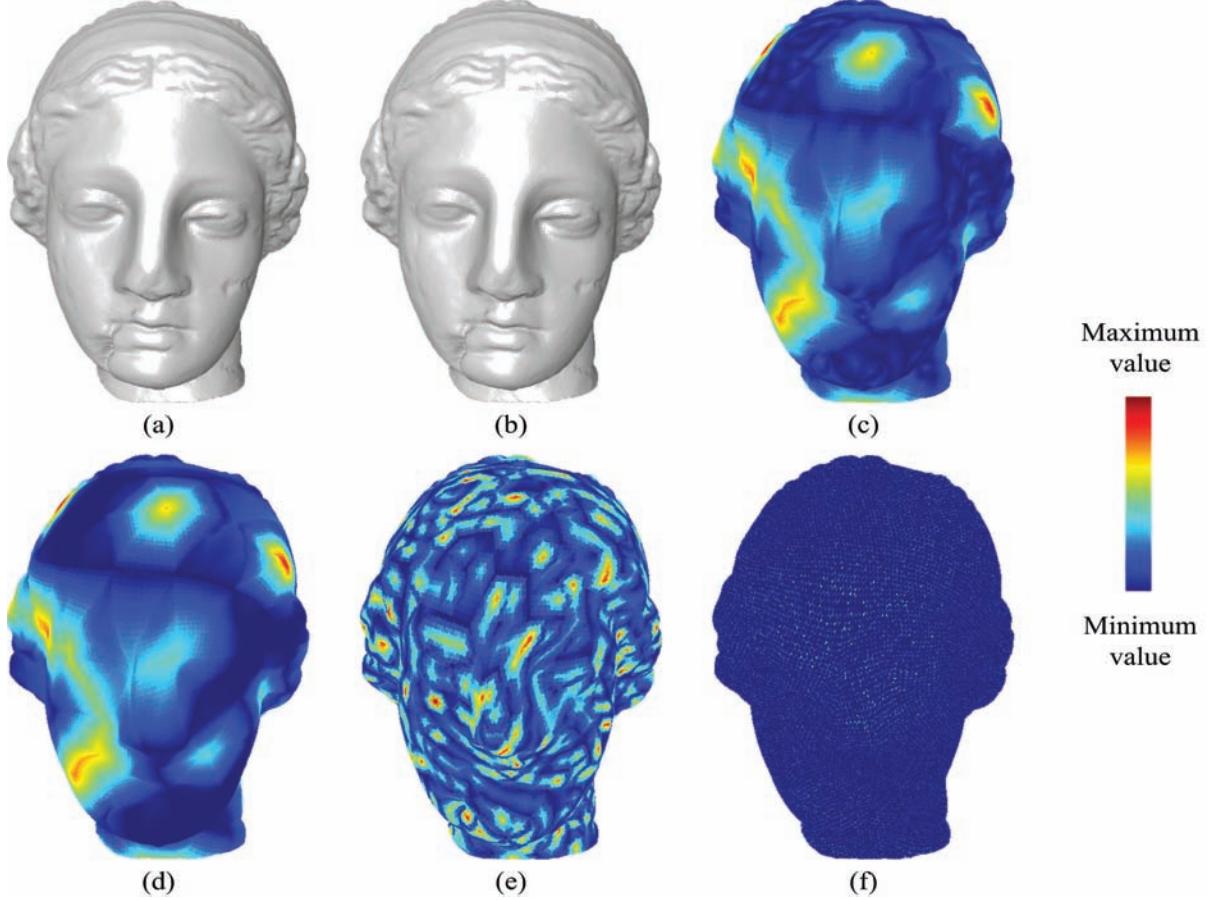
Figure 6.(c)-(f) illustrate the maps of the geometric distortions introduced by the different watermarks on the Venus model. The distortion pattern varies from relatively low frequency for the robust watermark, to intermediate frequency for the high-capacity watermark, and finally to high frequency for the fragile watermark. The maximum root mean square errors (Cignoni, Rocchini, & Scopigno, 1998) induced by the robust watermark, the high-capacity watermark, the fragile watermark and all the three watermarks are respectively 6.33×10^{-4} , 7.14×10^{-5} ,

4.21×10^{-6} and 6.36×10^{-4} , with regard to the mesh's bounding box diagonal. The maximum local distortion values of the maps illustrated in Figure 6.(c), 6.(d), 6.(e) and 6.(f) are respectively 3.06×10^{-3} , 3.66×10^{-4} , 4.70×10^{-5} and 3.06×10^{-3} , with regard to the mesh's bounding box diagonal. These maximum values are actually the Hausdorff distances (Cignoni et al., 1998) induced by the different watermarks. Both the above quantitative measurement results and the illustrations provided in Figure 6 confirm that the overall distortion of the hierarchical watermarking system is dominated by the robust watermark.

The robust watermark is experimentally invariant to vertex/facet reordering and similarity transformation. It is also fairly resistant against common geometry attacks, such as noise addition, smoothing and vertex coordinate quantization. Figure 7 shows several watermarked and attacked Venus models. The corresponding bit error rates (BER) of the extracted robust watermarks are reported in the caption of Figure 7. The obtained BER values are all relatively low under these easily perceived attacks. The high-capacity watermark is robust to content-preserving operations but fragile to other geometry attacks. It can resist until about 0.002% to 0.004% random additive noise. The maximum resistible noise amplitude seems inversely proportional to the edge number of the resolution level where the high-capacity watermark is embedded. Finally, it is important to note that the current parameter setting of the robust and high-capacity watermarks is very conservative and in favour of the watermark imperceptibility and security instead of the robustness. A better robustness can be achieved if we enhance the watermark embedding strength.

In order to verify the effectiveness of the fragile watermark, several attacked models have been prepared. These attacks include similarity transformation, local invisible noise addition, local deformation and global geometry processing. Figure 8.(a)-(d) illustrate four attacked Rabbit

Figure 6. (a) The original Venus model; (b) the stego Venus model with three watermarks embedded in it; (c) the map of the geometric distortion induced by all the three watermarks; (d) the distortion map of the robust watermark; (e) the distortion map of the high-capacity watermark; (f) the distortion map of the fragile watermark



models. Their corresponding authentication results are shown in Figure 8.(e)-(h). The proposed fragile watermark is experimentally invariant to similarity transformation (Figure 8.(e)). According to the watermark extraction results, we can successfully locate the noised part (Figure 8.(f)) and the deformed part (Figure 8.(g)) on the modified models. We can also detect a global geometric modification, such as a smoothing in Figure 8.(h).

Summary and Comparisons

In the proposed hierarchical watermarking framework, three different watermarks (robust,

high-capacity, and fragile) can co-exist in a same semi-regular mesh without interference. To the best of our knowledge, this framework constitutes the first attempt on multiple watermarking of 3-D meshes in the literature. In the following, we will summarize the features of the proposed watermarking schemes and also conduct some brief comparisons between our schemes and several state-of-the-art methods.

During the design of the robust watermark, the causality problem and the synchronization problem are carefully taken into account. Compared with the existing blind and robust mesh watermarking methods, the main advantage of the

Figure 7. Some watermarked and attacked Venus models: (a) by a 0.20% random additive noise, the corresponding BER of the extracted robust watermark is 0.11; (b) by a 30-iteration Laplacian smoothing with deformation factor equal to 0.10, the BER is 0.11; (c) by a 9-bit vertex coordinate quantization, the BER is 0.17

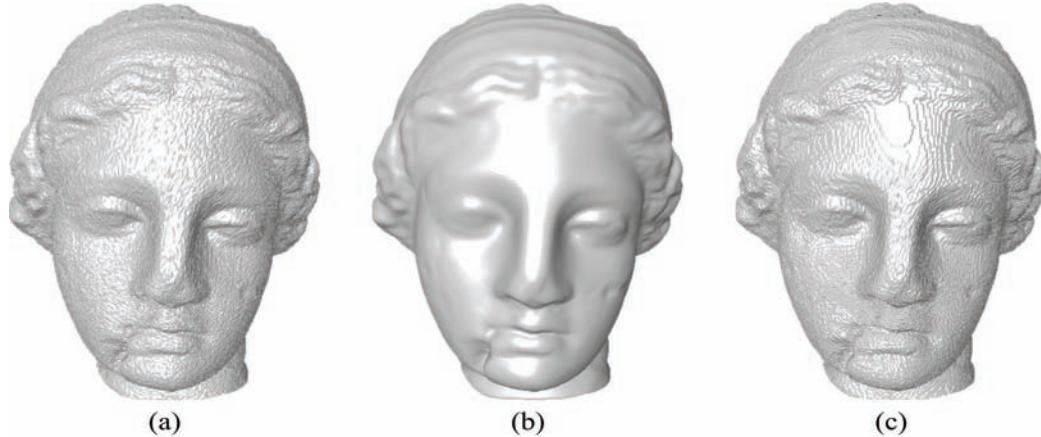
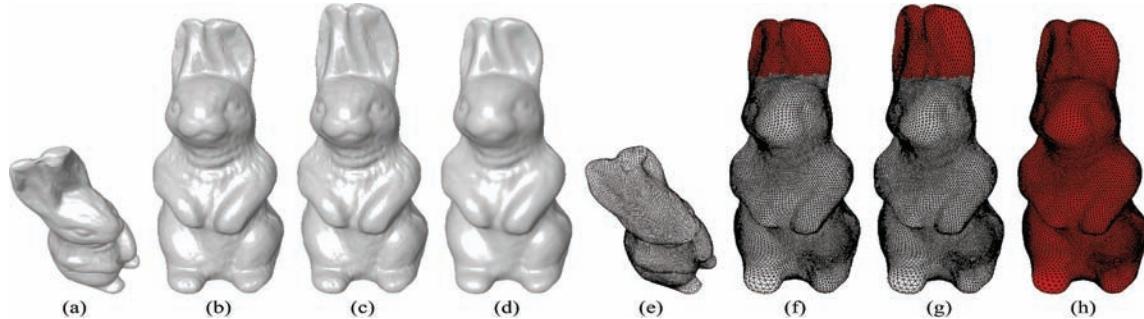


Figure 8. Some attacked Rabbit models for the fragile watermark test: (a) by a similarity transformation; (b) by a 0.0005% binary invisible noise on the ears; (c) by a local deformation where the ears have been pulled up; and (d) by a 30-iteration Laplacian smoothing with deformation factor equal to 0.10. The corresponding authentication results are shown in (e)-(h), where the valid parts are rendered in white, while the invalid parts are rendered in red.



proposed scheme is that it can introduce relatively high-amplitude objective modifications while keeping them perceptually invisible, since these modifications are rather of low frequencies. It is well known that for 3-D mesh watermarking, the lower frequency component modifications are both more imperceptible and more robust (Sorkine, Cohen-Or, & Toledo, 2003; Zhang, van Kaick, & Dyer, 2007). In general, the robustness of our scheme outperforms the early non-blind

wavelet-based algorithm of Kanai, Date, & Kishinami (1998). It is difficult to compare our multi-bit watermarking scheme with the one-bit watermarking scheme of Uccheddu et al. (2004) which is also based on the wavelet analysis of semi-regular meshes; nonetheless, the critical attack amplitude (e.g. for which the BER is equal to 0.20) in our algorithm seems comparable with the maximum tolerable attack amplitude in their method. In general, the proposed geometrically

robust watermark will be destructed under connectivity attacks, which yet can be omitted in semi-regular mesh watermarking (as pointed out at the beginning of the section titled “The Robust Watermark”). If we want also the robustness against connectivity attacks, one possible solution is to devise a robust remeshing technique that is insensitive to connectivity changes. Before watermark extraction, the attacked mesh is first remeshed to reconstruct a semi-regular mesh with the same connectivity configuration as the one in which the watermark is initially embedded. Such a remeshing technique could possibly rely on a blind and robust feature point detection algorithm but its development seems quite difficult. Rondao-Alface & Macq (2005) have conducted some related work on this research problem.

By using the proposed high-capacity watermarking scheme, we can easily embed a large amount of auxiliary information in the cover semi-regular mesh. The embedded watermark achieves the invariance to both element ordering and similarity transformation. This scheme is somewhat fragile to the other geometry attacks which obviously modify the shape of the watermarked model. Technically, our high-capacity watermark combines the ideas of both geometry-based and order-based methods. Indeed, the watermark is embedded in a geometric primitive by applying the basic idea of the permutation-based steganography (Art, 2001). It has been demonstrated in Wang et al. (2008b) that the capacity limit of the proposed scheme is approximately equal to $3\lfloor N_0 / G \rfloor \cdot \lfloor \log_2(G!) \rfloor$ bits, where N_0 is the vertex number of the original semi-regular mesh. This capacity is much higher than those of the existing geometry-based high-capacity methods (e.g. Cayre & Macq, 2003; Wang & Cheng 2005; Cheng & Wang 2007). The advantage of our scheme over the existing order-based methods (e.g. Cheng & Wang, 2006; Bogomjakov et al., 2008) is its invariance to vertex/facet reordering.

As far as we know, the proposed fragile watermarking scheme is the first on this topic that

is robust against all the content-preserving operations while being capable of precisely locating the other attacks considered harmful to the integrity of the watermarked mesh. We have carefully selected two similarity-transformation-invariant quantities as the watermarking primitives. These two quantities are independent from each other and are both local geometric properties of the cover mesh; therefore, we can avoid the causality problem during the watermark embedding and also attain a high precision of the attack localization. The integrity of the raw authentication primitives (i.e. the edges in the less dense semi-regular mesh obtained after one wavelet decomposition) relies on the equality relationship of the watermark symbols embedded in its two associated watermarking primitives. Compared with the fragile scheme of Cho et al. (2005), our method does not suffer from the causality problem and also possesses a higher attack localization precision.

The main limitation of our wavelet-based hierarchical watermarking system is that it can only be applied on meshes with a semi-regular connectivity, because regular wavelet transform can only be performed on this particular kind of meshes. In the future, we would like to investigate the possibility of constructing such a multiple watermarking framework for arbitrary meshes.

FUTURE WORKING DIRECTIONS AND CONCLUSION

In this chapter, we first provided an overview of the research on blind mesh watermarking. Then, we presented our recent work on hierarchical blind watermarking of semi-regular meshes. Examples have been given on how to design, implement and test blind robust, high-capacity and fragile mesh watermarking schemes. In the future, we would like to conduct studies on the following open problems existing in the field of 3-D mesh watermarking research.

- **Robust mesh watermarking based on 3-D shape descriptors.** It can be seen that 3-D shape descriptors may be effective mesh watermarking primitives. Indeed, the histograms used in the methods of Zafeiriou et al. (2005) and Cho et al. (2007) are two statistical shape descriptors. It seems interesting to explore the possibility of using other 3-D shape descriptors for robust and blind mesh watermarking. Such descriptors are supposed to capture the essential properties of the 3-D surface represented by the mesh model. Therefore, the methods using these descriptors as the watermarking primitives may be robust against all kinds of attacks as long as they do not seriously modify the shape of the watermarked mesh.
- **Robustness against cropping combined with connectivity changes.** This operation has been considered as the most intractable attack to a robust and blind mesh watermark. It seems that there exist two possible solutions: the first is to introduce a robust and “blind” mesh segmentation preprocessing that is capable of resisting this attack, and then repetitively embed the watermark in each segmented mesh patch; the second is to use a robust local shape descriptor as the watermarking primitive, which can still be accurately retrieved under cropping combined with connectivity alteration. When performing research on these two solutions, the mesh watermarking community may benefit from the recent achievements in the field of 3-D shape analysis and indexing, such as the work of Shapira, Shamir, & Cohen-Or (2008) and that of Liu, Zhang, Shamir, & Cohen-Or (2009).
- **Adaptive watermarking.** The performance of a mesh watermarking method can be improved if it takes the mesh local properties into account. For example, in the areas with low vertex sampling density or with high roughness, we can enhance the embedding strength of a robust scheme or increase the number of embedded bits for a high-capacity scheme.
- **Mesh watermarking benchmark.** It is necessary to build a benchmarking system so as to facilitate the evaluation and comparison of different mesh watermarking algorithms (especially the robust schemes). Such a benchmarking system may contain a standard data set of mesh models, the standard implementation of a variety of attacks, some metrics to measure the objective and perceptual distortions induced by the watermark embedding, and finally an evaluation protocol that indicates the main steps to follow while performing the benchmarking experiments.
- **High-capacity watermark with invariance to all content-preserving operations.** In many applications, we require that a high-capacity mesh watermark should be invariant to both element reordering and similarity transformation while providing a very high payload. In order to achieve this target, the high-capacity scheme presented in the last section applies the basic idea of permutation steganography when embedding a watermark in the mesh geometry. It would be interesting to investigate whether it is possible to devise a similar scheme for arbitrary meshes.
- **Fully functional fragile watermark for arbitrary meshes.** Although in this chapter we devised an effective fragile watermarking method for semi-regular meshes, it seems much more difficult to design such a scheme for arbitrary meshes. The main difficulty is how to achieve the following properties at the same time: immunity to causality problem, invariance to element reordering and similarity transformation, a high-level security and the numerical stability.

- **Deformation-invariant watermarking.** A 3-D mesh may be subject to some realistic (and high-amplitude) deformations to form a sequence of moving objects. For instance, we can make the Bunny model run, or make the Venus model have different facial expressions. Ideally, a robust watermark should be able to resist such realistic deformations of the stego model. In order to build a deformation-invariant blind mesh watermark, one possible solution would be looking for an invariant 3-D shape descriptor and using it as the watermarking primitive. Once again, we may benefit from the achievements in the shape analysis research, especially from the studies on deformation-invariant shape representation (Elad & Kimmel, 2003; Jain & Zhang, 2007; Rustamov, 2007).

In all, blind mesh watermarking is a challenging and interesting research area, with many open problems and potential applications. As observed from the above discussion, the study in this area seems highly related to the advances in geometry processing and shape analysis. Therefore, in order to promote the research on blind mesh watermarking, watermarking researchers should probably work more closely with geometry processing and shape analysis experts.

ACKNOWLEDGMENT

This work is in part supported by China Scholarship Council of the Chinese government and by French National Research Agency (ANR) through COSINUS program (project COLLAVID n°ANR-08-COSI-003). The authors would like to thank Dr. C. Wolf for proofreading one part of the chapter. We are also very grateful to Dr. C. Roudet for her help on the wavelet transform of semi-regular meshes. The Mannequin model was downloaded from the AIM@SHAPE Shape

Repository. The Bunny model is a courtesy of the Stanford Computer Graphics Laboratory. The Rabbit and Venus models are the properties of the Cyberware Incorporation.

REFERENCES

- Abdallah, E. E., Ben Hamza, A., & Bhattacharya, P. (2007). *Spectral graph-theoretic approach to 3D mesh watermarking* (pp. 327–334). Proc. of the Graphics Interface.
- Artz, D. (2001). Digital steganography: Hiding data within data. *IEEE Internet Computing*, 5(3), 75–80. doi:10.1109/4236.935180
- Benedens, O. (1999). Geometry-based watermarking of 3D models. *IEEE Computer Graphics and Applications*, 19(1), 46–55. doi:10.1109/38.736468
- Biggs, N. (1993). *Algebraic Graph Theory* (2nd ed.). Cambridge, UK: Cambridge University Press.
- Bogomjakov, A., Gotsman, C., & Isenburg, M. (2008). Distortion-free steganography for polygonal meshes. *Computer Graphics Forum*, 27(2), 637–642. doi:10.1111/j.1467-8659.2008.01161.x
- Botsch, M., Pauly, M., Kobelt, L., Alliez, P., Lévy, B., Bischoff, S., & Rössl, C. (2007). Geometric modeling based on polygonal meshes. In *Proc. of the ACM Siggraph Course Notes*.
- Cayre, F., & Macq, B. (2003). Data hiding on 3-D triangle meshes. *IEEE Transactions on Signal Processing*, 51(4), 939–949. doi:10.1109/TSP.2003.809380
- Cayre, F., Rondao-Alface, P., Schmitt, F., Macq, B., & Maître, H. (2003). Application of spectral decomposition to compression and watermarking of 3D triangle mesh geometry. *Signal Processing Image Communication*, 18(4), 309–319. doi:10.1016/S0923-5965(02)00147-9

- Cheng, Y.-M., & Wang, C.-M. (2006). A high-capacity steganographic approach for 3D polygonal meshes. *The Visual Computer*, 22(9-11), 845–855. doi:10.1007/s00371-006-0069-4
- Cheng, Y.-M., & Wang, C.-M. (2007). An adaptive steganographic algorithm for 3D polygonal meshes. *The Visual Computer*, 23(9), 721–732. doi:10.1007/s00371-007-0147-2
- Cho, J.-W., Prost, R., & Jung, H.-Y. (2007). An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms. *IEEE Transactions on Signal Processing*, 55(1), 142–155. doi:10.1109/TSP.2006.882111
- Cho, W.-H., Lee, M.-E., Lim, H., & Park, S.-Y. (2005). Watermarking technique for authentication of 3-D polygonal meshes. In *Proc. of the International Workshop on Digital Watermarking* (pp. 259–270).
- Chou, C. M., & Tseng, D. C. (2006). A public fragile watermarking scheme for 3D model authentication. *Computer Aided Design*, 38(11), 1154–1165. doi:10.1016/j.cad.2006.06.009
- Cignoni, P., Rocchini, C., & Scopigno, R. (1998). Metro: Measuring error on simplified surfaces. *Computer Graphics Forum*, 17(2), 167–174. doi:10.1111/1467-8659.00236
- Costa, M. (1983). Writing on dirty paper. *IEEE Transactions on Information Theory*, 29(3), 439–441. doi:10.1109/TIT.1983.1056659
- Dodgson, N. A., Floater, M. S., & Sabin, M. A. (Eds.). (2004). *Advances in Multiresolution for Geometric Modelling*. Berlin: Springer-Verlag.
- Eggers, J. J., Bauml, R., Tzschoppe, R., & Girod, B. (2003). Scalar costa scheme for information embedding. *IEEE Transactions on Signal Processing*, 51(4), 1003–1019. doi:10.1109/TSP.2003.809366
- Elad, A., & Kimmel, R. (2003). On bending invariant signatures for surfaces. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(10), 1285–1295. doi:10.1109/TPAMI.2003.1233902
- Jain, V., & Zhang, H. (2007). A spectral approach to shape-based retrieval of articulated 3D models. *Computer Aided Design*, 39(5), 398–407. doi:10.1016/j.cad.2007.02.009
- Kanai, S., Date, H., & Kishinami, T. (1998). Digital watermarking for 3D polygons using multiresolution wavelet decomposition. In *Proc. of the International Workshop on Geometric Modeling: Fundamentals and Applications*, (pp. 296–307).
- Karni, Z., & Gotsman, C. (2000). Spectral compression of mesh geometry. In *Proc. of the ACM Siggraph* (pp. 279–286).
- Kutter, M., & Petitcolas, F. A. P. (1999). A fair benchmark for image watermarking systems. In *Proc. of the SPIE Electronic Imaging*, (vol. 3657, pp. 226–239).
- Lavoué, G., Denis, F., & Dupont, F. (2007). Subdivision surface watermarking. *Computers & Graphics*, 31(3), 480–492. doi:10.1016/j.cag.2007.01.022
- Lee, S.-H., & Kwon, K.-R. (2007). A watermarking for 3D mesh using the patch CEGIs. *Digital Signal Processing*, 17(2), 396–413. doi:10.1016/j.dsp.2005.04.014
- Lin, H. S., Liao, H. M., Lu, C., & Lin, J. (2005). Fragile watermarking for authenticating 3-D polygonal meshes. *IEEE Transactions on Multimedia*, 7(6), 997–1006. doi:10.1109/TMM.2005.858412
- Liu, R., Zhang, H., Shamir, A., & Cohen-Or, D. (2009). A part-aware surface metric for shape analysis. *Computer Graphics Forum*, 28(2), 397–406. doi:10.1111/j.1467-8659.2009.01379.x

- Liu, Y., Prabhakaran, B., & Guo, X. (2008). A robust spectral approach for blind watermarking of manifold surfaces. In *Proc. of the ACM Workshop on Multimedia and Security*, (pp. 43-52).
- Lounsbery, M., DeRose, T. D., & Warren, J. (1997). Multiresolution analysis for surfaces of arbitrary topological type. *ACM Transactions on Graphics*, 16(1), 34–73. doi:10.1145/237748.237750
- Luo, M., & Bors, A. G. (2008). Principal component analysis of spectral coefficients for mesh watermarking. In *Proc. of the IEEE International Conference on Image Processing* (pp. 441-444).
- Luo, M., Wang, K., Bors, A. G., & Lavoué, G. (2009). Local patch blind spectral watermarking method for 3D graphics. In *Proc. of the International Workshop on Digital Watermarking*, (pp. 211-226).
- Ohbuchi, R., Masuda, H., & Aono, M. (1997). Watermarking three-dimensional polygonal models. In *Proc. of the ACM Multimedia* (pp. 261-272).
- Ohbuchi, R., Mukaiyama, A., & Takahashi, S. (2002). A frequency-domain approach to watermarking 3D shapes. *Computer Graphics Forum*, 21(3), 373–382. doi:10.1111/1467-8659.t01-1-00597
- Rondao-Alface, P., & Macq, B. (2005). Blind watermarking of 3D meshes using robust feature points detection. In *Proc. of the IEEE International Conference on Image Processing*, (vol. 1, pp. 693–696).
- Rondao-Alface, P., & Macq, B. (2007). From 3D mesh data hiding to 3D shape blind and robust watermarking: A survey. *LNCS Transactions on Data Hiding and Multimedia Security*, 2, 99–115.
- Rustamov, R. M. (2007). Laplace-Beltrami eigenfunctions for deformation invariant shape representation. In *Proc. of the Symposium on Geometry processing* (pp. 225-233).
- Shapira, L., Shamir, A., & Cohen-Or, D. (2008). Consistent mesh partitioning and skeletonization using the shape diameter function. *The Visual Computer*, 24(4), 249–259. doi:10.1007/s00371-007-0197-5
- Sorkine, O., Cohen-Or, D., & Toledo, S. (2003). High-pass quantization for mesh encoding. In *Proc. of the Symposium on Geometry Processing* (pp. 42-51).
- Uccheddu, F., Corsini, M., & Barni, M. (2004). Wavelet-based blind watermarking of 3D models. In *Proc. of the ACM Workshop on Multimedia and Security* (pp. 143-154).
- Vallet, B., & Lévy, B. (2007). *Manifold harmonics*. Technical Report of INRIA-ALICE Project Team.
- Vallet, B., & Lévy, B. (2008). Spectral geometry processing with manifold harmonics. *Computer Graphics Forum*, 27(2), 251–260. doi:10.1111/j.1467-8659.2008.01122.x
- Wang, C.-M., & Cheng, Y.-M. (2005). An efficient information hiding algorithm for polygon models. *Computer Graphics Forum*, 24(3), 591–600. doi:10.1111/j.1467-8659.2005.00884.x
- Wang, K., Lavoué, G., Denis, F., & Baskurt, A. (2008a). A comprehensive survey on three-dimensional mesh watermarking. *IEEE Transactions on Multimedia*, 10(8), 1513–1527. doi:10.1109/TMM.2008.2007350
- Wang, K., Lavoué, G., Denis, F., & Baskurt, A. (2008b). Hierarchical watermarking of semi-regular meshes based on wavelet transform. *IEEE Transactions on Information Forensics and Security*, 3(4), 620–634. doi:10.1109/TIFS.2008.2007229
- Wang, K., Luo, M., Bors, A. G., & Denis, F. (2009). Blind and robust mesh watermarking using manifold harmonics. In *Proc. of the IEEE International Conference on Image Processing*.

Wang, W.-B., Zheng, G.-Q., Yong, J.-H., & Gu, H.-J. (2008). A numerically stable fragile watermarking scheme for authenticating 3D models. *Computer Aided Design*, 40(5), 634–645. doi:10.1016/j.cad.2008.03.001

Wu, H.-T., & Cheung, Y.-M. (2006). A high-capacity data hiding method for polygonal meshes. In *Proc. of the International Workshop on Information Hiding* (pp. 188-200).

Yeo, B., & Yeung, M. M. (1999). Watermarking 3D objects for verification. *IEEE Computer Graphics and Applications*, 19(1), 36–45. doi:10.1109/38.736467

Zafeiriou, S., Tefas, A., & Pitas, I. (2005). Blind robust watermarking schemes for copyright protection of 3D mesh objects. *IEEE Transactions on Visualization and Computer Graphics*, 11(5), 596–607. doi:10.1109/TVCG.2005.71

Zhang, H., van Kaick, O., & Dyer, R. (2007). Spectral Methods for Mesh Processing and Analysis. In *Proc. of the Eurographics State-of-the-art Report* (pp. 1-22).

KEY TERMS AND DEFINITIONS

3-D Mesh: A 3-D model is often numerically represented as a 3-D mesh, which is a collection of polygonal facets targeting to constitute an appropriate piecewise linear approximation of the surface of the real 3-D object. A mesh has three different combinatorial elements: vertices, edges and facets.

Similarity Transformation: Similarity transformation of a 3-D mesh includes translation, rotation, uniform scaling and combination of the above three operations. This transformation modifies the spatial position of the mesh but always keeps the mesh shape unchanged.

Content-Preserving Operation: A content-preserving operation does not modify the shape of the mesh on which the operation is performed. Content preserving operation mainly contains the vertex/facet reordering in the mesh file and the similarity transformation.

Geometry Attack: In a geometry attack on the watermarked mesh, only the coordinates of the mesh vertices are modified. Typical geometry attacks include noise addition, smoothing and vertex coordinate quantization.

Connectivity Attack: In a connectivity attack on the watermarked mesh, the adjacency relationships between the mesh vertices (i.e. the edges and facets) are also modified. Examples of connectivity attacks are surface simplification, subdivision, remeshing and cropping.

Semi-Regular Mesh: A mesh is regular if all its vertices have a same valence, i.e. a same number of direct neighbors. A semi-regular mesh is a piecewise regular structure and consists of a patchwork of large regular regions; hence, it owns regular vertices almost everywhere.

Wavelet Transform: Wavelet transform is an efficient multiresolution analysis tool of semi-regular meshes. While being iteratively applied on a dense semi-regular mesh, the wavelet transform can finally produce a coarse irregular mesh that represents the basic shape of the model and a set of details information (i.e. the wavelet coefficients) at different resolution levels.

Multiple Watermarking: In a multiple watermarking system, several different watermarks are embedded in a same multimedia content. For instance, these watermarks can be of different types (robust, fragile and high-capacity) which serve for different applications (intellectual property protection, content authentication and content enhancement).

Section 3

Multimedia Watermarking

Chapter 10

A Unified Approach Towards Multimedia Watermarking

Ali Al-Haj

Princess Sumaya University for Technology, Jordan

Ahmad Mohammad

Princess Sumaya University for Technology, Jordan

Samir Abou El-Seoud

Princess Sumaya University for Technology, Jordan

Tuqa Manasrah

The University of Jordan, Jordan

Lama Rajab

The University of Jordan, Jordan

Tahani Al-Khatib

The University of Jordan, Jordan

ABSTRACT

The tremendous advancement of digital technology has increased the ease with which digital multimedia signals (image, video, audio) are stored, transmitted, and reproduced. Consequently, the content providers and owners are faced with problems of protection against copyright violation and other forms of abuse to their digital property. Digital watermarking has been proposed in the last decade as a solution to prevent illegal and malicious copying and distribution of digital media by embedding an unnoticeable information into the media content. This chapter describes three imperceptible and robust watermarking algorithms for different types of multimedia objects (image, video, audio). The three algorithms are based on cascading two powerful mathematical transforms; the Discrete Wavelet Transform (DWT), and the Singular Value Decomposition (SVD). The two transforms are different, and thus provide complementary levels of robustness against the same attack. In the proposed dual-transform algorithms, the watermark bits are not embedded directly on the wavelet coefficients, but rather on the elements of singular values of the DWT sub-bands of the multimedia object. Effectiveness of the proposed algorithms is demonstrated through extensive experimentation.

DOI: 10.4018/978-1-61520-903-3.ch010

INTRODUCTION

Digital watermarking has been proposed in the last decade as a solution to prevent illegal and malicious copying and distribution of digital media by embedding an unnoticeable information (called a watermark) into the media content. The watermark is usually a random number sequence, copyright messages, ownership identifier, or control signal identifying the ownership information of the media object (Bender et al., 1996; Cox, 2001; Katzenbeisser & Petitcolas, 2000; Langelaar et al., 2000). Effective watermarking has many requirements, the most important of which are imperceptibility (perceptual transparency) and robustness. Imperceptibility requires the watermarking algorithm to embed the watermark information in the digital media in such a way that the quality of the underlying media is not affected. As for the robustness requirement, the watermark must always remain in the watermarked host media, even if the quality of the media is degraded intentionally or unintentionally (Voloshynovskiy et al., 2001).

Current digital multimedia watermarking techniques can be grouped into two major classes; spatial-domain watermarking techniques and frequency-domain watermarking techniques (Arnold, 2003). Spatial-domain techniques embed watermarks directly in the host digital media object, however, these techniques are not robust against common digital signal processing operations (Chan & Cheng, 2004). On the other hand, transform-domain watermarking techniques embed watermarks by modifying the coefficients of the transformed media object according to a predetermined embedding scheme. The scheme disperses the watermark in the spatial domain of the host media, hence making it very difficult to remove the embedded watermark (Chu, 2003).

In this chapter, we propose three imperceptible and robust watermarking techniques for different types of multimedia objects (image, video, audio). Proposed techniques are based on cascading two

powerful mathematical transforms; the Discrete Wavelet Transform (DWT), and the Singular Value Decomposition (SVD) (Mitra, 1998). The two transforms are different transform domain techniques and thus provide different, but complementary, levels of robustness against the same attack. More robustness is expected by combining benefits of the two transforms. In the proposed dual-transform algorithms, the watermark bits are not embedded directly on the wavelet coefficients, but rather on the elements of singular values of the DWT sub-bands of the media object. In the next section, DWT and SVD are described and their relevance to digital watermarking is outlined. In subsequent sections, three DWT-SVD hybrid watermarking algorithms are described for image, video and audio watermarking, respectively. The conclusion is outlined in the last section.

THE DWT AND SVD TRANSFORMS

The Discrete Wavelet Transform (DWT), and the Singular Value Decomposition (SVD), are different transforms, and thus provide different levels of performance for different applications. We argue that better multimedia watermarking performance could be obtained by combining benefits of the two transforms. In this section, we briefly describe the two transforms and outline their relevance to multimedia watermarking. Next sections describe our proposed watermarking methods for image, video, and audio based on different formulations of the two transforms.

DWT and its Relevance to Multimedia Watermarking

The discrete wavelets transform (DWT) is a novel discipline capable of giving a *time-frequency* representation of any given signal (Strang & Nguyen, 1996). Wavelets are special functions which, in a form analogous to sines and cosines

Figure 1. One-dimensional DWT decomposition – one level

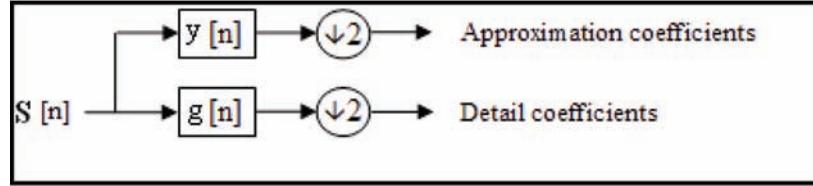
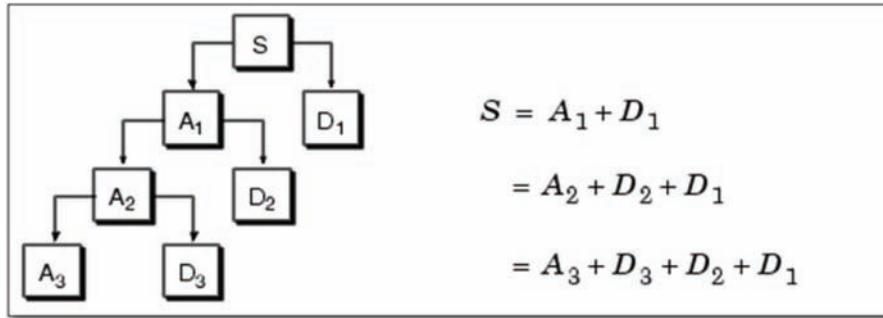


Figure 2. One-dimensional DWT decomposition – three levels



in Fourier analysis, are used as basal functions for representing signals. DWT can be applied to one-dimensional signals such as audio signals, and two-dimensional signals such as images and video frames. A brief description of one-dimensional and two-dimensional DWT is given below.

One-Dimensional DWT

Audio signals are one-dimensional signals. Starting from the original audio signal S , shown in Figure 1, DWT produces two sets of coefficients (Mallat, 1989). The approximation coefficients A (low frequencies) are produced by passing the signal S through a low pass filter y , and the detail coefficients D (high frequencies) are produced by passing the signal S through a low pass filter g . Depending on the application and the length of the signal, the low frequencies part might be further decomposed into two parts of high and low frequencies. Figure 2 shows a three-level DWT decomposition of signal S . The original

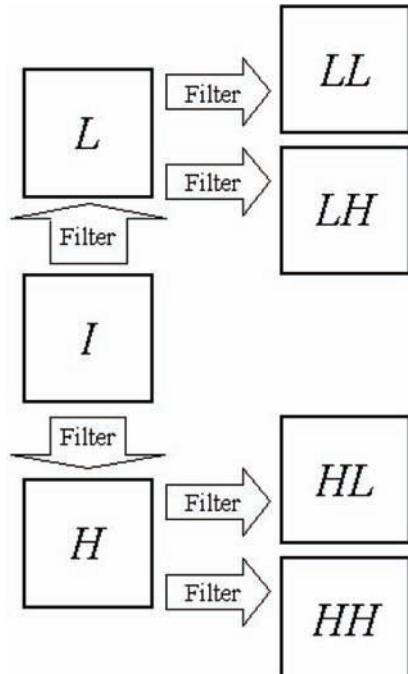
signal S can be reconstructed using the inverse DWT process.

Due to its excellent spatio-frequency localization properties, DWT is very suitable to identify areas in an audio signal where a watermark can be embedded effectively (Hsieh, Tseng & Huang, 2001). Many DWT-based audio watermarking techniques can be found in literature (Swanson et al., 1998; Wu & Shimamoto, 2006; Erelibi & Bataki, 2009; Wei & Xue, 2003; Li & Yu, 2000; Wang & Zhao, 2006).

Two-Dimensional DWT

For two-dimensional images and video frames, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL , LH , HL , and HH , as shown in Figure 3. The LL sub-band represents the coarse-scale DWT coefficients while the LH , HL , and HH sub-bands represent the fine-scale

Figure 3. Two-dimensional DWT decomposition – one level



DWT coefficients. To obtain the next coarser scale of wavelet coefficients, the LL sub-band is further processed until some final scale N is reached. When N is reached, we will have $3N + 1$ sub-bands consisting of the multi-resolution sub-bands LL_N and LH_x , HL_x and HH_x where x ranges from 1 until N .

Due to its excellent spatio-frequency localization properties, the DWT allows the exploitation of the masking effect of the human visual system such that if a DWT coefficient is modified, only the region corresponding to that coefficient will be modified. In general, most of the image energy is concentrated at the lower frequency sub-bands LL_x , and therefore embedding watermarks in these sub-bands may degrade the image significantly. Embedding in the low frequency sub-bands, however, could increase robustness significantly. On the other hand, the high frequency sub-bands HH_x include the edges and textures of the image,

for which the human eye is not generally sensitive to changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye. The compromise adopted by many DWT-based watermarking algorithm, is to embed the watermark in the middle frequency sub-bands LH_x and HL_x where acceptable performance of imperceptibility and robustness could be achieved. Many DWT-based image and video watermarking techniques can be found in literature (Wang et al., 2002; Reddy & Chatterji, 2005; Tay & Havlicek, 2002; Huang & Yang, 2004; Guzman et al., 2004; Jung et al., 2003; Guo & Georganas, 2002; Safabakhsh et al., 2004; Niu et al., 2000; Hsu and Wu, 1998).

SVD and its Relevance to Multimedia Watermarking

The traditional frequency transforms; FFT, DCT and DWT transforms attempt to decompose signals in terms of a standard basis set (Mitra, 1998). This needs not necessarily be the optimal representation for a given signal. On the other hand, the singular value decomposition (SVD) is a numerical technique for diagonalizing matrices in which the transformed domain consists of basis states that is optimal in some sense (Andrews & Patterson, 1976). The SVD of an $N \times N$ matrix A is defined by the operation $A = USV^T$ as shown in Figure 4.

The diagonal entries of S are called the singular values of A and are assumed to be arranged in decreasing order $\sigma_i > \sigma_{i+1}$. The columns of the U matrix are called the left singular vectors while the columns of the V matrix are called the right singular vectors of A . By virtue of the fact that slight variations in the elements of matrix S does not affect visual perception of the quality of the cover object, SVD-based watermarking algorithms add the watermark information to the singular values of the diagonal matrix S in such a way to meet the imperceptibility (inaudibility)

Figure 4. The three matrices produced by the SVD operation

$$\begin{bmatrix} \mathbf{u}_{1,1}, \dots, \mathbf{u}_{1,n} \\ \mathbf{u}_{2,1}, \dots, \mathbf{u}_{2,n} \\ \vdots \\ \mathbf{u}_{n,1}, \dots, \mathbf{u}_{n,n} \end{bmatrix} \begin{bmatrix} \sigma_{1,1}, 0, \dots, 0 \\ 0, \sigma_{2,2}, \dots, 0 \\ \vdots \\ 0, 0, \dots, \sigma_{n,n} \end{bmatrix} \begin{bmatrix} \mathbf{v}_{1,1}, \dots, \mathbf{v}_{1,n} \\ \mathbf{v}_{2,1}, \dots, \mathbf{v}_{2,n} \\ \vdots \\ \mathbf{v}_{n,1}, \dots, \mathbf{v}_{n,n} \end{bmatrix}^T$$

and robustness requirements of effective digital watermarking algorithms.

The SVD transform has been used extensively in image watermarking (Basso et al., 2009; Chang, Tsai & Lin, 2005; Mohammad, Al-Haj & Shaltaf, 2008; Liu & Tan, 2002), however, SVD-based audio watermarking techniques are quite a few, and some of which can be found in (Ozer, Sankur & Memon, 2005; Bao & Ma, 2004). In our proposed algorithms, which will be described in the next three sections, the watermark bits are not embedded directly on the wavelet coefficients, but rather on the elements of singular values of the DWT sub-bands.

IMAGE WATERMARKING

The ease of the production and distribution of digital images has lead to a matched ease in the illegal and unauthorized manipulation of digital images. Such illegal manipulation has lead the industry to look for approaches to implement copyright protection in digital images. A promising solution has been image watermarking technology where copyright information is embedded in digital images robustly and imperceptibly. Many digital image watermarking algorithms have been proposed in the literature (Chang, Tsai, & Lin, 2005; Ganic & Eskicioglu, 2004; Huang, & Yang, 2004; Jung, et al., 2003; Niu, Lu, & Sun, 2000; Poddar, Han, & Chang, 2005; Reddy & Chatterji, 2005; Safabakhsh, et al., 2000; Wang, Doherty,

& Van Dyke, 2002; Qiao & Nahrstedt, 1998; Ramkumar & Akansu, 2004; Ejima & Myazaki, 2001; Hsu & Wu, 1998; Liu & Tan, 2002; Guo & Georganas, 2002; Mohammad, Al-Haj, & Shaltaf, 2008). In this section, we propose an imperceptible and robust image watermarking technique based on cascading two powerful mathematical transforms; the Discrete Wavelet Transform (DWT), and the Singular Value Decomposition (SVD). In the algorithm, the watermark bits are not embedded directly on the wavelet coefficients, but rather on the elements of singular values of the matrix \mathbf{S} of the original image's DWT sub-bands. The proposed algorithm consists of a watermark embedding procedure, and a watermark extraction procedure. Descriptions of both procedures are given below.

Watermark Embedding Procedure

The watermark embedding procedure is shown in Figure 5, and explained in the steps that follow.

1. Compute the 3-level DWT for the host image \mathbf{I} . This will generate 10 sub-bands as follows:

$$DWT(\mathbf{I}) = [\mathbf{LL}_3, \mathbf{LH}_3, \mathbf{HL}_3, \mathbf{HH}_3, \mathbf{LH}_2, \mathbf{HL}_2, \mathbf{HH}_2, \mathbf{LH}_1, \mathbf{HL}_1, \mathbf{HH}_1] \quad (1)$$

Each sub-band is a matrix of DWT coefficients at a specific resolution. Figure 6 shows

Figure 5. Image watermarking - the DWT-SVD based watermark-embedding procedure

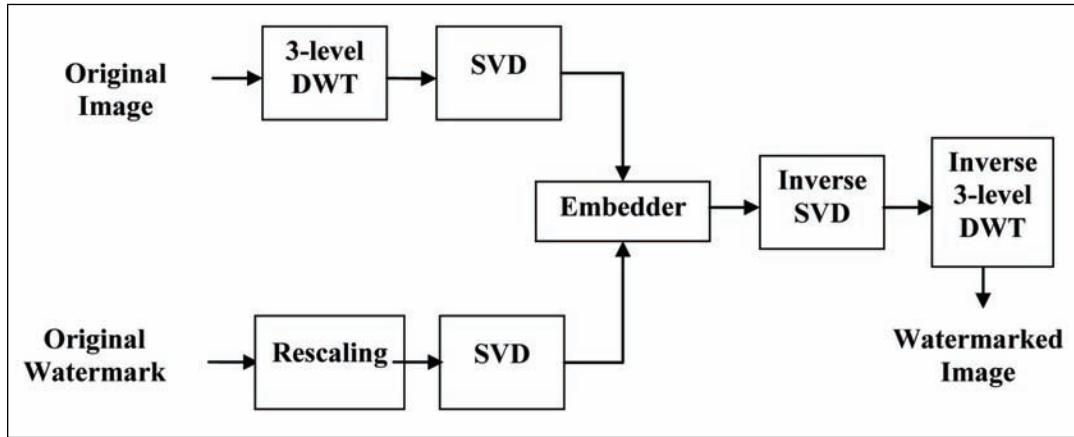
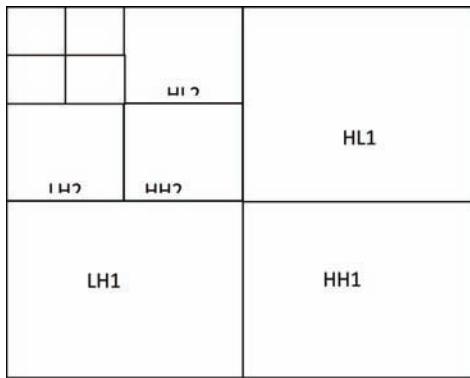


Figure 6. Two-dimensional DWT decomposition of an image – three levels



the sub-bands produced by the 3-level DWT decomposition.

2. Compute SVD for each of the 10 sub-band's coefficient matrices. The SVD operator decomposes a given sub-band matrix into three independent matrices. If X_i represents coefficient matrix of sub-band X at level i , then SVD of X_i is computed as follows:

$$SVD(X_i) = U_{xi} S_{xi} V_{xi}^T \quad (2)$$

3. Compute SVD for the watermark image W and its down-scaled versions. Down-scaling

is necessary so that the size of the watermark will match the size of the sub-band which will embed it. If subscript i denotes the down-scaled watermark at level i (where $i = 1, 2, 3$), then SVD of W_i is computed as follows:

$$SVD(W_i) = U_{wi} S_{wi} V_{wi}^T \quad (3)$$

4. Embed the watermark in every sub-band X_i by modifying its V_{xi} matrix. Watermark embedding is done according to the following formula:

$$V_{xi}' = V_{xi} + \alpha V_{wi} \quad (4)$$

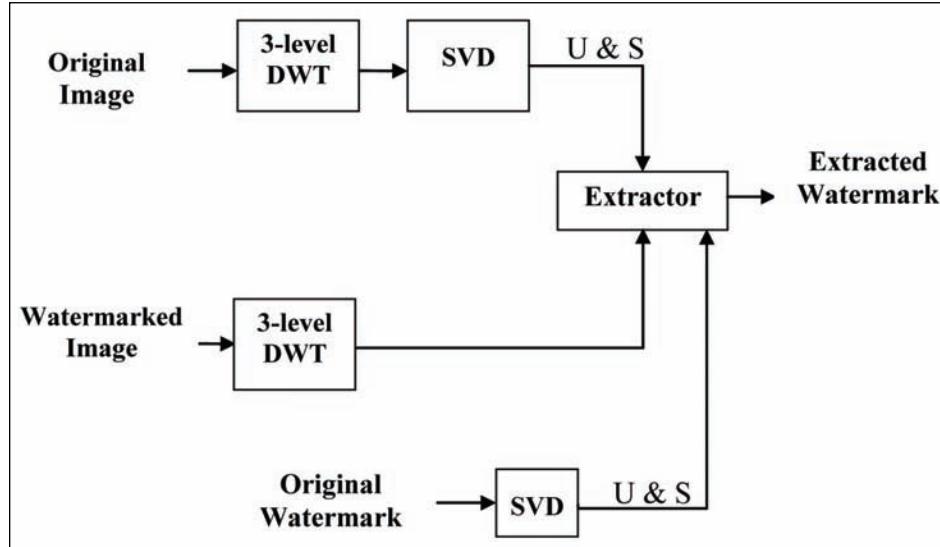
where α is a scaling factor that has a value in the range $1 \geq \alpha \geq 0$.

5. Apply the inverse SVD operation using the new V_{xi}' matrices to get a modified coefficient matrix X_i' for each sub-band i . The inverse SVD operation is given as follows:

$$X_i' = U_{xi} S_{xi} V_{xi}'^T \quad (5)$$

6. Apply the inverse DWT on the modified coefficient matrices X_i' 's. This operation produces the final watermarked image I_w .

Figure 7. Image watermarking - the DWT-SVD based watermark-extraction procedure



Watermark Extraction Procedure

The watermark extraction procedure is shown in Figure 7, and explained in details as follows:

1. The proposed DWT-SVD algorithms is a non-blind watermarking algorithms, and thus it requires the original image I in the extraction process. Therefore, we need to perform 3-level DWT on the host image I , as well as on the watermarked image I_w . Let the 10 DWT sub-bands of the watermarked image I_w be as follows:

$$DWT(I_w) = [mLL, mLH, mHL, mHH, mLH, mHL, mHH, mLH, mHL, mHH] \quad (6)$$

where mX_i refers to the modified sub-band X of level i .

2. The embedded watermark is extracted from each sub-band by a straightforward reversal of the steps described in the watermark embedding procedure. If we denote the extracted watermark from sub-band mX_i as W_{xi} , then

W_{xi} is extracted according to the following extraction formula:

$$W_{xi} = U_{wi} S_{wi} V_{Ewi}^T \quad (7)$$

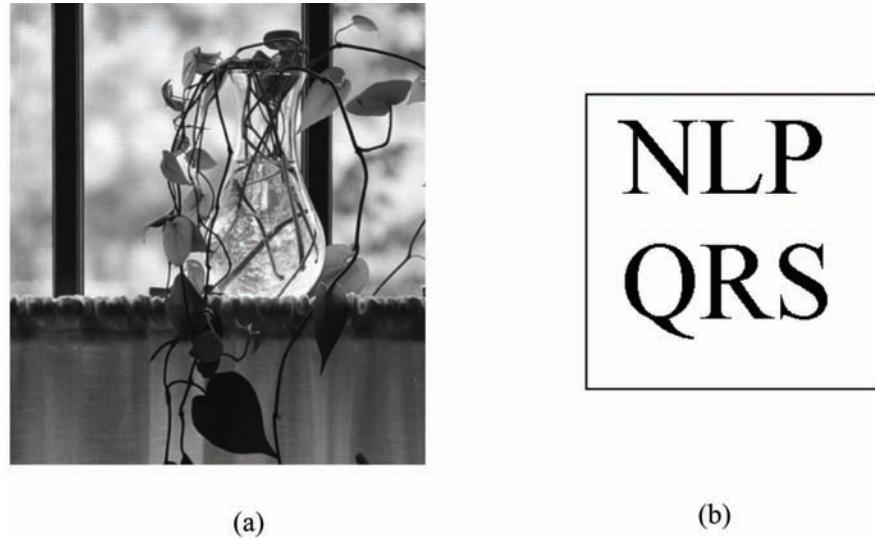
where

$$V_{Ewi}^T = ((U_{xi} S_{xi})^{-1} mX_i - V_{xi}^T) / \alpha \quad (8)$$

Results and Performance Evaluation

We evaluated the performance of our proposed DWT-SVD image watermarking algorithm using a 512 x 512 grayscale ‘Vessel’ image, and a 256 x 256 grayscale ‘NLP QRS’ watermark image, as shown in Figure 8. Two down-scaled versions of the watermark were also used for embedding in the smaller DWT sub-bands. The watermark images were embedded and extracted as described in details in the previous subsections. Effectiveness of the embedding and extraction procedures were measured using three metrics: imperceptibility and robustness (Ejima & Myazaki, 2001). Performance results are reported in this subsection.

Figure 8. (a). The original host image. (b). the original watermark



Imperceptibility. Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark. As a measure of the quality of a watermarked image, the peak signal to noise ratio (PSNR) is typically used. PSNR in decibels (dB) is represented as follows:

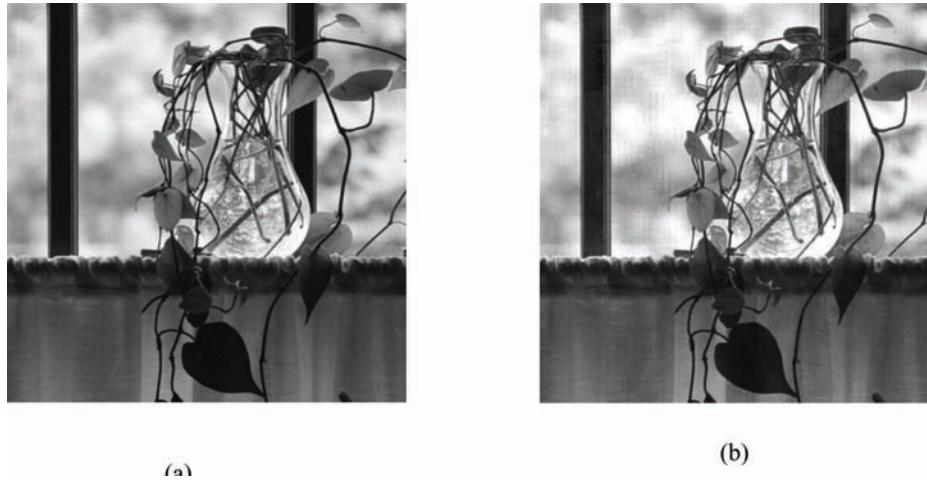
$$PSNR_{dB} = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) = 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \quad (9)$$

where MSE is the mean square error between the original image and the watermarked image, and MAX_I is the maximum pixel value of the image which is equal to 255 in our implementations since pixels were represented using 8 bits per sample. In our work, the watermark was embedded in the host image according the procedure described in details in the previous section. The watermarked image gave a high PSNR value of 79.564, which proves imperceptibility of the proposed SVD-DWT algorithm. This result can be further verified by referring to Figure 9 which shows that the original image and the watermarked image are almost identical.

Robustness. Robustness is a measure of the immunity of the watermark against attempts to remove or degrade it, intentionally or unintentionally, by different types of digital signal processing attacks (Voloshynovskiy et al., 2001). In what follows, we report on robustness results which we obtained for four digital signal processing operations (attacks): image compression, image cropping, low-pass filter, and salt & pepper noise. The low-pass filter and salt & pepper noise are considered watermark-degrading attacks, the JPEG compression is a watermark-removal attack, and image cropping is classified as watermark-dispositioning geometrical attacks. We measured the similarity between the original watermark and the watermark extracted from the attacked watermarked images using the correlation factor ρ which is computed using Equation 10 below:

$$\rho(w, \hat{w}) = \frac{\sum_{i=1}^N w_i \hat{w}_i}{\sqrt{\sum_{i=1}^N w_i^2} \sqrt{\sum_{i=1}^N \hat{w}_i^2}} \quad (10)$$

Figure 9. Imperceptibility performance: (a). original image. (b).watermarked image



where N is the number of pixels in watermark, w and w^* are the original and extracted watermarks respectively. The correlation factor ρ may take values between 0 (random relationship) to 1 (perfect linear relationship). Figures 10 through 13 show the attacked watermarked images and the corresponding extracted watermarks. Values of ρ which measure the correlation between the extracted watermarks and the original watermark are also shown in the figures. A brief description of the attacks is given as follows:

- **Image compression:** the original image is compressed with varying quality factors. As shown in Figure 10, its obvious that the bit rate decreases as the quality factor decreases. JPEG quality 100 is the highest quality.
- **Image cropping:** the original image is cropped by different ratios as shown in Figure 11. Image cropping is a common technique for creating thumbnail images that download quickly.
- **Image filtering:** a slow-pass filter operation is applied to the original image, and results are shown in Figure 12.
- **Image noising:** different types of noise were added to the original image to

measure robustness. Results for the salt & pepper noise are shown below in Figure 13.

VIDEO WATERMARKING

Digital video is becoming popular more than ever due to the widespread of video-based applications such as Internet video, wireless video, videophones, video conferencing, among many others. However, a byproduct of such popularity is the worldwide unauthorized copying and distribution of digital video. To solve this problem, many video watermarking algorithms have been proposed in the literature (Chan & Lyu, 2003; Dorr & Dugelay, 2003; Gao & Tang, 2002; Hartung & Girod, 1998; Kundur, Su, and Hatzinakos, 2004; Langelaar et al., 2000; Nahrstedt & Qiao, 1998). In this section, we extend our hybrid-transform DWT-SVD approach to watermark video files, imperceptibly and robustly. The proposed algorithm is also ‘blind’ in the sense that it does not require the original video in order to extract the embedded watermark.

Figure 10. Image compressed at different ratios, and corresponding extracted watermarks

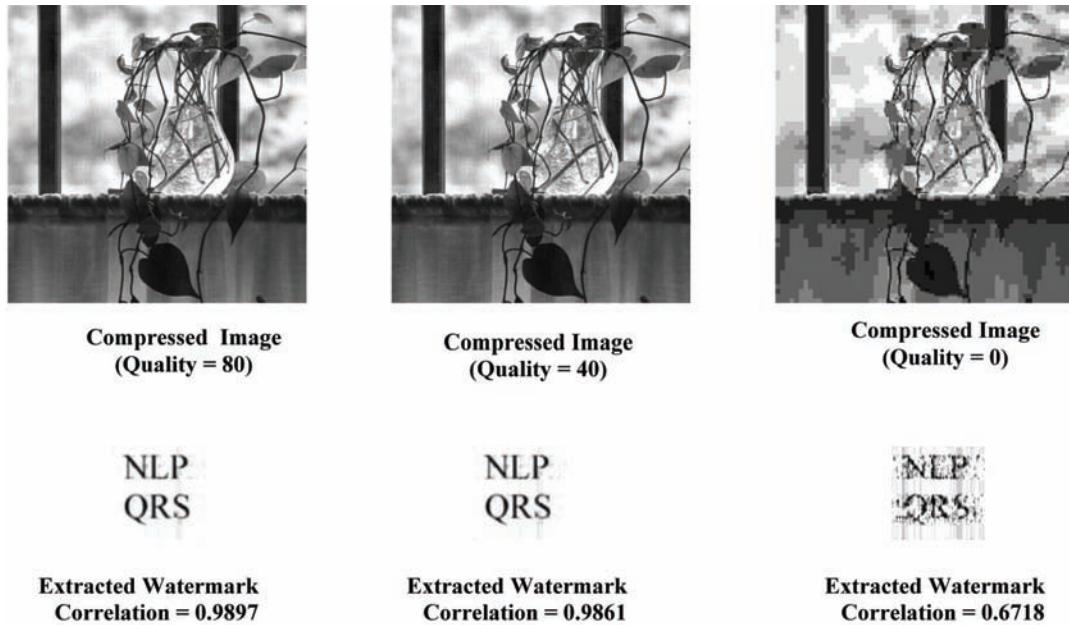


Figure 11. Image cropped at different ratios, and corresponding extracted watermarks

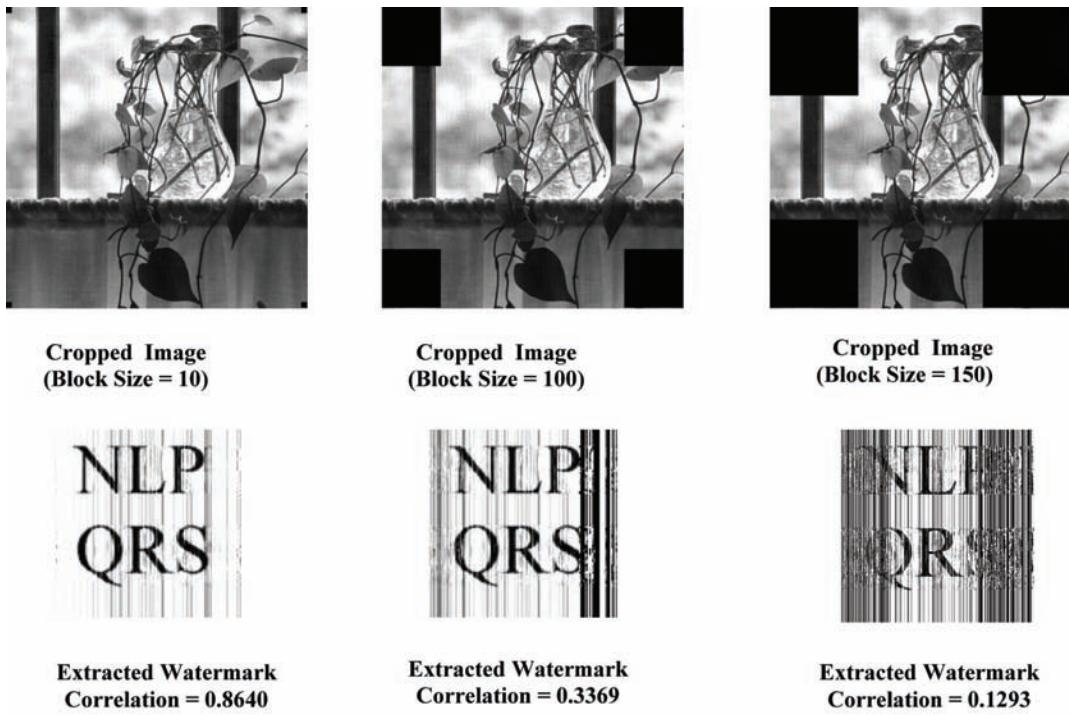


Figure 12. Image low-pass filtered at different ratios, and corresponding extracted watermarks

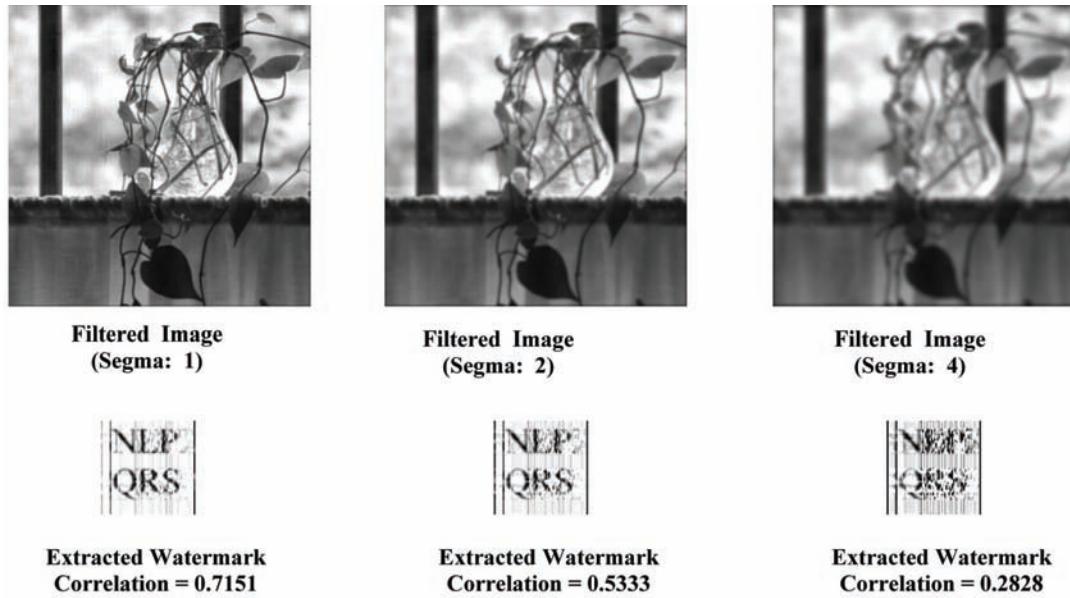


Figure 13. Image salt-pepper-noised at different ratios, and corresponding extracted watermarks

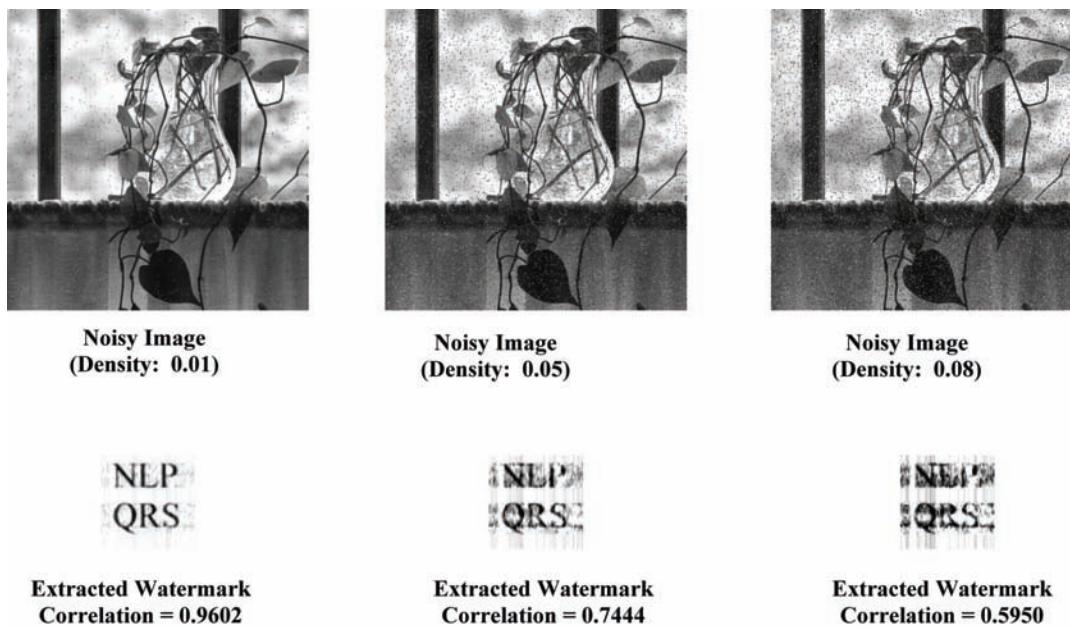
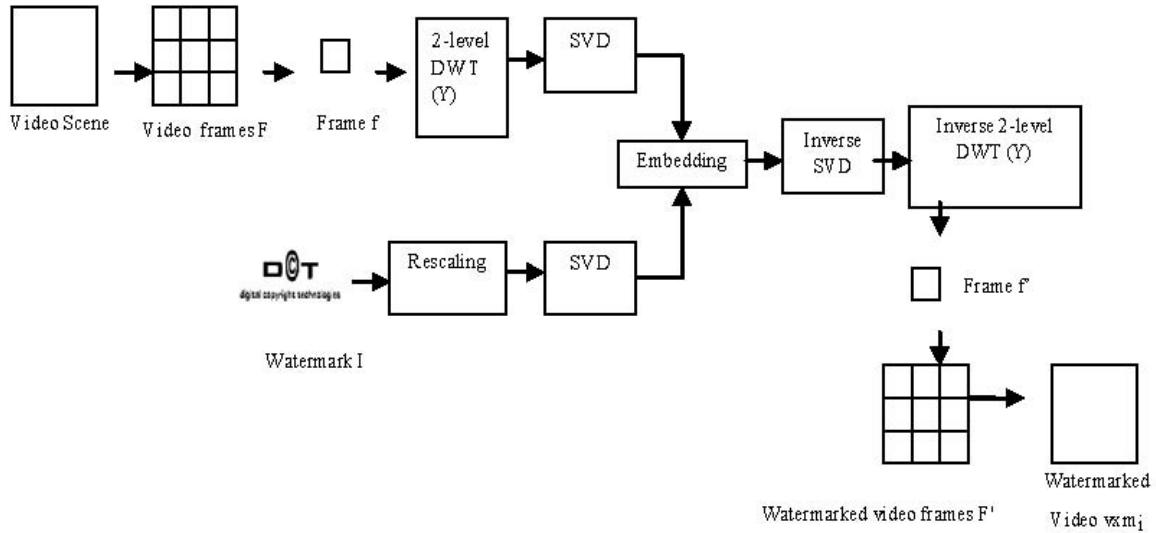


Figure 14. Video watermarking - the DWT-SVD based watermark-embedding procedure



Watermark Embedding Procedure

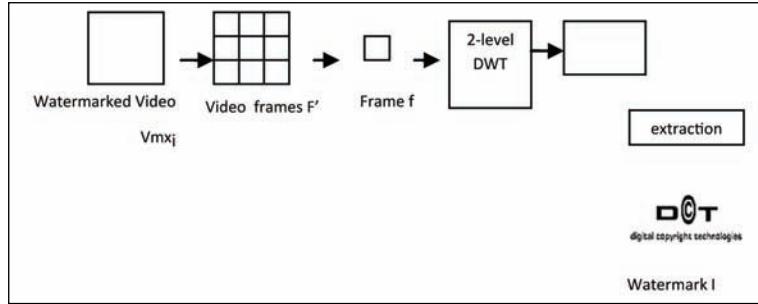
The embedding procedure is depicted in the block diagram shown in Figure 14, and described in details in the steps that follow.

1. Divide the video clip V into video scenes V_{S_i}
2. Process the frames of each video scene using DWT and SVD as described in steps 3 ~ 10.
3. Convert every video frame F from RGB to YUV color matrix format.
4. Compute the 2-level DWT for the Y (luminance) matrix in each frame F . This operation generates seven DWT sub-bands $[LL_1, LL_2, HL_2, LH_2, HH_2, LH_1, HH_1]$. Each sub-band is a matrix of DWT coefficients at a specific resolution.
5. Apply the SVD operator on the HL_2 sub-band. The SVD operator decomposes the sub -band's coefficient matrix into three independent matrices:

$$HL_2 = U_{HL_2} S_{HL_2} V_{HL_2} \quad (11)$$

6. Rescale the watermark image so that the size of the watermark will match the size of the HL_2 sub-band which will be used for embedding.
 7. Embed the binary bits of the watermark W_{Vsi} into S_{HL_2} by substituting the watermark bit W_i with the LSB (Least significant Bit) bit of $S_{HL_2}(i, i)$:
- $$LSB(S_{HL_2}(i, i)) = W_{Vsi} \quad (12)$$
8. Apply the inverse SVD operator on the modified S_{HL_2} ' matrix to get a modified coefficient matrix $HL2'$. The inverse SVD operation is as follows:
- $$HL2' = U_{HL_2} S_{HL_2}' V_{HL_2}^T \quad (13)$$
9. Apply the inverse DWT on the modified coefficient matrix $HL2'$. This operation produces the final watermarked Video frame F' .
 10. Convert the video frames F' from YUV to RGB color matrix.

Figure 15. Video watermarking - the DWT-SVD based watermark-extraction procedure



11. Reconstruct frames into the final watermarked Video scene V_{s_i}' .
12. Reconstruct watermarked scenes to get the final watermarked Video clip V' .

Watermark Extraction Procedure

The proposed DWT-SVD algorithm is blind in the sense that it does not need the original video in the extraction process. Therefore, we can extract the watermark image from the watermarked video frames from the LSBs directly, as depicted in the block diagram shown in Figure 15.

1. Divide the watermarked Video clip V' into watermarked scenes V_{s_i}' .
2. Process the watermarked frames of each watermarked video scene using DWT and SVD as described in s 3 ~ 6.
3. Convert the video frame F' from RGB color matrix to YUV.
4. Compute the 2-level DWT for the frame F' . Let the seven sub-bands produced after this process be: $[wLL_1, wLL_2, wHL_2, wLH_2, wHH_2, wLH_1, wHH_1]$.
5. Apply the SVD operator on the wHL_2 sub-band. The SVD operator decomposes the sub-band's coefficient matrix into three independent matrices:

$$wHL_2 = U_{wHL2} S_{wHL2} V_{wHL2}. \quad (14)$$

6. Extract the embedded watermark from the diagonal matrix S_{wHL2} as follows:

$$W_{s_i}(i) = LSB(S_{HL2}(i, i)) \quad (15)$$

7. Construct the watermark W_{s_i} by cascading all watermark bits extracted from all frames.
8. Repeat the same procedure for all video scenes.

Results and Performance Evaluation

We evaluated the performance of the proposed DWT-SVD video watermarking algorithm using a colored video clip having a size of 351 frames each of size of 240 x 352 pixels. The video clip was partitioned into four different scenes having the size of 101, 74, 102, and 75, frames, respectively. A snapshot of each scene is shown in Figure 16. The watermark was embedded in the Y component each frame of all scenes as described in the previous section. A different watermark was embedded in each of the four scenes. The four watermark images are shown below in Figure 17. The four watermarks have the same size of 72 x 181 pixels.

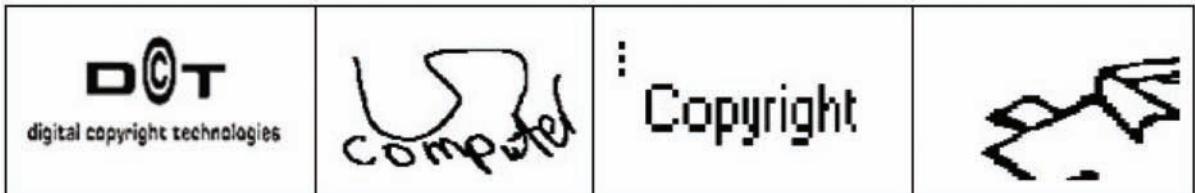
We evaluated the performance of the proposed DWT-SVD video watermarking algorithm with respect to two metrics: imperceptibility and robustness. Results are presented below.

Imperceptibility. Imperceptibility means that the perceived quality of the video clip should not be distorted by the presence of the watermark. As

Figure 16. Snapshots of the four scenes of the video clip



Figure 17. The four watermarks embedded in the scenes of the video clip



a measure of the quality of a watermarked video, the peak signal to noise ratio (PSNR) is typically used. In our work, the watermark was embedded in the video according the procedure described in details in the previous section. The average PSNR for the all frames of the four watermarked scenes was 48.1308, which proves imperceptibility of the proposed SVD-DWT algorithm.

Robustness. Robustness is a measure of the immunity of the watermark against attempts to remove it or degrade it by different types of digital signal processing attacks. We measured the similarity between the original watermark and the watermark extracted from the attacked watermark images using the correlation factor ρ which may take values between 0 to 1. In Figures 18 ~ 21 we show the robustness results obtained for three standard attacks: *rotation, JPEG compression, and salt and pepper noise*. The high correlation values obtained for all attacks clearly indicate the robustness of the algorithm against standard attacks. Brief description of the results obtained are summarized below.

Video Compression. The watermarked video frames were compressed with different quality factors. As shown in Figure 18, the correlation values indicate clearly robustness of the algorithm against the video compression.

Video Rotation. The watermarked video frames were rotated with different angles. As shown in Figure 19, the correlation values indicate clearly robustness of the algorithm against the video frames rotation.

Salt & Pepper Noise. A salt & pepper noise was added with varying intensities to the watermarked video frames. As shown in Figure 20, the correlation values indicate clearly robustness of the algorithm against the addition of salt & pepper noise.

Other than the standard attacks, we evaluated robustness due to video frame dropping. The attackers hope that by performing such an attack the embedded watermark will be degraded or removed without hindering the original video. This is due to the fact that large amount of redundancy exist between video frames, and therefore video dropping should leave the integrity of the original

Figure 18. Correlation values due to different rates of frame compression

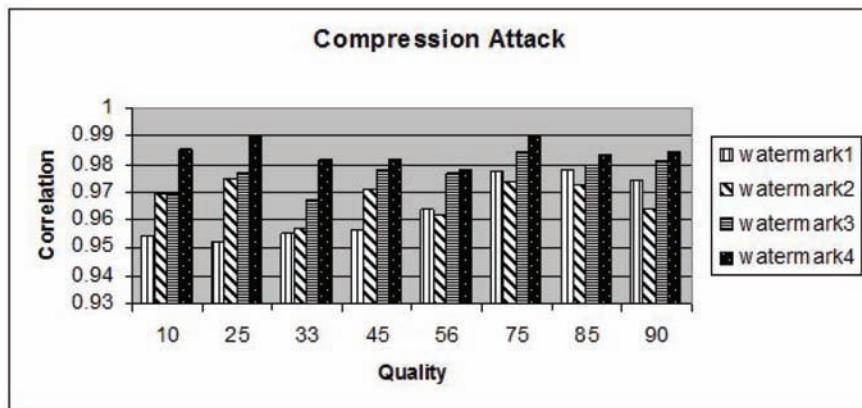


Figure 19. Correlation values due to frame rotations at different angles

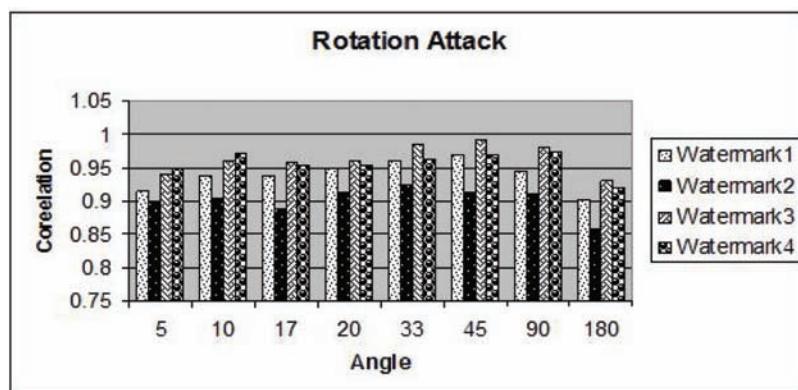


Figure 20. Correlation values due to Salt & pepper noise addition

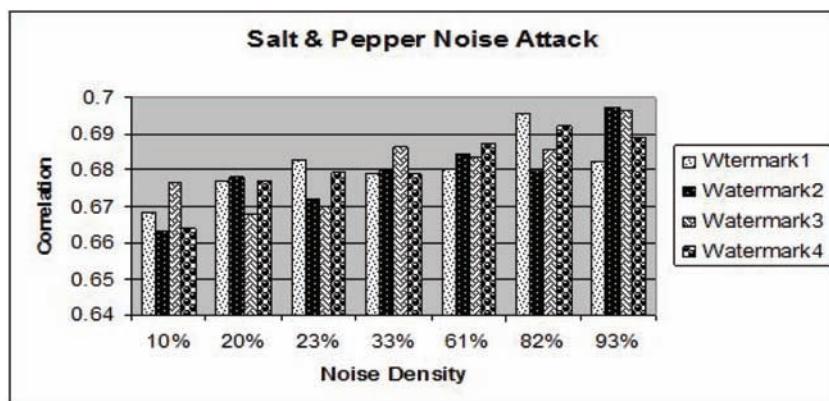
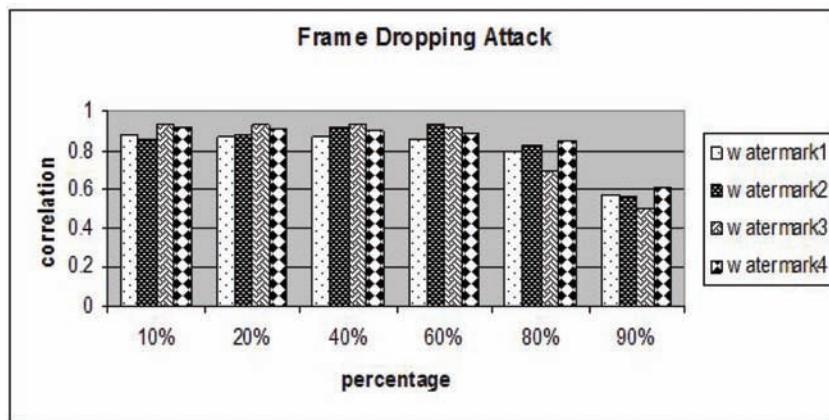


Figure 21. Correlation values due to video frame dropping



video intact. The results are shown in Figure 21. As seen, even if the attacker drops 60% of the frames, the watermark can still be extracted with a correlation value.

AUDIO WATERMARKING

Unauthorized copying and distribution of digital audio has become a dilemma for the music industry. As a matter of fact, it has been reported that the music industry claims a multi-billion dollar annual revenue loss due to piracy which is likely to increase due to file sharing web communities. Audio watermarking has been proposed as a promising technology to solve this problem. Audio watermarking exploits the irrelevant properties of the human auditory system (HAS) to establish copyright information in audio objects. In particular, HAS is insensitive to small amplitude changes in the time domain and frequency domains, allowing the addition of weak noise signals (watermarks) to the host audio signal such that the changes are inaudible. Frequency-domain techniques, in particular, have been more effective than time-domain techniques since watermarks are added to selected regions in the transformed domain of the host audio signal, such that inaudibility and robustness are maintained.

Many time-domain and frequency-domain audio watermarking algorithms have been proposed in the literature (Arnold, 2000; Bassia, Pitas, & Nikolaidis, 2001; Bassia, Pitas, & Nikolaidis, 2003; Basso, et al., 2009; Cvejic & Seppänen, 2002; Erelebi, & Bataki, 2009; Kim, & Choi, 2003; Kirovski & Malvar, 2003; Ko, Nishimura, & Suzuki, 2005; Lie & Chang, 2006; Malik, Ansari, & Khokhar, 2008; Ozer, Sankur, & Memon, 2005; Wang & Zhao, 2006; Wei & Xue, 2003; Wu, Su, & Kuo, 2000; Wu & Shimamoto, 2006; Yeo & Kim, 2003; Hsieh, Tseng, & Huang, 2001; Swanson, Zhu, Tewfic & Boney, 1998; Li & Yu, 2000; Chang, Tsai & Lin, 2005). In this section, we extend our hybrid-transform DWT-SVD approach to watermark audio signal imperceptibly and robustly.

Watermark Embedding Procedure

The watermark embedding procedure transforms the audio signal using DWT and SVD, embeds the bits of a binary image watermark in appropriate locations, and finally it produces a watermarked audio signal that contains an imperceptible watermark. The procedure is illustrated in the block diagram shown in Figure 22, and described in details below.

Figure 22. Audio watermarking - the DWT-SVD based watermark-embedding procedure

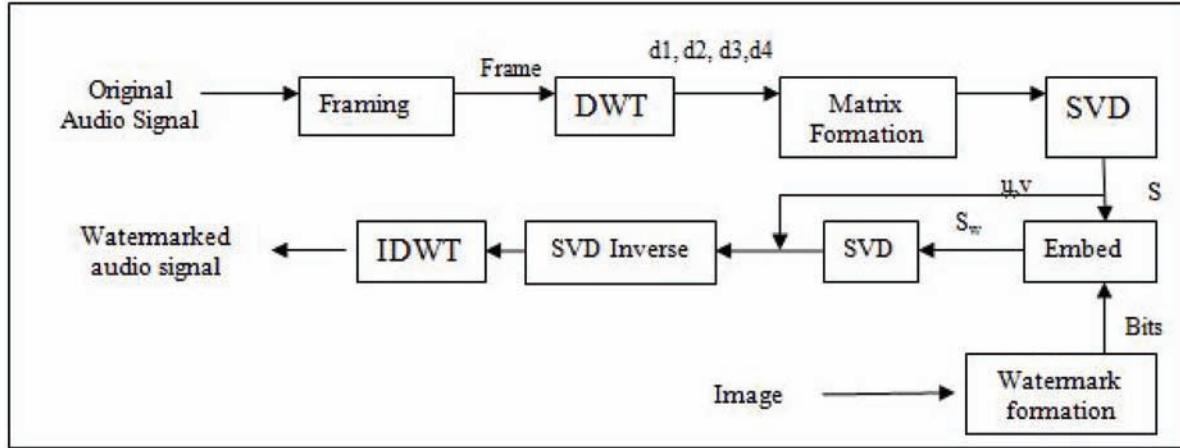


Figure 23. A vector representing multi-resolution sub-bands of the four-level DWT operation

A	D4	D3	D2	D1
---	----	----	----	----

1. A binary image is used as a watermark. A binary image is believed to be more convenient because it contains more meaningful information about the copyright owner, in addition to the fact that an image could still be identified if some of its bits go missing during extraction. The watermark image used here is a binary image represented by matrix $I (m \times n)$.
2. Convert matrix I into a one dimensional vector W of length $m \times n$.

$$W_i = \{[0, 1], 1 \leq i \leq (m \times n)\} \quad (16)$$

3. Sample the original (WAV) audio signal at sampling rate of 44100 sample per second. The sampled file is broken down into frames of multiples of 50,000 samples in length. The total number of ‘overlapping’ frames is N as given in Equation (17).

$$A = \sum_{i=1}^N A_i \quad (17)$$

The length of the frame (50,000 samples) was chosen to enable higher level of DWT decomposition, and to increase maximum watermark payload and the size of the watermark to be embedded.

4. Perform a four-level DWT transformation on each frame A_i of the sampled audio signal A . This operation produces five multi-resolution one-dimensional sub-bands: D1, D2, D3, D4 and A4. The D sub-bands represent the detailed-coefficients and the A sub-band represents the approximated-coefficients sub-band. The four sub-bands are arranged in the vector shown in Figure 23.
5. Form a matrix using the four detailed coefficients sub-bands D1, D2, D3, D4 as shown in Figure 24 below. The matrix, named DC

Figure 24. Matrix formulation of the of detailed coefficients sub-bands

D1							
D2				D2			
D3		D3		D3		D3	
D4	D4	D4	D4	D4	D4	D4	D4

thereafter, is of size $4 \times (L/2)$ where L is the frame length.

6. Apply the SVD operator on the \mathbf{DC} matrix producing the three orthonormal matrices \mathbf{S} , \mathbf{U} and \mathbf{V}^T as follows:

$$\mathbf{DC} = \mathbf{U} \times \mathbf{S} \times \mathbf{V}^T \quad (18)$$

The \mathbf{S} matrix is a 4×4 diagonal matrix which has the following format:

$$\mathbf{S} = \begin{bmatrix} S_{11} & 0 & 0 & 0 \\ 0 & S_{22} & 0 & 0 \\ 0 & 0 & S_{33} & 0 \\ 0 & 0 & 0 & S_{44} \end{bmatrix} \quad (19)$$

where the diagonal S_{ii} entries are the non-zero singular values of the \mathbf{DC} matrix. The four S_{ii} values are used for embedding as will be shown later, and need to be stored for later use in the watermark extraction process.

7. Form a watermark matrix \mathbf{W} using 12 watermark bits obtained from the original watermark.

$$\mathbf{W} = \begin{bmatrix} 0 & bit1 & bit2 & bit3 \\ bit4 & 0 & bit5 & bit6 \\ bit7 & bit8 & 0 & bit9 \\ bit10 & bit11 & bit12 & 0 \end{bmatrix} \quad (20)$$

For example, for the watermark bit pattern 1010 0011 0101, the watermark matrix \mathbf{W} will have the following formation:

$$\mathbf{W} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad (21)$$

8. Embed the watermark bits into the DWT-SVD-transformed audio signal according to the following formula: The general watermark embedding formula:

$$S_w = S + 3 \times W ; \quad (22)$$

where α is the watermark intensity. α has been chosen to be 3 to minimize the distortion caused from adding the watermark. Many values for α were tested, and this one was found optimal.

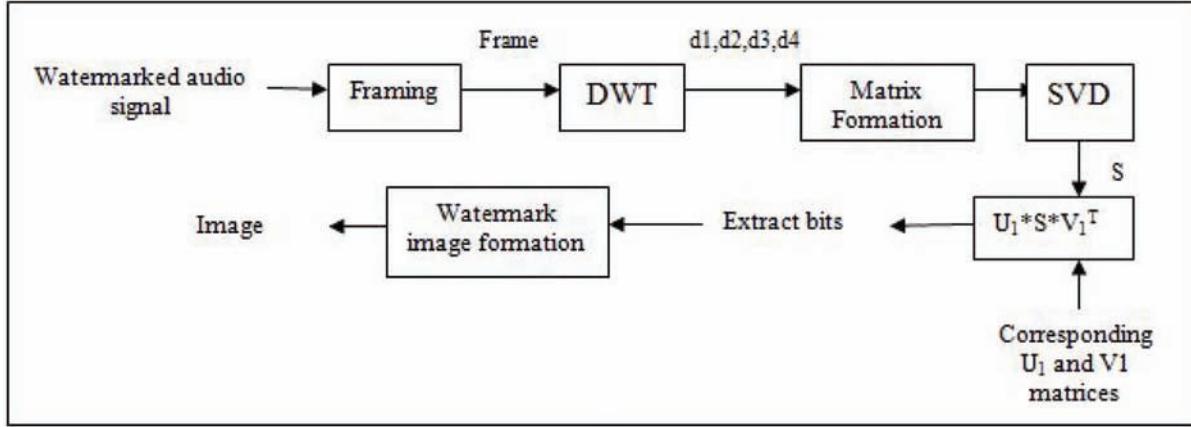
9. The new matrix S_w enters a new stage of SVD which produces three new matrices

$$S_w = U_1 \times S_1 \times V_1^T \quad (23)$$

where the matrices \mathbf{U}_1 and \mathbf{V}_1 are stored for later use in extraction.

10. Perform the inverse SVD operation with the \mathbf{U} and \mathbf{V}^T matrices unchanged and the

Figure 25. Audio watermarking - the DWT-SVD based watermark-extraction procedure



S matrix modified as described in Equation (20).

- $$CD_w = U \times S_1 \times V^T \quad (24)$$
11. Use the new values of the watermarked CD_w matrix to modify the D sub-bands or detailed coefficients given in Figure 23. For duplicate portions the first one was chosen.
 12. Perform the Inverse DWT operation to obtain each watermarked audio frame A_{iw}
 13. Obtain the overall watermarked audio signal by cascading the watermarked frames obtained in step 3 in the same order.

$$A_w = \sum_i A_{iw} \quad (25)$$

Watermark Extraction Procedure

Given the watermarked audio signal and the corresponding U_1 and V_1 matrices that have been computed in Equation (23) and stored for each frame, the watermark can be extracted according the procedure outlined in Figure 25 and described in details in the following steps.

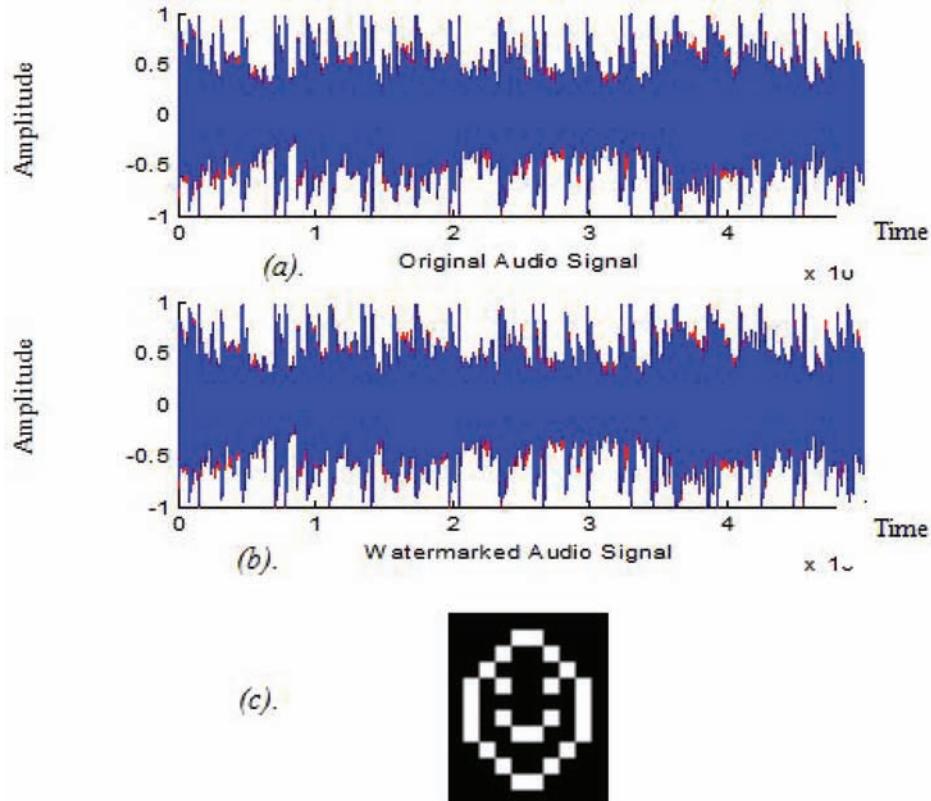
1. Obtain matrix S from each frame of the watermarked audio signal following the general steps presented in Figure 25.
2. Multiply the matrix by U_1 and V_1 which have been computed in the watermark embedding procedure and stored for use in the extraction process. This results in the matrix M_{4x4} , as shown below:

$$M_{4x4} = U_1 \times S \times V_1^T \quad (26)$$

3. To extract the 12 watermark bits from each frame, examine non-diagonal values of the M_{4x4} matrix. It has been experimentally noticed that there are two groups of non-diagonal values that are extremely distinct, meaning that the values at the positions where a 0 bit has been embedded tend to be much smaller than those values at the positions where a 1 bit has been embedded. Thus, to determine the watermark bit $w(n)$, the average of non-diagonal values is first computed, name it avg , then for each non-diagonal value M_{ij} $w(n)$ is extracted according to the following formula:

$$w(n) = \begin{cases} 0 & M_{i,j} \leq avg \\ 1 & \text{Otherwise} \end{cases} \quad (27)$$

Figure 26. (a). The original pop signal, (b). the watermarked pop signal, (c). the original watermark



4. Assemble the extracted bits form the individual frames to construct the original watermark image.

Results and Performance Evaluation

Audio signals can be of different types; instrumental, pop, speech, and others. Each type has its own different perceptual properties and therefore watermarking performance may vary from type to type. A Pop music file of length 600,000 samples (13 seconds) has been used to evaluate our proposed algorithm. The pop file (pop.wav) is a stereo type signal that left and right channels. The proposed embedding procedure embeds a watermark into both channels. The original pop audio signal is shown in Figure 26, before being watermarked as in Figure 26(a), and after being

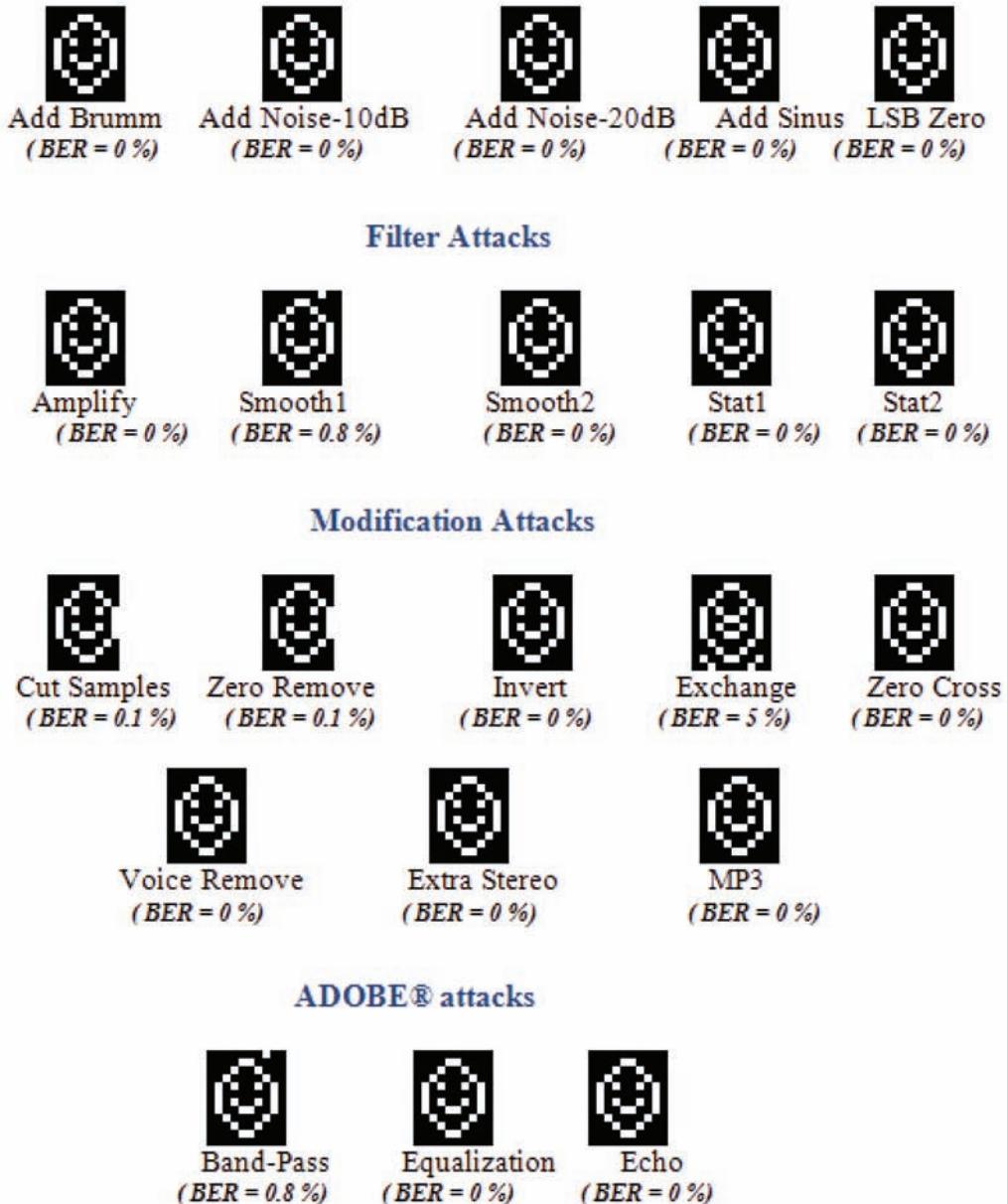
Table 1. SDG Rates Description

SDG	Description
5	Imperceptible
4	Perceptible, but not annoying
3	Slightly annoying
2	Annoying
1	Very Annoying

watermarked as in Figure 26(b). The watermark that we used to evaluate the performance of the proposed watermarking algorithm is shown in Figure 26(c). It's 12 x 10 binary image. The size of the image watermark has been chosen taking into consideration the length of the host audio files.

Performance of Audio watermarking algorithms is usually evaluated with respect to sev-

Figure 27. Extracted watermarks after applying different attacks to the watermarked pop signal



eral metric including: fidelity, imperceptibility (inaudibility), and robustness (Grody & Brutun, 2000; Sehirli, Gurgen, & Ikizoglu, 2004; Steinebach, et al., 2001). In this section we give a brief description of each metric and the corresponding results obtained.

- **Fidelity.** The similitude between the original audio signal and the distorted watermarked audio signal has been measured using PSNR, as described earlier. The computed PSNR values were 51.1083 for α equals 3.0, and 43.1998 for α equals 5.0.

- **Imperceptibility (Inaudibility).** To get an estimation of the audio quality the PEAQ method was used “Perceptual Evaluation of Audio Quality” (PEAQ). Table 1 lists the output values of the PEAQ system. The PEAQ listening test was performed with 5 listeners. The achieved the given rate was (5) indicating perfect audibility and thus imperceptible watermarking.
- **Robustness..** To evaluate robustness of the proposed audio watermarking algorithms we implemented a set of attacks that have commonly affect audio signals. Most of implemented attacks have been defined by Stirmark® watermarking benchmark. They include three different classes of attacks; Add/Remove attacks, Filter attacks, and Modification attacks. The watermarks extracted after application of the various attacks are given in the following figures. The effects of the attacks vary from one attack to another, however, as shown below in Figure 27, it was possible to extract the embedded watermark after each attack.

To measure the robustness of a watermarking algorithm to a signal processing attack, a measurement metric called the bit error rate (BER) is computed. BER reflects the certainty of detection of the embedded watermark and is expressed by Equation (28) below which defines the ratio of incorrect extracted bits to the total number of embedded bits.

$$w(n) = \begin{cases} 0 & M_{i,j} \leq avg \\ 1 & Otherwise \end{cases} \quad (28)$$

Where I is the watermark length, W_n corresponds to the n^{th} bit of the embedded watermark and W'_n corresponds to the n^{th} bit of the extracted watermark. As shown in Figure 27, BER is 0% for most extracted images except for the *Exchange* attack, where its equal to 5%, and for the *Smooth1* and

Band Pass attacks, its equal to 0.8% for each. The *Zero Remove* and *Cut Samples* have low BER values equal to 0.1.

CONCLUSION

In this chapter we described three imperceptible and robust watermarking techniques for different types of multimedia objects (image, video, audio). The proposed techniques were based on cascading two powerful mathematical transforms; the Discrete Wavelet Transform (DWT), and the Singular Value Decomposition (SVD). The two transforms are different transform domain techniques and thus provided different, but complementary, levels of robustness against the same attack. Effectiveness of the proposed algorithms was demonstrated through extensive experimentation for each media type.

REFERENCES

- Andrews, H., & Patterson, C. (1976). Singular Value decompositions and Digital Image Processing. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 24(1), 26–53. doi:10.1109/TASSP.1976.1162766
- Arnold, M. (2000). Audio watermarking: features, applications and algorithms. In *Proceeding. of the IEEE International Conference on Multimedia and Expo*, (Vol. 2, pp. 1013-1016).
- Arnold, M., Schumucker, M., & Wolthusen, S. (2003). *Techniques and Applications of Digital Watermarking and Content Protection*. Boston: Artech House.
- Bassia, P., Pitas, L., & Nikolaidis, N. (2001). Robust Audio Watermarking in the Time- Domain. *IEEE Transactions on Multimedia*, 3(2), 232–242. doi:10.1109/6046.923822

- Bassia, P., Pitas, L., & Nikolaidis, N. (2003). A temporal-domain audio watermarking technique. *IEEE Transactions on Signal Processing*, 51(4), 1088–1097. doi:10.1109/TSP.2003.809372
- Basso, A., Bergadano, F., Cavagnino, D., Pomponiu, V., & Vernone, A. (2009). A Novel Block-based Watermarking Scheme Using the SVD Transform. *Algorithms*, 2(1), 46–75. doi:10.3390/a2010046
- Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, 35, 313–336. doi:10.1147/sj.353.0313
- Chan, C., & Cheng, L. (2004). Hiding Data in Images by Simple LSB Substitution. *Pattern Recognition*, 37(3), 469–474. doi:10.1016/j.patcog.2003.08.007
- Chan, P., & Lyu, M. (2003). ADWT-Based Digital Video Watermarking Scheme with Error Correcting Code. In *Proceedings of the 5th International Conference on Information and Communications Security*, (pp. 202-213).
- Chang, C., Tsai, P., & Lin, C. (2005). SVD-based digital image watermarking scheme. *Pattern Recognition Letters*, 26(10), 1577–1586. doi:10.1016/j.patrec.2005.01.004
- Chu, W. (2003). DCT-Based Image Watermarking Using Subsampling. *IEEE Transactions on Multimedia*, 5(1), 34–38. doi:10.1109/TMM.2003.808816
- Cox, I., Miller, M., & Bloom, J. (2002). *Digital Watermarking*. New York: Academic Press.
- Cvejic, N., & Seppänen, T. (2002). Increasing the capacity of LSB-based audio steganography. In *Proceedings of the IEEE International Workshop on Multimedia Signal Processing*, (pp. 336–338).
- Doerr, G., & Dugelay, J. (2003). A Guided Tour to Video Watermarking. *Signal Processing Image Communication*, 18, 263–282. doi:10.1016/S0923-5965(02)00144-3
- Ejima, M., & Myazaki, A. (2001). On the evaluation of performance of digital watermarking in the frequency domain. In *Proceedings of the IEEE International Conference on Image Processing*, Thessaloniki, Greece.
- Erelebi, E., & Bataki, L. (2009). Audio watermarking scheme based on embedding strategy in low frequency components with a binary image. *Digital Signal Processing*, 19(2), 265–277. doi:10.1016/j.dsp.2008.11.007
- Ganic, E., & Eskicioglu, A. (2004). Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies. In *Proceedings of the ACM Workshop on Multimedia and Security*, Germany.
- Gao, X., & Tang, X. (2002). Unsupervised Video-Shot Segmentation and Model-Free Anchorperson Detection for News Video Story Parsing. *IEEE Trans. Circuits and Systems for Video Technology*, 12(9), 765–776. doi:10.1109/TCSVT.2002.800510
- Grody, J., & Brutun, L. (2000). Performance Evaluation of Digital Audio Watermarking algorithms. In *Proceedings of the 43rd IEEE Midwest Symposium on Circuits and Systems*, (pp. 456-459).
- Guo, H., & Georganas, N. (2002). Multi-resolution Image Watermarking Scheme in the Spectrum Domain. In *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering*, Canada.
- Guzman, V., Miyatake, M., & Meana, H. (2004). Analysis of Wavelet –Based Watermarking Algorithm. In *Proceedings of the 14th International IEEE Conference on Electronics, Communications and Computers*, Veracruz, Mexico.
- Hartung, H., & Girod, B. (1998). Watermarking of Compressed and Un-Compressed Video. *Signal Processing*, 66(3), 283–301. doi:10.1016/S0165-1684(98)00011-5

- Hsieh, M., Tseng, D., & Huang, Y. (2001). Hiding Digital Watermarks Using Multiresolution Wavelet Transform. *IEEE Transactions on Industrial Electronics*, 48(5), 875–882. doi:10.1109/41.954550
- Hsu, C., & Wu, J. (1998). Multiresolution Watermarking for Digital Images. *IEEE Transactions on IEEE Transactions on Circuits and Systems II*, 45(8), 1097–1101. doi:10.1109/82.718818
- Huang, J., & Yang, C. (2004). Image Digital Watermarking Algorithm Using Multiresolution Wavelet Transform. In *Proceedings of the International IEEE Conference on Systems, Man, and Cybernetics*, the Hague, the Netherlands.
- Jung, H., Cho, S., & Shik, S. Koh, Chung, Y., Lee, K., Lee, S. & Kim, C. (2003). Image Watermarking Based on Wavelet Transform Using Threshold Selection. In *Proceedings of the International IEEE SICE Conference*.
- Katzenbeisser, S., & Petitcolas, F. (2000). *Information Hiding: Techniques for Steganography and digital watermarking*. Boston: Artech House.
- Kim, H., & Choi, Y. (2003). A Novel Echo-hiding Scheme with backward and Forward Kernels. *IEEE Transactions on Circuits and Systems for Video Technology*, 13(8), 885–889. doi:10.1109/TCSVT.2003.815950
- Kirovski, D., & Malvar, H. (2003). Spread Spectrum watermarking of Audio Signals. *IEEE Transactions on Signal Processing*, 51(4), 1020–1033. doi:10.1109/TSP.2003.809384
- Ko, B. S., Nishimura, R., & Suzuki, Y. (2005). Time-spread echo method for digital audio watermarking. *IEEE Transactions on Multimedia*, 7(2), 212–221. doi:10.1109/TMM.2005.843366
- Kundur, D., Su, K., & Hatzinakos, D. (2004). Digital Video Watermarking: Techniques, Technology, and Trends. In Pan, P., Huang, H., & Jain, L. (Eds.), *Intelligent Watermarking Techniques* (pp. 265–314). Singapore: World Scientific Computing.
- Langelaar, G., Setyawan, I., & Lagendijk, R. (2000). Watermarking Digital Image and Video Data: A State-of-Art Overview. *IEEE Signal Processing Magazine*, 17(5), 20–46. doi:10.1109/79.879337
- Li, X., & Yu, H. (2000). Transparent and robust audio data hiding in sub-band domain. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, (pp. 74–79).
- Lie, W., & Chang, L. (2006). Robust and high-quality time-domain audio watermarking based on low-frequency amplitude modification. *IEEE Transactions on Multimedia*, 8(1), 46–59. doi:10.1109/TMM.2005.861292
- Liu, R., & Tan, T. (2002). A SVD-Based Watermarking Scheme for Protecting Rightful Ownership. *IEEE Transactions on Multimedia*, 4(1), 121–128. doi:10.1109/6046.985560
- Malik, H., Ansari, R., & Khokhar, A. (2008). Robust audio watermarking using frequency-selective spread spectrum. *IET Information Security*, 2(4), 129–150. doi:10.1049/iet-ifs:20070145
- Mallat, S. (1989). A theory for multi-resolution signal decomposition: The wavelet Representation. *IEEE Trans. on Pat. Anal. Mach. Inte.*, 11(7), 674–693.
- Mitra, S. (1998). *Digital Signal Processing*. Columbus, OH: McGraw –Hill.

- Mohammad, A., Al-Haj, A., & Shaltaf, S. (2008). An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Processing Journal*, 88(9), 2158–2180. doi:10.1016/j.sigpro.2008.02.015
- Nahrstedt, K., & Qiao, L. (1998). *Non-Invertible Watermarking Methods for MPEG Video and Audio*. Paper presented at the ACM Multimedia Security Workshop, England.
- Niu, X., Lu, Z., & Sun, S. (2000). Digital Image Watermarking Based on Multi-resolution Decomposition. *IEEE Electronics Letters*, 36(13), 1108–1110. doi:10.1049/el:20000819
- Ozer, H., Sankur, B., & Memon, N. (2005). An SVD-based audio watermarking technique. In *Proceedings of the Multimedia and Security Workshop*, (pp. 51-56).
- Potdar, V., Han, S., & Chang, E. (2005). A Survey of Digital Image Watermarking Techniques. In *Proceedings of the 3rd International IEEE Conference on Industrial Informatics*, Perth, Australia.
- Qiao, L., & Nahrstedt, K. (1998). Watermarking Schemes and Protocols For Protecting Rightful Ownership and Customer's Rights. *Journal of Visual Communication and Image Representation*, 9(3), 194–210. doi:10.1006/jvci.1998.0391
- Ramkumar, M., & Akansu, A. (2004). A Robust Protocol for Proving Ownership of Multimedia Content. *IEEE Transactions on Multimedia*, 6(3), 496–478. doi:10.1109/TMM.2004.827494
- Reddy, A., & Chatterji, B. (2005). A New Wavelet Based Logo-watermarking Scheme. *Pattern Recognition Letters*, 26(7), 1019–1027. doi:10.1016/j.patrec.2004.09.047
- Safabakhsh, R., Zaboli, S., & Tabibiazar, A. (2004). Digital Watermarking on Still Images Using Wavelet Transform. In *Proceedings of the International IEEE Conference on Information Technology: Coding and Computing*, Las Vegas, Nevada.
- Sebe, F., Domingo-Ferrer, J., & Herrera, J. (2000). Spatial Domain Image Watermarking Robust Against Compression, Filtering, Cropping, and Scaling. In *Proceedings of the 3rd Int. Workshop on Info. Security*, Australia.
- Sehirli, M., Gurgen, F., & Ikizoglu, S. (2004). Performance evaluation of digital audio watermarking techniques designed in time, frequency and cepstrum domains. In *Proceedings of the International Conference on Advances in Information Systems*, (pp. 430–440).
- Steinebach, M., Petitcolas, F., Raynal, F., Dittmann, J., Fontaine, C., Seibel, S., et al. (2001). Stirmark benchmark: Audio watermarking attacks. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, (pp. 49–54).
- Strang, G., & Nguyen, T. (1996). *Wavelets and Filter Banks*. Wellesley, MA: Wellesley-Cambridge Press.
- Swanson, M., Zhu, B., Tewfic, A., & Boney, L. (1998). Robust audio watermarking using perceptual masking. *Signal Processing*, 66(3), 337–355. doi:10.1016/S0165-1684(98)00014-0
- Voloshynovskiy, S., Pereira, S., & Pun, T. (2001). Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks. *Communications Magazine*, 39(8), 118–126. doi:10.1109/35.940053
- Wang, C., Doherty, J., & Van Dyke, R. (2002). A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images. *IEEE Transactions on Image Processing*, 11(2), 77–78. doi:10.1109/83.982816
- Wang, X., & Zhao, H. (2006). A novel synchronization invariant audio watermarking scheme based on DWT and DCT. *IEEE Transactions on Signal Processing*, 54(12), 4835–4840. doi:10.1109/TSP.2006.881258

- Wei, L., & Xue, X. (2003). An audio watermarking technique that is robust against random cropping. *Computer Music Journal*, 27(4), 58–68. doi:10.1162/014892603322730505
- Wu, C., Su, P., & Kuo, J. (2000). Robust and Efficient Digital Audio Watermarking Using Audio Content analysis. In *Proceedings of the SPIE 12th International Symposium on Electronic Imaging, CA* (Vol. 3971, pp. 382-392).
- Wu, Y., & Shimamoto, S. (2006). A Study on DWT-Based Digital Audio Watermarking for Mobile Ad Hoc Networks. In *Proceedings of the International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*.
- Yeo, I. K., & Kim, H. J. (2003). Modified patchwork algorithm: A novel audio watermarking scheme. *IEEE Transactions on Speech and Audio Processing*, 11(4), 381–386. doi:10.1109/TSA.2003.812145

Chapter 11

Data Hiding Schemes Based on Singular Value Decomposition

Victor Pomponiu

University of Torino, Italy

Davide Cavagnino

University of Torino, Italy

Alessandro Basso

University of Torino, Italy

Annamaria Vernone

University of Torino, Italy

ABSTRACT

Information hiding techniques are acquiring an always increasing importance, due to the widespread diffusion of multimedia contents. Several schemes have been devised in the fields of steganography and digital watermarking, exploiting the properties of different domains. In this chapter, the authors focus on the SVD transform, with the aim of providing an exhaustive overview (more than 100 papers are analyzed) on those steganography and watermarking techniques leveraging on the important properties of such a transform. The large number of algorithms operating in the image, video and audio contexts is first classified by means of a general approach, then analyzed, to highlight the advantages and disadvantages of each method. The authors also give a detailed discussion about the applicability of each reviewed and compared data hiding scheme, in order to identify the most appropriate candidates for practical applications.

INTRODUCTION

Due to the rising dependence on digital media and the unexpected expansion of the distribution opportunities over the Internet, techniques for hiding information into digital contents are achieving

significant importance. Such techniques aim to provide the ability to communicate secretly and the capacity to protect copyrighted multimedia content against illegal distribution. Designing such schemes has become a topic of great importance and many researchers have spent much effort in the last years to obtain an effective solution. However, despite

DOI: 10.4018/978-1-61520-903-3.ch011

many different approaches have been attempted, there is currently no scheme that can preserve imperceptibility of the hidden data while ensuring a high security against malicious attacks.

To help characterizing the differences in capacity, requirements and intended use, data hiding is often divided into two broad subcategories:

- *Steganography* (from the Greek words στεγανός and γράφειν that mean “cover writing”) enables secret communication and is characterized by obscuring the existence of secret messages enclosed into apparently inoffensive cover media (Katezenbeisser & Petitcolas, 1999). Unlike cryptography which aims to scramble the content of the message to keep it secret, the main intention of steganography is to facilitate the existence of a hidden channel that permits transmission of private messages. The model for this secret communication was inspired from a famous example called the “prisoners’ problem” (Simmons, 1984). Briefly, two persons, Alice and Bob, are arrested and thrown in prison. During detention, they try to devise an escape plan. However, there is a prison guard, called Eve, which examines the messages exchanged between each other, making the communication extremely difficult. Therefore, Alice and Bob are forced to exchange cover messages, which in reality contain hidden messages linked to the escape plan. In this model, the guardian may have a passive involvement, only observing the messages, or an active implication, trying to modify the private messages without destroying the cover message.
- *Digital watermarking* is a widespread information hiding technique, aimed to resolve different multimedia security issues (e.g., copyright protection, illegal distribution, broadcast monitoring and authentication) by embedding secret information

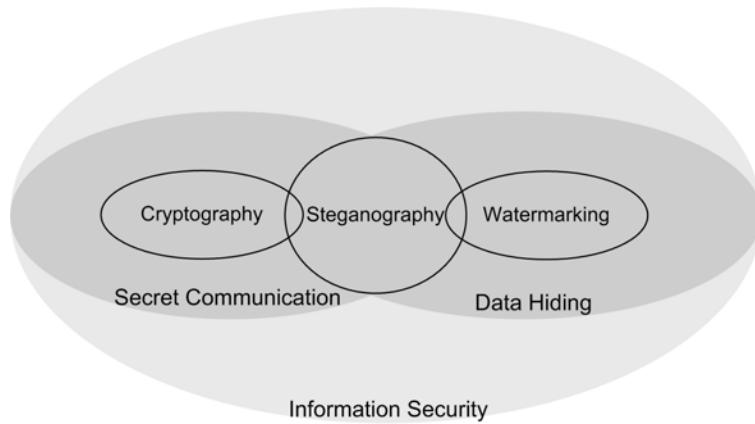
(i.e., digital watermarks) into media contents. However, differently from steganography, the fact that a content is watermarked is not necessarily a secret. Hence, watermarking techniques require an intrinsic higher robustness if compared to steganography methods, due to the existence of a whole class of attacks aimed to specifically remove the embedded information. Moreover, it should not be possible to remove the inserted watermark without possessing additional information (e.g., a secret key) while maintaining the usability of the digital content. For these reasons, the watermarking context is generally considered more challenging and demanding in terms of security requirements than steganography. Furthermore, while steganographic transmission takes place between two parties, i.e., sender and receiver, watermarking schemes involve one-to-many communication (Katezenbeisser & Petitcolas, 1999).

In the last years, information security requirements have changed from traditional mechanisms to complex and integrated schemes which are able to protect data during transmission. However, each of such hiding schemes cannot provide a complete security solution, since different applications use them to assess a specific goal (i.e., secret communication or copyright protection) in a particular framework. A reliable security solution should wisely combine these primary mechanisms, i.e., cryptography, steganography and watermarking, into a global system (Barni, Bartolini & Furon, 2005; Chandramouli, Kharrazi & Memon, 2004).

It is worthwhile to point out that the secret message can be encrypted before embedding, thus improving the security of the data hiding schemes. The main security primitives, along with their spheres of application, are outlined in Figure 1.

Several techniques have been devised for steganography and digital watermarking. Among

Figure 1. The main security primitives and their application relationships



them, SVD has obtained a wide popularity due to its own intrinsic properties. The Singular Value Decomposition is a powerful numerical tool for factorizing matrices that has been formerly applied to various signal processing applications. The essential characteristic of the SVD is the slight variation of singular values when a wide variety of image processing operations and geometric transforms are applied to the matrix. The SVD transform began to be used extensively in various data hiding schemes especially for devising robust watermarking algorithms resistant to geometric attacks. Indeed, many of the existing SVD-based techniques insert the secret information into the singular values of the cover signal, which implies a high robustness against common and geometric attacks but, in contrast, a complete vulnerability towards attacks based on noise addition or singular value modification or substitution.

Moreover, it was recently discovered that a specific issue, referred as the ambiguity problem, affects the features of the SVD transform. In some cases this problem determines the inability to ensure the correct detection of hidden data and consequently the impossibility to certainly identify the ownership of a media (Rykaczewski, 2007; Ting, Goi & Heng, 2008; Ting, 2006; Wu, 2005; Xiao-Ping & Kan, 2005; Zhang & Li, 2005). However, in the last years the powerful features

of this transform attracted many researchers, sometimes without them taking into account its difficulties. For this reason, numerous emerging SVD-based applications have appeared for various types of digital contents (e.g., image, voice and video), making them difficult to classify, analyze and evaluate.

In this chapter we focus on the main data hiding techniques (i.e., steganography and digital watermarking) which work in the SVD transform domain. Firstly, we propose a general approach to classify the applications based on SVD in the context of data hiding. Furthermore, we emphasize the issues and challenges, such as robustness, security, fidelity and data capacity of these techniques. Whenever possible, for those schemes which are not affected by ambiguity, a comparison with well-known data hiding schemes is presented. In depth, we examine different possibilities of performing the SVD transform over the cover media, highlighting the advantages and disadvantages of each technique. We therefore conclude this chapter with a detailed discussion of the applicability of each reviewed and compared data hiding scheme.

The chapter is organized as follows: the first section presents in detail the SVD transform together with its properties and characteristics, while the second section focuses on the design of the

most relevant work related to data hiding based on singular values, singular vectors or combined features. Future research directions of data hiding techniques based on SVD and several concluding remarks are given in the last section.

BACKGROUND

This section overviews the Singular Value Decomposition, an essential tool for numerical analysis. In addition, the main features and properties of the transform are discussed, highlighting their meaning for different types of multimedia content.

The SVD Transform

One of the most interesting and important developments of linear algebra is the concept of Singular Value Decomposition of matrices. In essence, the SVD is a matrix factorization technique. It is applicable to rectangular matrices with complex or real values and has been extensively applied in information retrieval, recommender systems and signal processing, like image compression (Anderson & Patterson, 1976; Yang & Lu, 1995), noise reduction (Hou, 2003) or data hiding. The SVD transform was also employed to assess the image quality under different types of distortions (Shnayderman, Gusev & Eskicioglu, 2004).

Consider a digital content that can be represented as an $m \times n$ matrix, $A_{m \times n}$; then, the singular value decomposition of A is defined as:

$$SVD(A_{m \times n}) = [U_{m \times m}, S_{m \times n}, V_{n \times n}] \quad (1)$$

Another way to define the matrix $A_{m \times n}$ is as a weighted sum of outer products:

$$A_{m \times n} = \sum_{i=1}^p \sigma_i u_i v_i^T, \quad p = \min(m, n) \quad (2)$$

where $\sigma_i \in \mathbb{R}_+, i=1 \dots p$ are the *singular values*, i.e., the diagonal components of the matrix S sorted in descending order, u_i are the corresponding *left singular vectors*, i.e., the columns of U , and v_i^T denotes the transpose of v_i which are the related *right singular vectors*, i.e., the rows of V^T (or columns of V). U and V are unitary matrices, that means $U \cdot U^T = I_{m \times m}$, $V \cdot V^T = I_{n \times n}$, where $I_{m \times m}$ and $I_{n \times n}$ are the identity matrices.

The Properties of the SVD Transform

The large utilization of the SVD transform in many applications is due to its powerful properties. Next, we summarize these characteristics, which are both related to algebraic and geometric aspects as follows (Trefethen & David, 1997):

- **Existence and Uniqueness.** Every matrix A , with real or complex values, has a singular value decomposition. If A is a square matrix and its singular values are distinct, than the left and right singular vectors are determined uniquely up to the sign, i.e., a coordinate reflection of each set of singular vectors (Bro, Acar & Kolda, 2008).
- **Energy.** The largest singular value is related to the spectral norm of the matrix A , i.e., $\sigma_1 = \|A\|_2$, while the square root of the sum of its squared SVs is equal to the Frobenius norm, i.e., $\|A\|_F = \left(\sum_{i=1}^p \sigma_i^2 \right)^{1/2}$.
- **Stability.** The SVs have a strong stability since the variation of both original and disturbed SVs can not exceed the 2-norm of the difference between the original A and modified C matrices, i.e., $|\sigma_i - \pi_i| \leq \|A - C\|_2$ where σ_i and π_i are the SVs of the matrices A and C respectively.
- **Low-rank approximation.** The rank r of the matrix A is equal to the number of its non-zero singular values. From (2) we can observe that the matrix A is decomposed

into p rank-one matrices (i.e., $\sigma_i u_i v_i^T$ with $i=1\dots,p$). Each of these matrices represents an energy level, which is induced by its corresponding SV. Supported by this observation, it is possible to neglect several insignificant energy levels obtaining an approximation of the matrix A . Moreover, to obtain the best approximation of the matrix A of rank r it is necessary to meet the following condition:

$$\|A - A_\gamma\|_2 = \sigma_{\gamma+1}, \text{ where } A_\gamma = \sum_{i=1}^{\gamma} \sigma_i u_i v_i^T, \\ \text{and } 0 \leq \gamma \leq r-1 \quad (3)$$

- **Link between SVD and eigenvalues decomposition.** To calculate the SVD we need to compute the eigenvalues and eigenvectors of $A \cdot A^T$ and $A^T \cdot A$. The eigenvectors of $A \cdot A^T$ form the columns of U , whilst the eigenvectors of $A^T \cdot A$ form the columns of V . Moreover, the singular values (SVs) in S are the square roots of the eigenvalues of $A^T \cdot A$ or $A \cdot A^T$.
- **Invariance to geometric distortions.** According to (Zhou & Chen, 2004), the geometric invariance can be expressed in the following way:
 - **Rotation invariance:** both the matrix A and its rotated counterpart A^r have the same singular values.
 - **Translation invariance:** both the matrix A and its translated counterpart A^t have the same singular values.
 - **Scaling invariance:** if A_{mn} has the singular values s_i , $1 \leq i \leq p$, then its scaled counterpart A^s has the singular values equal to $s_i \sqrt{F_r F_c}$ where F_r and F_c are the scaling factors of rows and columns respectively. In case the scaling function affects only the

rows or the columns, A^s has the singular values equal to $s_i \sqrt{F_r}$ or $s_i \sqrt{F_c}$ respectively.

- **Flip invariance:** Both the matrix A and its flipped counterparts (i.e., flip over horizontal or vertical axis) have the same singular values.
- **Transposition:** Both the matrix A and its transpose A^T have the same singular values.

In case of a specific multimedia content, e.g., an image, these properties can be interpreted in a particular manner, revealing new important implications. Thereby, depending on their energy distribution, the SVs together with their associated singular vectors can be split in three bands: low, medium and high. The *low band* contains the first most significant singular values and their associated left and right singular vectors, in which the most of the image information is concentrated. Generally, modifications of SVs of this band cause visible changes in the image. Instead, alterations of the singular values and vectors of the *medium* and *high bands* are considered less influent, since these bands only give a substantial contribution in images with random texture (Liu, Niu & Kong, 2006) (see Figure 2).

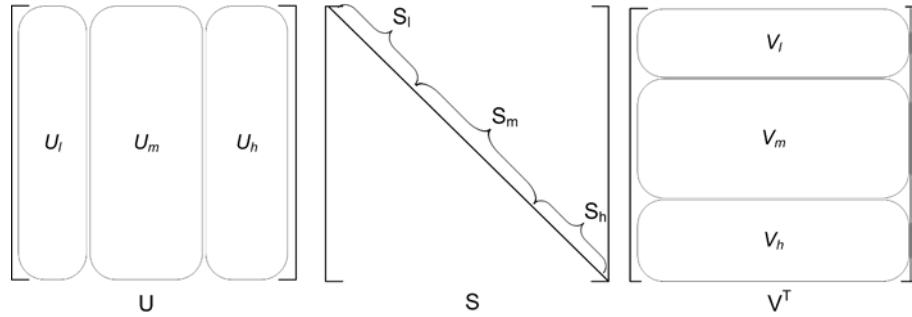
Furthermore, an alternative way of defining the matrix A_{mn} is as a sum of block matrices as can be seen in the relation below:

$$A = U_l S_l V_l^T + U_m S_m V_m^T + U_h S_h V_h^T \quad (4)$$

where $\{U_p, S_p, V_p\}$, $\{U_m, S_m, V_m\}$ and $\{U_h, S_h, V_h\}$ are the sets of singular values and vectors corresponding to the low, medium and high bands, respectively.

Another important observation is the relation between the features of the SVD (i.e, the singular values and vectors) and the characteristics of the image. Modifying the magnitude of the singular

Figure 2. Block partitions of the decomposition matrices depending on the energy distribution



values will affect the image luminance. The underlying structure of the image depends upon the orthogonal matrices U and V representing the *horizontal* and *vertical details* of the image respectively (Gorodetski, Popyack, Samoilov & Skormin, 2001). Thus, the decomposition of the matrix A has an important meaning: each SV represents the weight for each pair of left and right singular vectors. Hence, this creates different image layers where the first one i.e., $\sigma_1 u_1 v_1^T$, represents the image profile. This underlying layer concentrates a significant amount of image energy (Wu, 2005). Consequently, singular vectors corresponding to the largest SV's represent the shape (i.e., strong edges) of the image, while the rest of the singular vectors express weak edges and texture regions. Due to these properties, the SVD has been used (also combined with other techniques) for devising robust data hiding schemes.

APPLICATION OF THE SVD TRANSFORM

Steganographic and watermarking techniques may be applied to different kinds of media. Nowadays the most common digital objects used to convey secret data are images and audio/video streams.

Another possibility to classify steganographic techniques is to divide them in private schemes, which use the same stego-key during the hiding

and the revealing processes, and public techniques, which involve two different keys. In the second case, the first key is public and is used in the embedding process whereas the second one is secret and is needed during the extraction process.

Instead, watermarking schemes can be classified, in the following classes according to the amount of information necessary in the recovery process: *non-blind techniques*, which require, during the retrieval process, the original media or some other information derived from it and *blind schemes*, which do not use any data linked to the original media. A different scheme class, called *semi-blind*, can be identified when only the watermark is used in the extraction.

In addition, depending on the type of application to which a watermarking scheme is applied, digital watermarks can be subdivided in *robust watermarks*, *semi-fragile watermarks* and *fragile watermarks*. *Robust watermarks* are devised to resist against “non-destructive” manipulations of the media or against a reasonable amount of time spent to remove them. Both these requirements, together with the fidelity of the watermarked media, change drastically the entire design of the watermarking schemes. On the other hand, *fragile watermarks* are designed to fail when the media is inadequately tampered while *semi-fragile* watermarks can survive to some image processing operations which do not change the meaning of the media. Both watermarks are intended for

integrity verification (authentication) of digital media and, in addition, they must be capable to detect and localize content's modifications.

Depending on how the cover media is modified during the insertion process data hiding techniques can be splitted into:

- Methods working in the *spatial domain*, that insert the secret message by modifying or replacing redundant components of the cover media. The main issue of these methods is due to weakness against small cover modification.
- Schemes operating in a *transform domain*, which represent the original content in a transformed domain where the embedding is performed. It is worthwhile to point out that these schemes are more robust against a wide range of signal processing operations than those in the spatial domain, since the secret messages are embedded in significant areas of the cover signal. Common examples are schemes based on the *frequency domain*, such as the Discrete Cosine Transform (DCT), the Discrete Fourier Transform (DFT) and the Discrete Wavelet Transform (DWT) or schemes based on the Singular Value Decomposition (SVD).

In the following sections, we focalize on steganography and digital watermarking techniques which work in the SVD transform domain. Furthermore, a taxonomy of the applications based on SVD in the context of data hiding is given. This classification takes in consideration the way the secret information is bonded to different features of the transformed content through the data hiding process and can be summarized as follows:

- Data hiding algorithms which embed the secret information into the *singular values* (SVs) of the cover signal.

- Data hiding algorithms which insert the secret information by modifying the *right/left singular vectors* of the cover signal.
- Data hiding methods that combine all features of the SVD transform (*singular vectors and values*) with other well-known transforms (e.g., DCT, DWT, Zernike Moments Transform, Hadamard Transform and Karhunen–Loëve Transform).

This taxonomy mainly focuses on the *embedding process* since the way of defining it has a crucial effect on watermark properties, e.g., imperceptibility and robustness. To complete their characterization we further divide them depending on the extraction method, e.g., blind, semi-blind and non-blind (Cox, Miller & Bloom, 1997). Hence, the description of the schemes based on SVD is organized on a three-layer architecture, i.e., *information hiding*, *embedding procedure* and *extraction type* levels (see Figure 3).

All the requirements, design issues and performances related to current data hiding techniques are discussed. Table 1 depicts the main variables, together with their meaning, used in the forthcoming sections on digital watermarking only.

Using Singular Values Only

In this case, the generic embedding process uses the SVs of the digital object to convey the secret message. In earlier schemes, the SVs of the message were added directly to the SVs of the content or to its blocks. Due to many drawbacks, recent schemes avoid to employ the SVD transform over the secret message while choosing to insert directly its bits into the SVs of the digital object.

Steganographic Techniques

During the last years few steganographic schemes based on SVD have been proposed, all using an image as the cover object. The wide utilization of images for steganography can be partly justified

Figure 3. Three-level organization of the data hiding techniques based on SVD

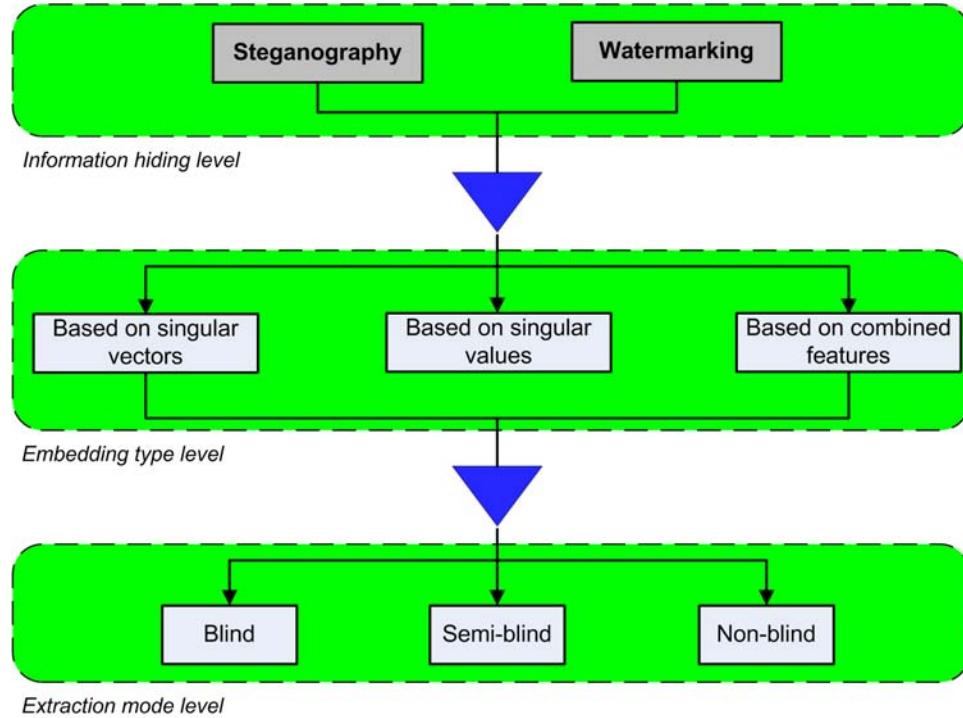


Table 1. Variable notations used for digital watermarking schemes only

Variable	Meaning
I, I_w, I_m	Original, Watermarked and stego image, video or audio signal
I_{wn}	Distorted (attacked) watermarked image, video or audio signal
I_f	Fake original image, video or audio signal
W	Owner watermark, which could be an image or a pseudo-random sequence
W_R, W_E, W_F	Reference, Extracted and Fake watermark
$[U_M, S_M, V_M]$	Singular value decomposition of M , where M could be I, I_w, I_{wn} , etc.
$\sigma_i^M, \sigma_{ij}^M$	i -th SV of M or of j -th block of M , where M could be I, I_w, I_{wn}, W, W_R etc.
y_i	i -th value (or bit) of Y , where Y could be W, W_R, W_E or W_F
α	Strength factor of W

by the following reasons (Bergman & Davidson, 2005):

- Images contain a lot of redundant data; thus, by replacing part of the data, it is possible to embed large messages without affecting the quality of the image.

- The process of identifying the modified images is hampered by the large amount of images over the Internet. Instead, it is well-known that video and audio contents are much more analyzed to detect any copyright infringements.

Blind Schemes

Among blind schemes, the most representative one was proposed by Gorodetski et al. in 2001. It was the first scheme which revealed the possibility of using the SVD transform for data hiding. In their paper the authors proposed two techniques which exploit the main properties of the SVD, i.e., the singular values representing the image luminance and the singular vectors representing the image geometry. In both of these techniques, the cover object is a color image represented in RGB format while the secret message is a gray-scale image. Due to space limitation, prior to insertion, the secret image is preprocessed by a lossy compression method which is derived from (Gorodetski, Skormin & Popyack, 2000). In the first method, the cover image is decomposed in three color layers (Red, Green and Blue) and each layer is segmented into non-overlapping blocks of fixed size. Next, each block is transformed using SVD and the largest SV is quantized in order to embed one bit of data. The experimental results show that the method is only robust against JPEG compression with quality factor 100% and that the embedding capacity is sufficiently high. However, modifying the first SV may diminish the quality of the stego-image.

The second method is also block-based, the only difference with respect to the first one consists in the quantization of the Frobenius norm of each block in order to embed one bit of data. This scheme shows a better robustness against JPEG compression. A detailed simulation of this method, performed by varying the block-size, quantization step and the degree of JPEG compression, revealed that the stability of the SVs is directly proportional to the block size, i.e., increasing the block size improves the robustness against JPEG compression (Gorodetski, & Samoilov, 2003). On the other hand, the authors proposed several solutions in order to embed larger messages: firstly, to reduce its size via compression and secondly, to split it into several parts and to send it using multiple cover images. In addition, both schemes

do not use the cover image for the recovery of the secret message and can be easily extended to the copyright context. Due to these facts, the approach proposed in this pioneering paper gave birth to many robust watermarking schemes.

In (Babu et al., 2007) the main characteristics of the steganography techniques e.g., the perceptibility, the robustness and the security, are discussed. Their scheme is very similar to the Gorodetski's approach, proposing only minor changes to the base line, with focus on:

- **Increasing the capacity** by processing the secret message, prior to its insertion, using JPEG compression instead of SVD compression.
- **Increasing the perceptibility** by inserting one bit of data in the largest SV or in other nonzero SVs of each block of the cover image. Therefore, in some cases the largest singular value of the blocks is left apart being not involved in the embedding and detection process. However, it is unclear under which conditions the message bit can be embedded in the non-zero SVs, different from the largest SV.

Semi-Blind Schemes

In the mid-90s, Yang and Lu (1995) developed a new image compression technique based on SVD. Wishing to improve the compression ratio and to reduce the amount of complexity needed to compute the SVD transform, they combined an incremental procedure aiming to compute the transform components with the vector quantization technique. This approach started some interest in the area of data hiding and its first utilization appeared in the Chung, Shen and Chang (2001) scheme. To be able to conceal the secret information, i.e., a gray-scale image, into the cover image, first the images are split into non-overlapping blocks and the Yang's SVD compression procedure is applied to each block. Then, some SVD components of the cover image (the SVs and

their related singular vectors) are replaced with those of the secret image. Very likely, combining the first SVs of the cover image with those of the secret image produces a set of SVs which is not ordered. Thus, to restore the decreasing order, the SVs of each block of the secret image are quantized while the block's SVs of the cover image are rounded-off. Note that without downscaling the SVs of the secret image its visibility cannot be avoided, compromising the entire scheme. Applying the following algorithm to all blocks generates the stego-image. The proposed scheme has a high capacity, but its portability is reduced by the necessity to have the compression codebook on both the embedding and the extraction sides.

Watermarking Techniques

The limited number of steganography schemes based on SVD is fully compensated by the proliferation of many watermarking schemes whose central element is the Singular Value Decomposition. One of the schemes which aroused many debates over the last years was suggested by Liu and Tan (2002) with the aim of protecting the rightful ownership. The original signal is a gray-scale image whilst the watermark can be a pseudo-random sequence or a meaningful message (e.g., a gray-scale image). Unlike the scheme proposed by Gorodetski et al. (2001), in this case the SVD transform is performed on the *whole image* I and produces three matrices: U_I , S_I and V_I^T . In the embedding process, the watermarked image I_W is obtained according to the following steps:

- The matrix S_I and the watermark image W are combined to obtain the reference watermark, W_R , which is further transformed using SVD:

$$W_R = S_I + \alpha \cdot W$$

$$SVD(W_R) = [U_{W_R}, S_{W_R}, V_{W_R}] \quad (5)$$

where α is the strength factor of W .

- The watermarked image I_W is obtained by multiplying the SVs of W_R with the left and right singular vectors of I :

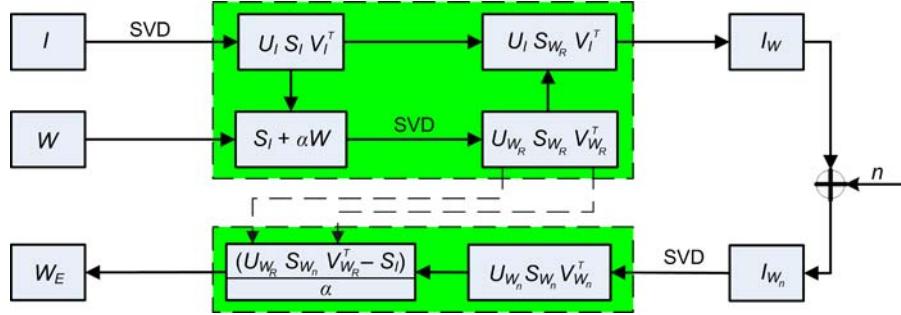
$$I_W = U_I S_{W_R} V_I^T. \quad (6)$$

The extraction process performs the following steps: the input image, possibly modified due to noise or other perturbations, is decomposed via SVD and its SVs, S_{W_R} , along with the singular vectors of W_R are combined to form an intermediary matrix, i.e., $U_{W_R} S_{W_R} V_{W_R}^T$. Finally, to obtain the extracted watermark W_E , the SVs of I are subtracted from the intermediary matrix and divided by α . A block diagram of the watermarking algorithm is given in Figure 4.

Regarding this scheme, the following considerations deserve attention:

- It was observed that the spectral norm of the watermark influences the quality of the watermarked image. Hence, the candidate watermarks must have the spectral norm as small as possible. Comparison between two types of watermarks, one a matrix with random elements while the other a gray-scale image, revealed that the random watermark achieved a smaller spectral norm. In addition, if the watermark to be embedded is a gray-scale image, first it should be preprocessed by randomization in order to reduce its spectral norm (Liu & Tan, 2002). However, since the original image is not splitted before applying the SVD transform, the modification of the SVs of I can greatly affect the quality of I_W .
- The reference watermark W_R is almost a diagonal matrix, as can be seen from the following equation:

Figure 4. Illustration of the Liu and Tan (2002) scheme. The black dashed upper and lower rectangles represent the embedding and extraction processes, respectively.



$$W_R = S_I + \alpha \cdot W = \begin{cases} \sigma_i^I + \alpha \cdot w_i, & \text{for the diagonal elements} \\ \alpha \cdot w_i, & \text{otherwise} \end{cases} \quad (7)$$

where w_i are the components of the watermark and σ_i^I are the SVs of the original image. Since the values w_i are small, multiplication with the strength factor $\alpha < 1$ will further reduce their magnitude. Instead, the additions of σ_i^I greatly increase the diagonal elements of W . Hence, the scheme applies the SVD on both the whole original image and on W_R (that greatly resembles a diagonal matrix).

- During the embedding process only the SVs of W_R are inserted while in the extraction phase, to recover the watermark, the singular vector matrices of the reference watermark are needed. This extraction mechanism leads to the *false positive problem*, which is an erroneously detection of a watermark in a signal which actually does not contain it (Cox, Miller & Bloom, 2000; Zhang & Li, 2005). Instead, an *ambiguous situation* may occur when a specific watermark is detected from a content in which a different watermark was embedded (Ting, 2006). Specifically, by joining the singular vectors of any fake watermark W_F with

the perturbed SVs, S_{W_n} , W_F is obtained since the SVs merely represent a magnitude factor for the corresponding singular vectors which store most of the watermark information. Due to these considerations, the majority of the schemes which insert the SVs of W into the SVs of I can not resolve the rightful ownership problem (Mohammad, Al-Haj & Shalaf, 2008).

- As a consequence, the high robustness manifested by the proposed scheme is due to the use of the matrices U_W and V_W which makes possible the extraction of W even after the original image is heavily damaged.
- The extraction process is semi-blind since the watermark recovery requires three extra matrices, i.e., the matrix S_I and the singular vectors of W_R . Moreover, due to the subtraction of S_I in the last step of the extraction process a diagonal line which crosses the entire extracted watermark shows up. If the extracted watermark is a pseudo-random sequence, it is difficult to observe this line since no visual inspection is needed to evaluate W_E . However, in case of meaningful watermarks this behavior can be clearly distinguished. This specific pattern occurs in all schemes which relay on this approach.

- The application of the SVD transform twice increases the complexity and the execution time of the algorithm.

Non-Blind Schemes

A similar scheme was proposed in (Mohammad, Al-Haj & Shaltaf, 2008), which embeds only one bit of data in all SVs of each image block. The following relation gives the embedding rule:

$$\sigma_j^{I_w} = \sigma_j^I (1 + \alpha \cdot w_i), \text{ with } w_i = \{1, 0\} \quad (8)$$

where σ_j^I are the SVs of the j -th block of I and w_i is the i -th bit of W . The scheme requires the original image during extraction. In addition, to prove its performance the algorithm was compared with two schemes: one based on DCT transform (Cox, Kilian, Leighton & Shamoon, 1997) while the other based on DWT-SVD (Bao & Ma, 2005), showing better results. To enhance its security, the proposed algorithm can be extended with quantization and cryptographic techniques. Although the algorithm extracts a meaningful watermark, the robustness of the scheme can be hardly assessed by visually inspecting the recovered watermark. Moreover, a viable explanation to the fact that the extracted watermark contains also the original image is not given.

In the same paper, a variation of the Liu's scheme is also proposed. However, differently from the original scheme, I is segmented in fixed blocks and one bit of the watermark is inserted in each of them. In contrast with previous algorithms, this scheme embeds and extracts the *entire watermark* and not the SVs of the reference watermark. By using this approach, the ambiguity problem is completely resolved, but the robustness is considerably decreased since the algorithm cannot resist against attacks even if the original image is used in the detection process.

Instead, Jain, Arora and Panigrahi (2008) proposed a watermarking scheme which inserts

the principal components of W , i.e., $U_W S_W$, into the SVs of the original image. Thus, the reference watermark is:

$$W_R = S_I + \alpha U_W S_W. \quad (9)$$

Next, the watermarked image is obtained as follows:

$$I_W = U_I W_R V_I^T = I + \alpha U_I U_W S_W V_I^T \quad (10)$$

where W_R is a dense matrix. Note that the SVD transform is no more applied over W_R which, in this case, is entirely inserted into I . Due to this fact, the original image is required during the extraction process. The authors state that by using this approach and keeping private the orthogonal matrix V_W during the extraction process the false positive problem is resolved. Nevertheless, no experimental results are carried out to asses the robustness of the scheme against common attacks.

Rezazadeh and Yazdi (2006) proposed a non-blind scheme based on SVD and texture segmentation. Differently from other schemes, they embed a pseudo-random sequence with zero mean and unitary variance as W . Prior to embedding, I is preprocessed by means of an entropy masking model which aims to localize the highly textured regions of the image. Hence, the local properties of the image and the characteristics of the human visual system are considered. Further, I is split into non-overlapping blocks and several blocks are selected, using a secret key, for watermark insertion. On each selected block the SVD transform is applied followed by the insertion of one bit data into the largest SV of the j -th block, using the following relation:

$$\sigma_{1j}^{I_w} = \sigma_{1j}^I (1 + \alpha D_j w_i), \text{ with } D_j = \{6, \dots, 14\} \quad (11)$$

where $\sigma_{1j}^{I_w}$ is the largest SV of the j -block of I_w and D_j is the related distortion level which depends on the entropy masking model. The scheme was tested against several common attacks, e.g., addition of Gaussian noise, median filtering, JPEG compression, scaling and sharpening, and compared with the scheme proposed by Xia, Boncelet and Arce (1998), showing good robustness.

A novel non-blind MPEG video watermarking scheme based on tensor SVD was introduced in (Abdallah, Hamza & Bhattacharya, 2007). Wishing to improve the robustness, the proposed scheme hides the watermark only in the I-frames. In contrast with previous schemes, this approach joins several I-frames of each scene of the original video sequence to form a 3D tensor. Two dimensions of the tensor represent the space while the other dimension expresses the time. Then every watermark's SV is inserted into the largest SV of each 3D scene tensor using the following relation:

$$\sigma_1^{I_w} = \sigma_1^I + \alpha \sigma_i^W. \quad (12)$$

The experimental results prove the robustness of the proposed scheme against common and geometrical attacks. However, the utilization of a multidimensional SVD during the watermarking process significantly increases the overall complexity of the scheme. Moreover, the proposed scheme is unable to prove the ownership due to the faulty reconstruction of the extracted watermark.

Semi-Blind Schemes

Recently several algorithms have been developed based on Liu's scheme (Liu & Tan, 2002). For example, the scheme proposed in (Ghazy et al., 2007) splits I into blocks and embeds W in each of them. Since the embedding/extraction are similar to those of the Liu's scheme, this algorithm is also affected by the false positive problem. Instead, in the paper (Aslantas, 2009a), the author focused on achieving high robustness without losing the watermark invisibility. To realize this compromise, he

presents a scheme which uses a genetic algorithm to compute multiple strength factors for the SVs of the original image. However, the core of the technique (embedding and extraction) is based on (Liu & Tan, 2002). Therefore, the watermarking technique cannot be used in practical applications (Xing & Tan, 2008).

In (Chandra, 2002), Chandra proposed two watermarking schemes. In the first one, the SVs of W are added to the SVs of I . The modified SVs together with the singular vectors of the original image are joined to obtain the watermarked image. Alternatively, the second scheme is block-based and to enhance its security the watermark is pre-processed by randomization, before insertion. During the embedding process, each bit of the randomized watermark is added to the largest SVs of the block using the following relation:

$$\sigma_{1j}^{I_w} = \sigma_{1j}^I + \alpha w_i \quad (13)$$

where $\sigma_{1j}^{I_w}$ is the modified SV of the block j , σ_{1j}^I is the largest SV of the image block j , w_i is the i -th bit of W and α is the strength factor.

Ganic, Zubair and Eskicioglu, proposed an optimal watermarking method that joins the Chandra's (2002) schemes. The watermark (a gray-scale image) is embedded twice in the host image. First, a block-based SVD transform (layer 1) is applied to I while a whole SVD transform is performed on W . The order of the SVs of W is randomized and each of them is added to the largest SV of each image block in the following way:

$$\sigma_{1j}^{I_w} = \sigma_{1j}^I + \alpha_j \sigma_i^W \quad (14)$$

where α_j is a variable strength factor. Afterwards, a global SVD (layer 2) is performed and the SVs of the watermark are added to those of the host image as in the previous scheme. Thus, for the layer 1 we have a localized embedding whereas for the layer 2 we have a global embedding (Ganic,

Zubair & Eskicioglu, 2003). For both layers the SVs of the each block and those of the whole image are necessary to obtain the watermark. To be suitable for copyright protection and to provide good robustness against signal processing operations the proposed scheme requires a large amount of information to be kept secret.

Another double watermarking scheme, which combines the spread spectrum (SS) and singular value decomposition (SVD) techniques, is introduced in (Bahandri, Mitra & Jadhav, 2005). The key idea behind this combination resides in their complementary behavior against attacks. Thus, the weaknesses of the SS technique could be successfully compensated by the strengths of SVD. In comparison with the previous scheme, the binary watermark W is embedded twice using different approaches: firstly W is modulated by using a pseudo-noise sequence and added directly to the image pixel values; in the second phase, similar to previous schemes, the re-watermarked image is obtained by adding the SVs of W to the SVs of the image resulting from the first step. However, the scheme fails to accomplish its primary goal, i.e., the copyright protection, due to its incapacity to recover unambiguously the second watermark inserted through a flawed SVD approach.

To enhance the security of the embedded watermark, several schemes propose to process in advance the original image and the watermark. The purpose of this treatment is to change their semantic structure using cryptographic techniques, such that even if they are detected it is infeasible to reveal their meaning. In (Shieh, Lou & Chang, 2005), a watermarking scheme is proposed which first randomizes W and I by means of a *chaotic mixing*; then applies on both the randomized images a block-based SVD transform and interchanges the SVs of the randomized W with those of the randomized image. The method preserves the quality of the original image and experimental results show good robustness to common and geometric attacks. However, recently it was pointed out that this scheme cannot be considered

a watermarking scheme since it does not produce a watermarked image which can be made public. Thus, the scheme is non-blind and cannot be used to proof the ownership since it suffers of the same fundamental flaw which characterizes the Liu and Tan (2002) scheme (Ting, Goi & Heng, 2009).

Instead, in (Gao, Dong & Zhou, 2006; Xing & Tan, 2007) the preprocessing mechanism used to scramble the watermark was the Arnold transformation, also called “cat face” mapping. Every pixel of W at the location (x,y) is transformed using the following relation:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \quad (15)$$

where (x',y') is the position of the transformed pixel and N represents the size of W . Since W is an RGB color image the Arnold transformation is applied to every pixel in each channel. The original image, which is also a color image, undergoes different modifications. First, I is decomposed in three channels. Next, each channel is divided into non-overlapping blocks that are further processed by the SVD transform. Finally, every pixel in each channel of W is added to the largest SV of every block. Experimental simulations show that the scheme is only robust to common attacks, such as JPEG compression, Gaussian noise, low pass filtering and cropping.

In (Mohan, Srinivaskumar & Chatterji, 2008), the embedding space is chosen based on the Canny edge detector. Concretely, prior to embedding the watermark, the Canny edge detector algorithm is employed on the whole cover image. Then, the resulting image is segmented in non-overlapping blocks which are classified according to their complexity, e.g., number of edges within a block. The first singular values of the most complex blocks are quantized in order to insert W , which is a binary image. The scheme is semi-blind since a quantization table, which contains the largest SV of each block of I , is used in the extraction.

The proposed technique is shown to resist rotation and content-preserving operations and, at the same time, being superior to (Chang, Tsai and Lin, 2005).

In a follow-up paper, the authors of (Mohan & Kumar, 2008) proposed a hybrid block-based watermarking scheme which uses both the features of the singular value decomposition, i.e., singular values and vectors. Briefly, I is segmented in four non-overlapping blocks and W , a binary image, is embedded twice: first, in the upper-left block using the approach presented in (Mohan, Srinivaskumar & Chatterji, 2008), and second, in the left singular vectors of the bottom-right block, by using the method introduced by Chung et al. (2007). To improve the security of the scheme, the watermark is formatted (randomized) by means of a secret key prior to embedding. The scheme is robust against common and geometric attacks. However, by modifying only the upper-left and bottom-right blocks of the cover image different luminance levels may occur, that can be easily detected in I_w . In addition, the first copy of W is successfully extracted from the largest SVs of the upper-left block while the other copy is rarely recovered. Hence, this algorithm does not bring any noticeable contribution regarding the robustness in comparison to the previous scheme (Mohan, Srinivaskumar & Chatterji, 2008).

Similar to the second approach introduced by Chandra (2002), a semi-blind SVD-based algorithm is presented in (Calagna, Guo, Mancini & Jajodia, 2006). The SVD transform is applied to image blocks and the watermark pixels are inserted into the most significant SVs of each block. This scheme does not present the weakness found in (Liu & Tan, 2002), and the simulation results, compared to the Cox watermarking method (Cox, Kilian, Leighton & Shamoon, 1996), demonstrate a greater robustness to common attacks; however, the quality of I_w is fairly low, i.e., 30 dB, and there is no evidence that the algorithm is also resistant to geometric distortions.

The same flawed approach proposed by Liu and Tan (2002) was extended in (Zude, Qingsong & Quan, 2006; Quan & Xiaomei, 2006) for watermarking 3D models. Even if it is applied to other types of digital content (i.e., a 3D object), the defective use of the SVD transform affects both watermarking schemes and, thus, they cannot be used for copyright protection applications.

Blind Schemes

For testing the presence of the watermark all the schemes outlined above depend on the original content or make use of some information derived from it (e.g., the singular values, codebook or quantization tables). Indeed, in some applications, e.g., transaction tracking, the owner which runs the extractor (detector) feeds it with both the original and suspicious content without endangering the security of the watermarking scheme. In addition, the use of the original content significantly increases the robustness of the overall scheme towards common and geometric distortions (Cox, Miller & Bloom, 2000). On the other hand, certain applications, like copyright protection or copy control, require an extraction without accessing the original content.

Among the proposed blind SVD-based watermarking schemes, the Li's scheme (Li, Wang, Song & Wen, 2005) is one of the earliest. In their algorithm, which exploits the properties of the SVD transform, the watermark is a logo image with the same size as I . To extract W without using I , the scheme applies the fast Independent Component Analysis (FastICA) algorithm which was initially introduced in (Hyvärinen & Oja, 1997). The embedding process is similar to the one proposed in (Liu & Tan, 2002). The major difference is related to how W_R is constructed, i.e., instead of adding W to the SVs of I , in the proposed scheme the watermark is added directly to the pixel values of I as follows:

$$W_R = I + \alpha \cdot W . \quad (16)$$

To extract the watermark using the FastICA algorithm three mixtures are built. The output of the FastICA algorithm gives the recovered watermark. However, the extraction is not blind since the singular vectors of W_R are used to build one of the mixtures. In addition, by analyzing the embedding process, we discovered an important issue for the proposed algorithm. More precisely, to reconstruct the watermarked image the following relation is used:

$$I_W = U_I \cdot S_{W_R} \cdot V_I^T \quad (17)$$

where U_I and V_I are composed by the left and right singular vector of I and S_{W_R} represents the SVs of W_R . Given that the watermarked image is public anyone can apply the SVD transform on it thus achieving the matrices U_I and V_I which contain most of the image information. Leaving these features unprotected, an attacker can take the SVs of any image and, together with the U_I and V_I matrices, reconstruct a fake original image, I_F . To check this issue, we performed the embedding process using the well-known “Lena” image as I and a binary image for W . Next, we constructed I_F by combining the singular vectors of I_W with different SVs of random images, taken from the UCID image dataset (Schaefer & Stich, 2004). As it was expected, the visual quality of I_F was good, reaching a PSNR value of 39 dB. Moreover, in all these cases W was completely erased from I_F . To proof the applicability of the proposed attack we present in Figure 5 the attacked Lena image (bottom right) along with the watermarked Lena image (top right) where the mark is the Swan image. The attack image (bottom left) from which we collect the SVs to carry out the attack was taken from the UCID image dataset.

Noting that the watermark insertion may modify the order of the singular values in the original image, Liu, Niu and Kong (2006) proposed an image watermarking scheme which preserves the order of the SVs. This order is extremely im-

portant since it allows to extract the watermark without using the original image (Liu, Niu & Kong, 2006). To achieve a good quality and robustness, the middle SVs of the image I are selected for embedding: the watermark bits are inserted into a pair of SVs if the gap between them exceeds a predefined threshold. Since it is possible to lose the decreasing order after embedding the watermark, the smallest unmarked SVs are changed with new values obtained by linear interpolation. The watermarked image I_W is obtained by combining the modified SVs with the U_I and V_I matrices. The algorithm is particularly robust to JPEG compression, filtering and rescaling, but is very weak against rotation or cropping. In addition, the payload is very low, since only 32 bits can be embedded in the cover image. However, the substitution attack can be mounted because the scheme uses the same method to reconstruct the I_W as the previous algorithm.

Using the same idea of maintaining the order of the SVs, Chang, Hu and Lin (2007) proposed a block-based watermarking scheme which does not require I or any side information to recover W . Prior to watermark insertion, I is segmented into non-overlapping blocks. Some blocks are selected for watermark embedding with the help of a secure pseudo-random generator. In addition, to increase the robustness, the watermark (a binary image) is redundantly inserted in the original image. In each selected block, the binary values of W are hidden by slightly modifying the 2nd and 3rd SVs using the following formulas:

$$\begin{aligned} \hat{\sigma}_3 &= \sigma_2^I \\ \hat{\sigma}_2 &= \sigma_2^I + \alpha \cdot w_i \end{aligned} \quad (18)$$

To recover W , the difference between the 2nd and 3rd SVs in each block of I_W is compared to a specified threshold Th . If the difference is above Th then the value of the extracted watermark bit is 1, otherwise 0. Experimental results show that the proposed scheme is robust against several

Figure 5. Illustration of the substitution attack



image processing operations. In (Chang, Lin & Hu, 2007) the same authors presented an image watermarking scheme which extends the previous approach with a small modification in the embedding and extraction processes. This modification aims to recover the watermark while giving the opportunity to restore the original image with high quality. Each watermark value is embedded by modifying the 2nd SV of I 's block while the additional information required to restore I are kept into the 4th SV of the block. However, quite recently two attacks have been devised which show that both schemes cannot be considered robust, being unable to resolve the rightful ownership problem. As pointed in (Ling, Phan & Heng, 2008), these attacks succeed because an attacker can easily modify the embedding space.

The approach originally introduced by Gorodetski, Popyack, Samoilov and Skormin (2001), i.e., quantization of the largest SVs, along with

the capacity of the SVs to detect any modification incurred upon the image, have been successfully employed to devise fragile and semi-fragile watermarking schemes. In general, to achieve the goal of detecting and localizing tampered regions, these schemes select certain features that are sensible to content modifications and insert them as a watermark in the protected image. Next, the semi-fragile and fragile watermarking schemes are discussed, highlighting their design and issues.

The first application of the SVD transform for image authentication comes from the semi-fragile scheme proposed by Sun, Sun and Yao (2002). Essentially, a block-wise SVD transform is applied on I and, afterwards, W is embedded into the largest SV of each block by quantization. Although the scheme is robust to common image processing operations, it is vulnerable to block substitution, vector quantization (VQ) and histogram analysis attacks (Lee, Jang & Yoo, 2005). The former at-

tack may be performed because the watermarked blocks can be easily interchanged by blocks with similar largest SV, without raising any suspicion during the authentication process (Wu, Yeh & Tsai, 2006). On the other hand, the VQ attack (Wong & Memon, 2000), also known as birthday attack (Barreto, Kim & Rijmen, 2002), aims to create a database of images watermarked using the same secret key k and watermark W from which a counterfeit image can be assembled. Differently from the previous attacks, the histogram analysis aims to disclose the secret parameters of the watermarking scheme, like the quantization step size, making the watermark useless. To overcome these issues, Lee, Jang and Yoo (2005) proposed several solutions:

- *Against VQ attack.* Prior to embedding, the original image should be divided into non-overlapping blocks and their order randomized using a secret key.
- *Against histogram analysis.* After each watermark bit is embedded in every block of the randomized image by quantizing the largest SV, such values should be further dithered using random values.

However, the proposed scheme is unable to detect the tamper in case of JPEG compression with quality factor 80. To detect this malicious attack the detection threshold should be lowered, but this spreads the localization error over the entire image (Lee, Jang & Yoo, 2005).

Instead, Wu, Yeh and Tsai (2006) proposed a semi-fragile SVD-based watermarking scheme in which the VQ compression technique is used to encode the selected image features. Like many other schemes, the SVD transform is performed on I in a block-wise manner. It is interesting to outline the solution adopted to defeat the block substitution attack: the image features, which have the role to act as W , are obtained from the first left and the first right singular vectors of the block. Indeed, the most of the block's informa-

tion is stored in this first image layer which is determined by the largest SV and the first right and left singular vectors of each image block. Then, the attempt to substitute two blocks with similar SVs is prevented since the first right and left singular vectors of the blocks is considerably different. The image features are further used to generate the compression codebook necessary during the embedding and extraction processes. To obtain the watermarked image, the corresponding index of each feature in the codebook is buried into the largest SV of the block by quantization. The codebook and the selected features are then adjusted to enhance the robustness of the scheme. The main drawback of the scheme consists in the generation and utilization of the codebook which highly increases its load. In addition, the quality of the watermarked images is very low, e.g., 27.8 dB for the “Baboon” image while 30.4 dB for the “Lena” image. It is very likely that this low quality is caused by the abnormal reconstruction of I_W in which the U , and V , matrices are no longer orthogonal due to their adjustment.

A further semi-fragile authentication scheme for RGB color images has been proposed by Lu, Chang and Liu (2006). The image feature set F is selected from the green channel, which is first split into non-overlapping blocks of fixed size. To prevent the VQ attack, each image block is unambiguously identified by a combination of three features. The first feature is given by the largest SV of the block while the others represent the sum of the x and y coordinates of each pixel block. After collecting the features, they are inserted in every channel of the image. The embedding procedure evolves by splitting the entire color space into separated blocks, followed by their decomposition using SVD. Finally, the features are hidden in the last three nonzero SVs of each block. During the insertion process the order of the SVs is preserved by modifying them with suitable weighting factors: this is done to recover the watermark without questioning the original image. Experimental tests prove that the

scheme can detect and resist to intentional and common processing operations. To improve the performance of the scheme against geometrical distortions, the authors suggest a correction process which allows to better distinguish between tampered and non-tampered blocks. However, if the block's matrix has an insufficient number of non-zero SVs, i.e., less than five, then the insertion process cannot proceed since the first feature of the block cannot be computed.

The first SVD-based fragile watermarking scheme was proposed by Byun, Lee, Tewfik and Ahn (2003) and uses the SVs of I as the authentication signature. The watermark insertion can be summarized as follows:

- *Embedding site selection.* A number of pixels are randomly selected from I through a secret key. Then, the LSB of the selected pixels is set to zero.
- *Feature selection.* Perform the SVD on the resulting image and for each SVs apply the following relations:

$$b_i = [\text{floor}(\alpha \sigma_i)] \mod 2 \quad (19)$$

where σ_i are the original SVs, α is a strength factor and b_i represents the bits of the authentication data.

- The authenticated watermarked image is formed by placing each bit of the authentication sequence into the LSB of the randomly selected pixels of I .

The extraction procedure is the reverse of the insertion procedure and permits to recover the authentication data without using I . To achieve the localization requirement, a binary watermark W is designed. Due to their smaller size, the watermark and the authentication data are tiled until they reach the size of I . Then, the XOR operation is used to combine W and the authentication data.

Finally, the resulting bits are inserted into the LSB of the randomly selected pixels. However, the modification of image pixels can change the SVs, which propagate the error through the entire watermark (Oktavia & Lee, 2004).

Recently, it was pointed out that badly choosing the strength factor of the watermark could create a security breach to the Byun, Lee, Tewfik and Ahn (2003) scheme. After deeply analyzing the Byun's scheme, Ting, Goi and Heng (2007) conclude that by significantly increasing the strength factor, increases the probability to guess the authentication sequence.

To overcome this issue, the scheme of Oktavia and Lee (2004) adapts the Byun, Lee, Tewfik and Ahn (2003) algorithm to be able to work with the segmented cover image and watermark. Besides this, the LSB of *all* the block's pixels are replaced by a random sequence generated through a secret key, and not set to zero as in (Byun, Lee, Tewfik & Ahn, 2003). Another difference is related to the authentication data, which before being XORed with the watermark is permuted by another secret key. Thus, the whole security of the scheme relays on the secret keys used during the embedding process. However, since this scheme processes one block at a time, a VQ attack can be mounted against it (Ting, Goi & Heng, 2007).

Another scheme derived from the Byun's algorithm was developed in (Ting, Goi & Heng, 2007). The main difference resides in the addition of an encryption step which produces the final watermark. This avoids the security issues found in the Byun's scheme and, in addition, protects the originator's rights. Furthermore, this approach can be easily adapted to other fragile watermarking schemes.

All previous authentication schemes use certain local or global image features gathered with the aid of the SVD transform as watermark. Instead, in (Li, Su, Li, Wang & Yao, 2008) the authentication data represents a chaotic sequence generated by means of a secret key. In the embedding process,

I is divided into blocks and each watermark bit is added to the largest SV of the blocks through quantization. The ability to adaptively modify the quantization interval increases the overall security and enhances the quality and robustness of the watermarked image.

Using Singular Vectors Only

All the previous data hiding schemes only focus on singular values, especially on those of the cover digital object. Thus, in the embedding process the secret message bits (or, in some cases, its SVs) are embedded into the SVs of the digital object. This fact is fully justified since the stability of SVs with respect to attacks is well known.

On the other hand, using the SVs during the insertion process drastically limits the watermark payload to the number of SVs. Due to this reason, the majority of the watermarking schemes moved from *Liu's global approach* (Liu & Tan, 2002) towards *Gorodetski's local approach*: this method splits the content into non-overlapping blocks before applying the SVD transform. However, even this solution was not enough to satisfy the need for larger payloads.

Recently, looking for a larger embedding space, some researchers started to investigate the singular vectors of the cover object. It has already been mentioned that the left and right singular vectors are orthonormal and they have small value components, between -1 and 1. In addition, most of the digital object information is "coded" in the first singular vectors. Until year 2005, nobody investigated if these features were able to convey secret information while the content is subject to attacks. Nevertheless, in the last years several data hiding schemes based on the singular vectors of the cover have emerged. The forthcoming sections present a detailed description of these schemes, together with the problems deriving from this approach.

Steganographic Techniques

Bergman and Davidson (2005) proposed the only steganographic algorithm that uses the singular vectors of the cover object to conceal private information. The secret message m is a bipolar signal, i.e., $m_i = \{+1, -1\}$, while the cover object could be a gray-scale or a color image. Before proceeding, the cover image I is splitted into non-overlapping blocks and each of them is SVD transformed. The key idea of the algorithm is to select certain left singular vectors and then to modify the sign of each of their components with the corresponding sign of the message bit. The following formula gives the embedding relation performed in each block of I :

$$\hat{u}_{I_m}(i, l) = m_i \cdot |u_I(i, l)| \quad (20)$$

where $\hat{u}_{I_m}(i, l)$ is the modified coefficient of the l -th left singular vector of the stego-image I_m , $|u_I(i, l)|$ is the absolute value of the original coefficient and m_i is the i -th bit of the secret message.

To preserve the quality of the stego-image I_m the singular vectors which correspond to the first SVs are left unchanged. In addition, in order to have a *normal* SVD (Bergman & Davidson, 2005) the elements of the first row of U_I are left apart from the embedding process. The orthonormality of the modified vectors is maintained by further modifying the remaining elements of the matrix U_I with the aid of a system of linear equations. After completing the embedding process, the resulting stego-image has a good visual quality. The security of the scheme could be increased by encrypting m with a stream cipher before its insertion. In the extraction process, the only thing needed to recover the watermark is to gather the sign of the left singular values of the distorted matrix. However, the major drawback of this resides in its unacceptable high bit error rate (BER). After intensive experiments, the authors state that this behavior is mainly influenced by

the segmentation size of I and by the number of untouched (“protected”) singular vectors. To lower the BER, three solutions are proposed:

- Spacing the SVs of the cover blocks, which can limit the variation of the corresponding singular vectors.
- Performing the embedding process several times.
- Using error-correcting codes, like the Bose Ray Chaudhuri (BCH) codes.

Nevertheless, uniformly modifying the SVs of the blocks could change their natural distribution, fact that can be easily exploited by an attacker. On the other hand, iterating the insertion algorithm several times increases the execution time of the entire embedding process.

In our opinion the failure of the scheme to recover the embedded bits is caused by the sign of the singular vectors which *is given randomly* during the decomposition procedure of the SVD transform (Bro, Acar & Kolda, 2008). Thus, it is not possible to hide any secret message in the *sign* of the singular vectors components since it is not a robust feature.

Watermarking Techniques

In the field of digital watermarking, Chang, Tsai and Lin (2005) proposed the first important algorithm based on singular vectors. The original I is gray-scale image whereas W is a binary image. The original image is split into non-overlapping blocks as the previous scheme. Using a PRNG the embedding blocks are randomly selected from those with the highest rank. Each of the embedding blocks is further decomposed with the SVD transform. The second and third coefficient of the first left singular vector are retained and used in the embedding process. The following magnitude relationship is used to insert the watermark bits:

$$\begin{cases} |u_I(2,1)| - |u_I(3,1)| \geq Th & \text{if } w_i = 1 \\ |u_I(3,1)| - |u_I(2,1)| > Th & \text{if } w_i = 0 \end{cases} \quad (21)$$

where w_i is the watermark bit, Th is a preset threshold and $|\cdot|$ the modulus operator. It is worthwhile to point out that unlike to (Bergman & Davidson, 2007), in this scheme the embedding approach does not preserve the orthonormality of the matrix U_I . From the experimental results, the proposed scheme appears to be robust against common signal processing operations. In the extraction, it is not necessary to use any information related to I . However, W cannot be extracted exactly even if the watermarked image did not suffer any attack (Mohan, Srinivaskumar & Chatterji, 2008). Another problem of this scheme is related to the selection of the embedding blocks: using the rank for the selection process is not advisable since it is not a reliable feature (Patra, Soh, Ang & Meher, 2006).

Several improvements of the embedding procedure were proposed in (Patra, Soh, Ang & Meher, 2006). They are mainly focused on the selection mechanism of the embedding locations while the modification of the selected coefficients remains unchanged. Thus, the rank-based block selection is abandoned and the embedding space is enlarged by using also the right singular vector in the embedding process. In addition, instead of using only the 2nd and 3rd coefficients of the first left and the first right singular vectors the scheme randomly selects two of them.

Important guidelines on how to modify the coefficients of the left and right singular vectors to increase the imperceptibility and capacity of the watermarking schemes are given in the short notes presented by Chung, Yang, Huang, Wu and Hsu (2007). These notes state that modifying the columns of the U_I and V_I matrices will cause less visible artifacts. Thus, inserting a watermark simultaneously in both the matrices U_I and V_I leads to an increased capacity while maintaining the quality of I_W . However, theoretical analysis and

experimental tests carried out by Fan, Wang and Li (2008) prove that only the components of the first column of the matrices U_I and V_I are robust to general image processing operations. Instead, the components of the other vectors change drastically when the image undergoes to small perturbations. Another important aspect discussed in (Fan, Wang & Li, 2008) is the compensation of distortions. By using the components of U_I to insert w_p , the corresponding components of V_I can be modified to adjust the level of distortion. In this way, the quality of the I_w image may be kept very high, i.e., 51.97 dB.

Note that the previous scheme could not preserve the orthonormality of the U_I and V_I matrices during the embedding process. We are not aware of any other watermarking techniques that preserve this important property, except for the recently approach proposed by Basso et al. (2009). The proposed scheme works by initially dividing I into non-overlapping blocks, applying the SVD transform to each of them and subsequently embedding each watermark value by modifying a set of singular vector angles, i.e., angles formed by the right singular vectors of each block. The main contribution of this work can be identified in an increased security of the watermarking scheme against ambiguity and block substitution attacks, due to the use of singular vectors in the embedding process rather than singular values.

In (Agarwal & Santhanam, 2008) a completely different approach is presented. Unlike other schemes, this one applies a global SVD transform on both I and W , and directly inserts V_W in the singular vectors of the original image, i.e., $V_{I_w} = V_I + \alpha V_W$. Using this approach, the resulting right singular vectors are not orthonormal and the quality of I_w is unacceptable (around 25 dB). In addition, to accomplish the extraction process the scheme needs the original image and the principal components of the watermark, i.e., $U_W S_W$.

Combining SVD with Other Transforms

SVD has been used also in combination with other transforms, like DCT, DWT, Zernike Moments and Karhunen–Loève Transform. As far as we know, there are no steganographic schemes that adopt such an approach.

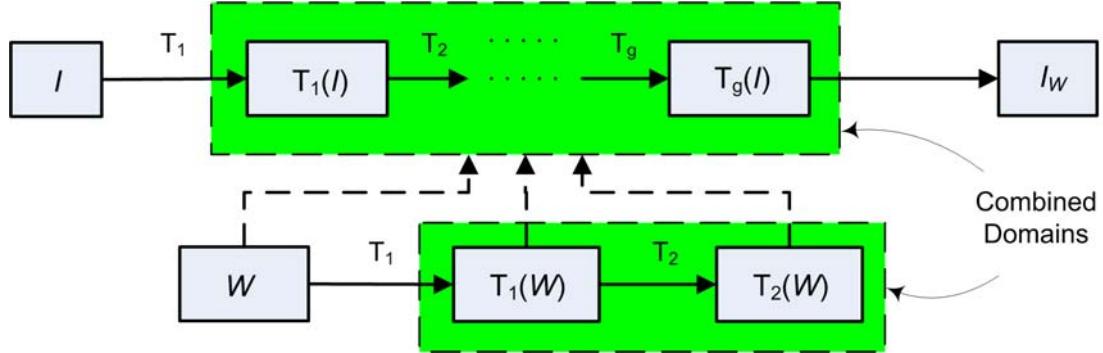
Watermarking Techniques

In general, the main goal of joining different transforms is to form a *combined domain* whose features are more powerful (stable) against attacks. The features of the combined domain are obtained by successively applying different transforms to the original content, i.e., the chain of transforms T_1, \dots, T_g . At each step, all (or certain) features of the previous transform are retained and further treated by the successive transform. Finally, the watermark bits (or its SVs) are embedded in the obtained features. An illustration of such an embedding process is given in Fig 6.

Depending when the SVD transform is employed in the chain, the following cases can be distinguished:

- *The SVD transform is applied in the initial stage.* This case, where the SVD is seen merely as a preprocessing operation to which the original image is subject to, rarely occurs (Tang, Yang, Li & Niu, 2004; Kaufman & Celenk, 2006) and provides poor performances, such as weak robustness against attacks, low quality for the watermarked image and high failure rate in the attack-free scenario.
- *The application of the SVD transform is in the final stage.* This is the most representative case, in which the watermark bits or its SVs are inserted into the SVs of the combined domain.

Figure 6. Embedding process in the combined domain



The watermark undergoes the same modifications, the only difference consisting in the application of fewer transformations, i.e., the G_1 and G_2 transforms in Fig 6. In general, the watermark is decomposed through the SVD transform. As far as we know, only in a single case (Sverdlov, Dexter & Eskicioglu, 2005) a sequence of two transforms is applied to the watermark.

Knowing the weakness of the SVD features to noise addition, combining them with transforms that have a complementary behavior can be successfully exploited to design robust watermarking schemes.

Non-Blind Schemes

In (Tang, Yang, Li & Niu, 2004), the Singular Value Decomposition is combined with KLT to embed a watermark into a set of features. The features are extracted from non-overlapping blocks of I by performing the KLT on the vector of SVs. The coefficients of the KLT are the features to which the watermark is added. The quality of the watermarked image is 19.2521 dB, which is not acceptable for all watermarking applications.

Quan and Qingsong (2004) proposed the first scheme of this kind, which successively applies the DCT and the SVD transforms to the original image. Rather than directly inserting the watermark into the pixels of I , the proposed algorithm embeds the SVs of W into the singular values of the middle frequency DCT coefficients. Instead,

in (Sverdlov, Dexter & Eskicioglu, 2005), the authors employ the DCT and the SVD transforms in cascade on both the original image and the watermark. In the embedding process, the SVs of both DCT domains are mixed together to obtain the watermarked image. For schemes that choose to embed the watermark into the features of the DCT-SVD domain, the robustness against common attacks is fully ensured.

Other schemes embed the watermark into the SVs of the DWT domain. After performing the DWT on I the four bands LL, HL, LH and LL are obtained. In this scenario, the watermark embedding locations are the SVs of all the frequency bands as in (Ganic & Eskicioglu, 2004). By applying this approach the transparency of the watermarked image is questionable, i.e., it can be easily seen that the watermarked image is much brighter than the original one. In addition, the ‘high robustness’ shown by the scheme towards common and geometric attacks is due to the fact that the embedded watermark can be extracted from *any* image. Recently, Aslantas (2009b) extends this scheme with a differential evolution algorithm, used to compute the optimal strength factors for the SVs. This adaptation strengthens the algorithm both in terms of transparency and robustness under attacks.

On the other hand, by performing recursively the DWT on the approximation band, i.e., LL, a multi-scale representation of I is obtained. This

approach is adopted in (Liu, Lin, Kuo & Chang, 2007; Lin, Liu & Han, 2008) which decompose the original image using a 3-level DWT and then the resulting subbands, i.e., LL_3 , LH_3 , HL_3 and HH_3 , are marked using two different approaches. The SVs of HL_3 and LH_3 are modified by the SVs of W while in LL_3 and HH_3 the watermark bits are inserted directly. From the experimental results, we notice that in most cases the algorithm is able to extract only the watermark from the HL_3 and LH_3 subbands. Thus, the robustness of the proposed scheme resides on this middle subbands watermark. Moreover, to retrieve the watermark, the extraction procedure needs a lot of auxiliary information, i.e., the original image, the marked versions of the HL_3 and LH_3 bands and W , overloading the whole scheme.

The main characteristic of the above schemes resides in the extraction process where the watermark is reconstructed using the U_w and V_w matrices, fact that creates the impression of high robustness against attacks. By using the singular vectors of the watermark in the extraction stage (which ‘helps’ to retrieve the mark even after I_w is heavily damaged) it is likely to extract the watermark even from images that do not contain it. Observing that this mode of extraction raises the ambiguity problem (Zhang & Li, 2005; Wu, 2005; Xiao, Wei & Ye, 2008), several schemes (Yavuz & Telatar, 2006; Yavuz & Telatar, 2007) proposed to embed also the singular vectors of the watermark as a control parameter. Yavuz and Telatar (2006) proposed the first scheme of this kind, which applies a block-DCT on I , followed by the insertion of S_w into the SVs of the approximation matrix, i.e., the matrix formed by collecting the DC coefficient of each block, and V_w into the AC coefficients. In the extraction, if the similarity between V_w and the right singular vectors of the extracted watermark exceeds a certain threshold, then the SVs of the watermark are extracted and used to reconstruct safely the watermark. Thus, by inserting V_w the algorithm is able to avoid the ambiguity problem. In (Yavuz & Telatar, 2007), the

same authors translate the approach to the DWT domain thereby inserting the SVs of W into the SVs of the LL and HH subbands and embedding the values of the control parameter, V_w , into the HL and LH subbands. Both schemes produce watermarked images of good quality, i.e., the PSNR is around 42 dB, and achieve the robustness requirement. It is important to note that for images similar to the cover image both schemes may fail in detecting the ambiguity problem (Mansouri, Aznaveh & Azar, 2008).

Semi-Blind Schemes

The majority of the algorithms in this category use the SVs of W and/or the SVs of I during the extraction process. Regarding the embedding process, the approaches proposed in (Liu & Tan, 2002; Chandra, 2002) are the most used, being extended to the DCT and the DWT domains.

For example, the Liu and Tan (2003) embedding algorithm is employed as a global approach on the LL band of the original image in (Shen, Zhang & Liu, 2006). Instead, in (Liu & Liu, 2008) it is applied on the DC approximation matrix obtained as in (Yavuz & Telatar, 2006), yielding to a local approach. However, the above schemes fail to achieve good results in terms of both imperceptibility (the watermarked images are of low quality) and robustness. Furthermore, the pattern that appears on the extracted watermarked (a common particularity for all schemes based on (Liu & Tan, 2002)) is present.

Ozer, Sankur and Memon (2005) proposed the only audio watermarking scheme based on SVD, adopting the same embedding procedure. In addition, since applying the SVD on a 1D signal produces only one SV, firstly the original signal is changed into a matrix by using the short-time Fourier transform prior to insertion. A detailed analysis of the embedding process along with many possible variants can be found in (Kardamis, 2007). Detailed robustness and comparison tests are carried out to demonstrate its performance.

Instead, the Chandra (2002) approach, in which the SVs of W are embedded into the SVs of the transformed coefficients, is adopted in (Li, Yuan & Zhong, 2007; Bhatnagar & Raman, 2008a; Bhatnagar & Raman, 2008b). Concretely, the SVs of the watermark are inserted into the SVs of the wavelet subbands. The watermark strength factor is computed by taking into consideration the human perceptual system. Robustness to attacks and the large capacity are the main features of these schemes.

However, as has been mentioned by numerous authors (Engedy, Parasad & Saxena, 2006; Lamarche, Liu & Zhao, 2006; Yavuz & Telatar, 2007) the watermarking algorithms introduced in (Liu & Tan, 2002; Chandra, 2002) generate an ambiguous situation in the detection stage that invalidates the performance achieved, in terms of watermark robustness, transparency and capacity. As a consequence, the same flaw affects all the schemes derived from them.

Blind Schemes

In contrast with the previous techniques, blind schemes use *segmentation* and *quantization mechanisms* in the embedding process. The features to which the quantization mechanism applies are obtained by combining the SVD with well-known transforms, i.e., DWT (Al-Khatib, Al-Haj, Rajab & Mohammed, 2008; Bao & Ma, 2005; Kim, Lee, & Lee, 2007; Peng & Liu, 2006; Qi, Bialkowski & Brimley, 2008; Zhu & Liu, 2009), DCT (Tsai & Yang, 2007; Wang, Lu, & Sun, 2008; Wu, Kong, Yang & Niu, 2008) or ZMT (Li, Wang, Song & Wen, 2005).

The first embedding approach used for developing blind schemes splits the original image into non-overlapping blocks followed by the *quantization of the largest SVs* (Li, Wang, Song & Wen, 2005). In this case, the watermark bits are inserted into the first image layer of each block, i.e., the most significant components of the blocks. However, such an approach may affect the quality of the watermarked image. Due to this reason, in

(Bao & Ma, 2005; Peng & Liu, 2006; Tsai & Yang, 2007; Qi, Bialkowski & Brimley, 2008; Zhu & Liu, 2009) the watermark bits are scattered over the entire set of SVs of each block, improving the robustness and the quality for the watermarked image. These embedding methods, which apply segmentation followed by quantization of the largest SV (or of the whole SVs), were first introduced in (Gorodetski, Popyack, Samoilov & Skormin, 2001) and offer the most promising results in terms of robustness, transparency and security.

After partitioning the original content, in order to construct the embedding space for the watermark, the insertion process may continue through successive application of DCT and SVD transforms as in (Tsai & Yang, 2007), or of DWT and SVD transforms as in (Bao & Ma, 2005; Peng & Liu, 2006; Qi, Bialkowski & Brimley, 2008). In the case of wavelet transform, the watermark may be embedded through quantization of the SVs of all the four subbands (Bao & Ma, 2005) or just in some subbands, i.e., the approximation subband (Peng & Liu, 2006; Qi, Bialkowski & Brimley, 2008) or high frequency subbands (Al-Khatib, Al-Haj, Rajab & Mohammed, 2008). A particular scheme which applies three transforms, i.e., DWT, DCT and SVD, over the original image followed by quantization of the singular values is proposed in (Zhu & Liu, 2009).

The embedding mechanism proposed in (Kong, Yang, Wu & Niu, 2006; Liu, Niu & Kong, 2006) is employed in the singular value domain of the DCT low frequency coefficients for real-time video watermarking, and consists in the modification of the middle SVs while maintaining their order (Wu, Kong, Yang & Niu, 2008). Even if the algorithm is much faster and lighter than its previous version (Kong, Yang, Wu & Niu, 2006), it is not robust against adversaries that use the knowledge of the scheme to remove the mark. This is because the middle SVs, where the watermark is hidden, can be easily identified and modified, even if they are computed in a different domain, e.g., DCT or DWT.

A different approach for watermarking video streams was proposed in (Al-Khatib, Al-Haj, Rajab & Mohammed, 2008), where the watermark bits are inserted into the LSBs of the SVs of the DWT domain, i.e., the HL sub-band, of the original image. This method has affinity with the ones introduced in (Byun, Lee, Tewfik & Ahn, 2003; Rajab, Al-Khatib & Al-Haj, 2009), which were applied to devise several authentication schemes (Oktavia & Lee, 2004; Ting, Goi & Heng, 2007). The algorithm achieves the optimal trade-off between the quality of the watermarked image and the robustness towards standard attacks, such as compression, rotation, noise addition and frame dropping. However, knowing the fragility of the LSB toward attacks it is surprising the robustness expressed by this watermarking scheme.

Besides the construction of robust features by joining several transforms, many combined schemes started to focalize on other issues, from which we can mention:

- *Selection of the embedding locations.* The schemes which segment the cover image into non-overlapping blocks for enlarging the embedding space choose the blocks for embedding the watermark based on their statistic i.e., mean and variance, as in (Li, Wang, Song & Wen, 2005; Bhatnagar & Raman, 2008b). The main advantage of this approach is the quality of the watermarked image since the block's statistic is closely related to the human visual system. On the other hand, the security of the approach is weak since it enables an adversary to mount powerful statistic attacks. Recently, this common approach was replaced by a more secure selection mechanism which uses spatio-temporal chaos (Peng & Liu, 2006) or a hash function (Qi, Bialkowski & Brimley, 2008).
- *Randomization of the watermark.* To enhance the security of the scheme, the watermark is preprocessed before its insertion

by means of a Torus automorphism (Li, Wang, Song & Wen, 2005), spatio-temporal chaos (Peng & Liu, 2006) or successive packing interleaving (Qi, Bialkowski & Brimley, 2008).

- *Choosing optimal strength factors and adaptive quantization steps.* By choosing suitable strength factors and quantization steps, an optimal watermarking scheme can be devised which realizes the trade-off between the transparency of the watermark and its robustness. Thus, linear programming techniques (Haghghi & Ghaemmaghami, 2005) or micro-genetic algorithms (Lai, Huang & Tsai, 2008) are used within the SVD domain to obtain the optimal strength factors. Instead, to compute the adaptive quantization parameters in the combined domain several approaches have been adopted, such as statistical methods (Bao & Ma, 2005; Peng & Liu, 2006), grid search algorithms (Qi, Bialkowski & Brimley, 2008) and artificial intelligence techniques (Aslantas, Dogan & Ozturk, 2008; Aslantas, 2009b; Zhu & Liu, 2009). The main disadvantage of these techniques is that they require an off-line learning step, overloading and slowing the overall scheme. Therefore, the applicability of the schemes which integrate such approaches is restricted to applications that do not require real-time processing.

Despite the difficulties, the blind watermarking schemes seem to offer the most promising performance: high quality for the watermarked image, i.e., above 40 dB, and good stability towards content-preserving distortions like compression, filtering, noise addition, sharpening and small rotations. Regarding the payload of the secret information, we can say that they are more suitable for watermarking applications rather than steganography, since the latter requires larger messages. However, there are still issues regard-

ing the security of blind schemes, since, to our knowledge, no provable secure data hiding scheme based on SVD has been developed yet.

FUTURE RESEARCH DIRECTIONS AND CONCLUSION

In this chapter, the most complete overview of steganographic and watermarking scheme based on the SVD transform has been presented. Due to different types of digital content (image, audio, video, 3D objects) and aimed applications (copyright protection, authentication) that can be considered, a general classification framework was proposed which focuses mainly on the embedding process and extraction type for both steganography and digital watermarking.

The overview also shows that there are several requirements which the embedding process must satisfy to achieve a high robustness and, at the same time, to solve the flaw of the Liu's scheme, namely the *ambiguity problem*. Currently, data hiding schemes that bound the SVs of the secret message to the features of the digital content, e.g., SVs, DCT coefficients (Huang & Guan, 2004) or any other transform coefficients, are affected by the ambiguity, thus are unable to protect the copyright of the content owner. Solutions proposed to solve this issue insert extra information, e.g., singular vectors which aim to act as a control parameter during the extraction process, or avoid to embed the SVs of the message into the SVs of the host signal (Mansouri, Aznaveh & Azar, 2008). Unfortunately, these schemes require the original content during extraction and, surprisingly, lose the ability to resist against attacks.

Not even the schemes which segment the cover media and use the quantization technique to hide the secret information are immune to the ambiguity problem. Since the singular values of the original content are used during the reconstruction of the modified content, the attack that causes the am-

biguity problem can be mounted on the modified content to remove the concealed information.

Wishing to avoid these drawbacks, recently several studies which investigate the use of the singular values of the digital content for hiding secret information have been proposed. These techniques do not suffer of the ambiguity and they seem a promising approach, even if difficult constraints, e.g., orthonormality, must be satisfied to achieve a good robustness, a high quality for the watermarked content and a perfect extraction of the secret information. Further research should be carried out to clarify the meaning of the singular vectors, their tight relation with the singular values and their ability to convey secret information. Regarding the combined domain techniques, in the majority of cases they are merely an extension of the flawed embedding approaches, without offering a viable solution to the ambiguity problem.

Nevertheless, creating provable secure data hiding schemes that are not affected by this weakness is still a challenging research problem. To provide a complete solution to the ambiguity problem each of such schemes should apply cryptographic techniques to the digital content or to the secret message before performing the hiding process. Given that many data hiding scheme based on SVD are flawed, the aim of this research is to identify them, to give main guidelines to devise secure and unambiguous schemes and to assist the researchers in the field of data hiding to aid their research further.

REFERENCES

- Abdallah, E. E., Hamza, A. B., & Bhattacharya, P. (2007). MPEG Video Watermarking using Tensor Singular Value Decomposition. In Kamel, M., & Campilho, A. (Eds.), *Image Analysis and Recognition* (Vol. 4633, pp. 772–783). Berlin: Springer-Verlag. doi:10.1007/978-3-540-74260-9_69

- Agarwal, R., & Santhanam, M. S. (2006Submitted to). *Digital watermarking in the singular vector domain*. Elsevier.
- Al-Khatib, T., Al-Haj, A., Rajab, L., & Mohammed, H. (2008). A robust Video Watermarking Algorithm. *Journal of Computer Science*, 4(11), 910–915. doi:10.3844/jcssp.2008.910.915
- Andrews, H. C., & Patterson, C. L. (1976). Singular Value Decomposition (SVD) Image Coding. *IEEE Transactions on Communications*, 42(4), 425–432. doi:10.1109/TCOM.1976.1093309
- Aslantas, V. (2009a). An optimal robust digital image watermarking based on SVD using differential evolution algorithm. *Optics Communications*, 282(5), 769–777. doi:10.1016/j.optcom.2008.11.024
- Aslantas, V., Dogan, A. L., & Ozturk, S. (2008). DWT-SVD based image watermarking using Particle Swarm Optimizer. In *Proceedings of 2008 IEEE International Conference on Multimedia* (pp. 241-244).
- Aslatnas, V. (2009b). SVD and DWT-SVD domain robust watermarking using differential evolution algorithm. In Ao, S. I. (Ed.), *Advances in Electrical Engineering and Computational Science* (Vol. 39, pp. 147–159).
- Babu, K. S., Raja, K. B., Uma, M. R. K., Rashmi, K. A., Venugopal, K. R., & Patnaik, L. M. (2007). Robust and high capacity image steganography using SVD. In *International Conference on Information and Communication Technology in Electrical Sciences* (pp. 718-723). Chennai, India: Dr. M.G.R. University Press.
- Bahandri, K., Mitra, S. K., & Jadhav, A. (2005). A Hybrid Approach to Digital Image Watermarking Using Singular Value Decomposition and Spread Spectrum. In Pal, S. K. (Eds.), *Information Assurance in Computer Networks* (Vol. 3776, pp. 447–452). Berlin: Springer-Verlag.
- Bao, P., & Ma, X. (2005). Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition. *IEEE Transactions on Circuits and Systems for Video Technology*, 15(1), 96–102. doi:10.1109/TCSVT.2004.836745
- Barni, M., Bartolini, F., & Furon, T. (2003). A general framework for robust watermarking security. *Signal Processing*, 83(10), 2068–2084. doi:10.1016/S0165-1684(03)00168-3
- Barreto, P. S. L. M., Kim, H. Y., & Rijmen, V. (2002). Toward secure public-key block-wise fragile authentication watermarking. *IEE Proceedings. Vision Image and Signal Processing*, 148(2), 57–62. doi:10.1049/ip-vis:20020168
- Basso, A., Bergadano, F., Cavagnino, D., Pomponiu, V., & Vernone, A. (2009). A Novel Block-based Watermarking Scheme Using the SVD Transform. *Algorithms*, 2(1), 46–75. doi:10.3390/a2010046
- Bergman, C., & Davidson, J. (2005). Unitary embedding for data hiding with the SVD. In Delp, E. J. (Eds.), *Security, Steganography, and Watermarking of Multimedia Contents* (Vol. 5681, pp. 619–630). Bellingham, WA: SPIE.
- Bhatnagar, G., & Raman, B. (2008b). Dual Watermarking Scheme via Sub-sampling in WPT-SVD domain. In *Proceedings of the First International Conference on Emerging Trends in Engineering and Technology* (pp. 850-855).
- Bhatnagar, G., & Raman, B. (in press). a. A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces*.
- Bro, R., Acar, E., & Kolda, T. G. (2008). Resolving the sign ambiguity in the singular value decomposition. *Journal of Chemometrics*, 22(1-2), 135–140. doi:10.1002/cem.1122

- Byun, S.-C., Lee, S.-K., Tewfik, A. H., & Ahn, B.-H. (2003). ASVD-Based Fragile Watermarking Scheme for Image Authentication. In Petitcolas, F. A. P. (Eds.), *Digital Watermarking* (Vol. 2613, pp. 375–391). Berlin: Springer-Verlag. doi:10.1007/3-540-36617-2_14
- Calagna, M., Guo, H., Mancini, L. V., & Jajodia, S. (2006). Robust Watermarking System based on SVD Compression. In *Proceedings of the ACM Symposium on Applied Computing* (pp. 1341–1347). New York: ACM Press.
- Chandra, D. V. S. (2002). Digital image watermarking using singular value decomposition. In *Proceedings of IEEE 45th Midwest Symposium on Circuits and Systems: Vol. 3* (pp. 264–267).
- Chandramouli, R., Kharrazi, M., & Memon, N. (2004). Image Steganography. Concepts and Practice. *Lecture Notes in Computer Science*, 2939, 35–49.
- Chang, C.-C., Hu, Y.-S., & Lin, C.-C. (2007). A Digital watermarking scheme based on singular value decomposition. In Chen, B. (Eds.), *Combinatorics, Algorithms, Probabilistic and Experimental Methodologies* (Vol. 4614, pp. 82–93). Berlin: Springer-Verlag. doi:10.1007/978-3-540-74450-4_8
- Chang, C.-C., Lin, C.-C., & Hu, Y.-S. (2007). An SVD oriented watermark embedding scheme with high qualities for the restored images. *International Journal of Innovative Computing. Information and Control*, 3(3), 609–620.
- Chang, C.-C., Tsai, P., & Lin, C.-C. (2005). SVD-based Digital Image Watermarking scheme. *Pattern Recognition Letters*, 26(10), 1577–1586. doi:10.1016/j.patrec.2005.01.004
- Chung, K.-L., Shen, C.-H., & Chang, L.-C. (2001). A novel SVD- and VQ-based image hiding scheme. *Pattern Recognition Letters*, 22(9), 1051–1058. doi:10.1016/S0167-8655(01)00044-7
- Chung, K.-L., Yang, W.-N., Huang, Y.-H., Wu, S.-T., & Hsu, Y.-C. (2007). On SVD-based watermarking algorithm. *Applied Mathematics and Computation*, 188(1), 54–57. doi:10.1016/j.amc.2006.09.117
- Cox, I., Kilian, J., Leighton, F. T., & Shamoon, T. (1996). Secure Spread Spectrum Watermarking for Images, Audio and Video. In *Proceedings of the International Conference on Image Processing*, 3, 243–246.
- Cox, I., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673–1687. doi:10.1109/83.650120
- Cox, I. J., Miller, M. L., & Bloom, J. A. (2000). *Digital Watermarking*. San Francisco, CA: Morgan Kaufmann.
- Engedy, M., Parasad, M. V. N. K., & Saxena, A. (2006). Singular Value Decomposition (SVD) Based Attack on Different Watermarking Schemes. *Computing Letters*, 2(3), 149–154. doi:10.1163/157404006778330843
- Fan, M.-Q., Wan, H.-X., & Li, S.-K. (2008). Restudy on SVD-based watermarking scheme. *Applied Mathematics and Computation*, 203(2), 926–930. doi:10.1016/j.amc.2008.05.003
- Ganic, E., & Eskicioglu, A. M. (2004). Robust DWT-SVD domain image watermarking: embedding data in all frequencies. In *Proceedings of the 2004 workshop on Multimedia and security* (pp. 166–174). New York: ACM Press.
- Ganic, E., Zubair, N., & Eskicioglu, A. M. (2003). An Optimal Watermarking Scheme Based on Singular Value Decomposition. In *Proceedings of the International Conference on Communication, Network, and Information Security* (pp. 85–90).

- Gao, K.-L., Dong, M., & Zhou, F.-Q. (2006). An image hiding algorithm using Arnold transform and technique of singular value. In Yunlong, S. (Eds.), *Optical Information Processing* (Vol. 6027, pp. 361–368). Bellingham, WA: SPIE Press.
- Ghazy, R., El-Fishawy, N., Hadhoud, M., Desouky, M., & El-Samie, F. (2007). An efficient block-by-block SVD-based image watermarking scheme. *Ubiquitous Computing and Communication*, 2(5), 1–9.
- Gorodetski, V., Skormin, V., & Popyack, L. (2000). SVD approach to Digital Image Lossy Compression. In *Proceedings of the 4th Conference on Systems, Cybernetics and Informatics*.
- Gorodetski, V. I., Popyack, L. J., Samoilov, V., & Skormin, V. (2001). SVD-Based Approach to Transparent Embedding Data into Digital Images. In Gorodetski, V. I. (Eds.), *Information Assurance in Computer Networks* (Vol. 2052, pp. 263–274). Berlin: Springer-Verlag. doi:10.1007/3-540-45116-1_26
- Gorodetski, V. I., & Samoilov, V. (2003). Simulation-Based Exploration of SVD-Based Technique for Hidden Communication by Image Steganography Channel. In Gorodetski, V. I. (Eds.), *Computer Network Security* (Vol. 2776, pp. 349–359). Berlin: Springer-Verlag.
- Haghghi, M. S., & Ghaemmaghami, S. (2005). An Optimal SVD-based Watermarking Framework through Linear Programming. In Hamza, M. H. (Ed.), *European Internet and Multimedia Systems and Applications* (pp. 271–274).
- Hou, Z. (2003). Adaptive singular value decomposition in wavelet domain for image denoising. *Pattern Recognition*, 36(8), 1747–1763. doi:10.1016/S0031-3203(02)00323-0
- Huang, F. J., & Guan, Z. H. (2004). Ahybrid SVD-DCT watermarking method based on LPSNR. *Pattern Recognition Letters*, 25(15), 1769–1775. doi:10.1016/j.patrec.2004.07.003
- Hyvärinen, A., & Oja, E. (1997). A fast fixed-point algorithm for independent component analysis. *Neural Computation*, 9(7), 1484–1492. doi:10.1162/neco.1997.9.7.1483
- Jain, C., Arora, S., & Prasanta, P. K. (2008Submitted to). *A reliable SVD based watermarking scheme*. Elsevier.
- Kardamis, J. (2007). *Audio Watermarking Techniques using Singular Value Decomposition*. Unpublished master dissertation, Rochester Institute of Technology, Rochester, NY.
- Katezenbeisser, S. C., & Petitcolas, F. A. P. (Eds.). (1999). *Information Techniques for Steganography and Digital Watermarking*. Norwood, MA: Artech House Press.
- Kaufman, J., & Celenk, M. (2006). Digital Video Watermarking using Singular Value Decomposition and 2D Principal Component Analysis. In *Proceedings of the 2006 IEEE International Conference on Image Processing* (pp. 2561-2564).
- Kim, K.-S., Lee, M.-J., & Lee, H.-K. (2007). Blind Image Watermarking Scheme in DWT-SVD Domain. In *Proceedings of the 3rd IEEE International Conference on Intelligent Information Hiding and Multimedia Digital Processing* (pp. 477-480).
- Kong, W., Yang, B., Wu, D., & Niu, X. (2006). SVDBased Blind Video Watermarking Algorithm. In *Proceeding of the First International Conference on Innovative Computing. Information and Control*, 1, 265–168.
- Lai, C.-C., Huang, H.-C., & Tsai, C.-C. (2008). Image Watermarking Scheme Using Singular Value Decomposition and Micro-genetic Algorithm. In *Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 469-472).

- Lamarche, L., Liu, Y., & Zhao, J. (2006). Flaw in SVD-based Watermarking. In *Proceedings of the Canadian Conference on Electrical and Computer Engineering* (pp. 2082-2085).
- Lee, S., Jang, D., & Yoo, C. D. (2005). An SVD-Based Watermarking Method for Image Content Authentication with Improved Security. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2, 525–528.
- Li, H., Wang, S., Song, W., & Wen, Q. (2005). A Novel Watermarking Scheme Based on Independent Component Analysis. In Wang, L. (Eds.), *Advances in Natural Computation* (Vol. 5326, pp. 448–453). Berlin: Springer-Verlag.
- Li, H., Wang, S., Song, W., & Wen, Q. (2005). A Novel Watermarking Algorithm Based on SVD and Zernike Moments. In Kantor, P. (Eds.), *Intelligence and Security Informatics* (Vol. 3495, pp. 972–975). Berlin: Springer-Verlag.
- Li, J., Su, B., Li, S., Wang, S., & Yao, D. (2008). A Semi-fragile Watermark Scheme Based on the Logistic Chaos Sequence and Singular Value Decomposition. In Fyfe, C. (Eds.), *Intelligent Data Engineering and Automated Learning* (Vol. 5326, pp. 57–64). Berlin: Springer-Verlag. doi:10.1007/978-3-540-88906-9_8
- Li, Q., Yuan, C., & Zhong, Y. Z. (2007). Adaptive DWT-SVD domain image watermarking using human visual model. In *Proceedings of the 9th International Conference on Advanced Communication Technology: Vol. 3* (pp. 1947-1951).
- Lin, C.-H., Liu, J.-C., & Han, P.-C. (2008). On the Security of the Full-Band Image Watermark for Copyright Protection. In *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing* (pp. 74-80).
- Ling, H.-C., Phan, R. C.-W., & Heng, S.-H. (2008). Attacks on SVD-Based Watermarking Schemes. In Yang, C. C. (Eds.), *Intelligence and Security Informatics* (Vol. 5075, pp. 83–91). Berlin: Springer-Verlag. doi:10.1007/978-3-540-69304-8_10
- Liu, F., & Liu, Y. (2008). A Watermarking Algorithm for Digital Image Based on DCT and SVD. In *Proceedings of the 2008 Congress on Image and Signal Processing: Vol. 1* (pp. 380-383).
- Liu, J., Niu, X., & Kong, W. (2006). Image watermarking scheme based on singular value decomposition. In *Proceedings of the IEEE International Conference on Intelligent Information Hiding and Multimedia* (pp. 457-460).
- Liu, J.-C., Lin, C.-H., Kuo, L.-C., & Chang, J.-C. (2007). Robust Multi-scale Full-Band Image Watermarking for Copyright Protection. In Okuno, H. G., & Ali, M. (Eds.), *New Trends in Applied Artificial Intelligence* (Vol. 4570, pp. 176–184). doi:10.1007/978-3-540-73325-6_18
- Liu, R., & Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*, 4(1), 121–128. doi:10.1109/6046.985560
- Lu, T.-C., Chang, C.-C., & Liu, X.-Y. (2006). A content-based image authentication scheme based on singular value decomposition. *Pattern Recognition and Image Analysis*, 16(3), 506–522. doi:10.1134/S1054661806030187
- Mansouri, A., Aznaveh, A. M., & Azar, F. T. (2008). Secure Digital Image Watermarking Based on SVD-DCT. In Sarbazi-Azad, H. (Eds.), *Advances in Computer Science and Engineering* (Vol. 6, pp. 645–652). Berlin: Springer-Verlag. doi:10.1007/978-3-540-89985-3_79

- Mohammad, A. A., Alhaj, A., & Shalaf, S. (2008). An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Processing Journal*, 88(9), 2158–2180. doi:10.1016/j.sigpro.2008.02.015
- Mohan, B. C., & Kumar, S. A. (2008). A Robust Digital Image Watermarking Scheme using Singular Value Decomposition. *Journal of Multimedia*, 3(1), 7–15. doi:10.4304/jmm.3.1.7-15
- Mohan, B. C., Srinivaskumar, S., & Chatterji, B. N. (2008). A Robust Digital Image Watermarking Scheme using Singular Value Decomposition (SVD), Dither Quantization and Edge Detection. *International Journal on Graphics, Vision and Image Processing*, 8(1), 17–23.
- Okttavia, V., & Lee, W.-H. (2004). A Fragile Watermarking Technique for Image Authentication Using Singular Value Decomposition. In Aizawa, K. (Eds.), *Advances in Multimedia Information Processing* (Vol. 3332, pp. 42–49). Berlin: Springer-Verlag.
- Ozer, H., Sankur, B., & Memon, N. (2005). An SVD-based audio watermarking technique. In A. M. Eskicioglu et al. (Eds.), *Proceedings of the Multimedia and Security Workshop* (pp. 51–56). New York: ACM Press.
- Patra, J. C., Soh, W., Ang, E. L., & Meher, P. K. (2006). An Improved SVD-Based Watermarking Technique for Image and Document Authentication. In *Proceedings of the IEEE Conference on Circuits and Systems* (pp. 1984–1987).
- Peng, Z., & Liu, W. (2006). Color image authentication based on spatiotemporal chaos and SVD. *Chaos, Solitons, and Fractals*, 36(4), 946–952. doi:10.1016/j.chaos.2006.07.015
- Qi, X., Bialkowski, S., & Brimley, G. (2008). An adaptive QIM- and SVD-based digital image watermarking scheme in the wavelet domain. In *Proceedings of the 15th IEEE International Conference on Image Processing* (pp. 421–424).
- Quan, L., & Qingsong, A. (2004). A combination of DCT-based and SVD-based watermarking scheme. In *Proceedings of the 7th international Conference on Signal Processing: Vol. 3* (pp. 873–876).
- Quan, L., & Xiaomei, Z. (2006). A SVD Based Digital Watermarking Algorithm for 3D Models. In *Proceedings of the 8th International Conference on Signal Processing: Vol. 4*.
- Rezazadeh, S., & Yazdi, M. (2006). A Non-oblivious Image Watermarking System Based on Singular Value Decomposition and Texture Segmentation. *Proceedings of the World Academy of Science, Engineering and Technology*, 13, 255–259.
- Rykaczewski, R. (2007). Comments on „An SVD-Based Watermarking Scheme for Protecting Rightful Ownership. *IEEE Transactions on Multimedia*, 9(2), 421–423. doi:10.1109/TMM.2006.886297
- Schaefer, G., & Stich, M. (2004). UCID-An Uncompressed Color Image Database. In *Proceedings of Society of Photo-Optical Instrumentation Engineers, Storage and Retrieval Methods and Applications for Multimedia: Vol. 5307* (pp. 472–480). Bellingham, WA: SPIE Press.
- Shen, Y.-Z., Zhang, M.-J., & Liu, F. (2006). A new algorithm of gray watermark Embedding. In Pan, Z. (Eds.), *Advances in Artificial Reality and Tele-Existence* (Vol. 4282, pp. 769–801). Berlin: Springer-Verlag. doi:10.1007/11941354_82
- Sheih, J.-M., Lou, D.-C., & Chang, M.-C. (2006). A semi-blind digital watermarking scheme based on singular value decomposition. *Computer Standards & Interfaces*, 28(4), 428–440. doi:10.1016/j.csi.2005.03.006

- Shnayderman, A., Gusev, A., & Eskicioglu, A. (2004). A Multidimensional Image Quality Measure Using Singular Value Decomposition. In Y. Miyake et al. (Eds.), *Image Quality and System Performance Conference: vol. 5294* (pp. 82–92). Bellingham WA: SPIE Press.
- Sun, R., Sun, H., & Yao, T. (2002). A SVD and quantization based semi-fragile watermarking technique for image authentication. In *Proceedings of the 6th International Conference on Signal Processing: Vol. 2* (pp. 1592–1595).
- Sverdlov, A., Dexter, S., & Eskicioglu, A. M. (2005). Robust dct-svd domain image watermarking for copyright protection: embedding data in all frequencies. In J. Dittmann (Ed.), *Proceedings of the 2004 Workshop on Multimedia and Security* (pp. 168–174). New York: ACM Press.
- Tang, X., Yang, L., Li, L., & Niu, Y. (2004). Study on a Multifunctional watermarking Algorithm. In. *Proceedings of the IEEE International Conference Signal Processing, 1*, 848–852.
- Ting, G. C.-W. (2006). Ambiguity Attacks on the Ganic-Eskicioglu Robust DWT-SVD Image Watermarking Scheme. In Won, D. (Eds.), *Information Security and Cryptology-ICISC 2005* (Vol. 3935, pp. 378–389). Berlin: Springer-Verlag. doi:10.1007/11734727_30
- Ting, G. C.-W., Goi, B.-M., & Heng, S.-H. (2007). A fragile watermarking scheme protecting originator's rights for multimedia service. In Gervasi, O. (Eds.), *Computational Science and Its Applications* (Vol. 4705, pp. 644–654). Berlin: Springer-Verlag.
- Ting, G. C.-W., Goi, B.-M., & Heng, S.-H. (2009). Attack on a semi-blind watermarking scheme based on singular value decomposition. *Computer Standards & Interfaces*, 31(2), 523–525. doi:10.1016/j.csi.2008.02.007
- Trefethen, L. N., & David, B. (1997). The Singular Value Decomposition. In *Numerical Linear Algebra* (pp. 25–31). Philadelphia, PA: Society for Industrial and Applied Mathematics.
- Tsai, C.-F., & Yang, W.-Y. (2007). Real-time color image watermarking based on D-SVD scheme. In Mery, D., & Rueda, L. (Eds.), *Advances in Image and Video Technology* (Vol. 4872, pp. 289–297). Berlin: Springer-Verlag. doi:10.1007/978-3-540-77129-6_27
- Wang, H.-X., Lu, Z.-M., & Sun, S.-H. (2008). A Blind Video Watermarking Algorithm Based on SVD in the DCT Domain. In *Proceeding of the International Electronic Conference on Computer Science: Vol. 1060* (pp. 360–364).
- Wong, P.-W., & Memon, N. (2000). Secret and public key authentication watermarking schemes that resist vector quantization attack. In Wong, P. W. (Eds.), *Security and Watermarking of Multimedia Contents* (pp. 417–427). Bellingham, WA: SPIE Press.
- Wu, D., Kong, W., Yang, B., & Niu, X. (2008). A fast SVD based video watermarking algorithm compatible with MPEG2. *Standard Soft Computing-A Fusion of Foundations. Methodologies and Applications*, 13(4), 375–382.
- Wu, H.-C., Yeh, C.-P., & Tsai, C.-S. (2006). A Semi-fragile Watermarking Scheme Based on SVD and VQ Techniques. In Gavrilova, M. (Eds.), *Computational Science and Its Applications* (Vol. 3982, pp. 406–415). Berlin: Springer-Verlag. doi:10.1007/11751595_44
- Wu, Y. (2005). On the Security of an SVD-Based Ownership Watermarking. *IEEE Transactions on Multimedia*, 7(4), 624–627. doi:10.1109/TMM.2005.846774
- Xia, X.-G., Boncelet, C. G., & Arce, G. R. (1998). Wavelet transform based watermark for digital images. *Optics Express*, 3(12), 497–511. doi:10.1364/OE.3.000497

- Xiao, L., Wei, Z., & Ye, J. (2008). Comments on “Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition” and theoretical analysis. *Journal of Electronic Imaging*, 17(4), 1–3. doi:10.1117/1.3041170
- Xiao-Ping, Z., & Kan, L. (2005). Comments on „An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*, 7(2), 593–594. doi:10.1109/TMM.2005.843357
- Xing, Y., & Tan, J. (2007). A Color Watermarking Scheme Based on Block-SVD and Arnold Transformation. In *Proceedings of the Second Workshop on Digital Media and its Application in Museum and Heritage* (pp. 3-8).
- Xing, Y., & Tan, J. (in press). Mistakes in the paper entitled “A singular-value decomposition-based image watermarking using genetic algorithm”. *International Journal of Electronics and Communications*.
- Yang, J.-F., & Lu, C.-H. (1995). Combined Techniques of Singular Value Decomposition and Vector Quantizationf for Image Coding. *IEEE Transactions on Image Processing*, 4(8), 1141–1146. doi:10.1109/83.403419
- Yavuz, E., & Telatar, Z. (2006). SVD Adapted DCT Domain DC Sub-band Image Watermarking Against Watermark Ambiguity. In Gunsel, B. (Eds.), *Multimedia Content Representation, Classification and Security* (Vol. 4105, pp. 66–73). Berlin: Springer-Verlag. doi:10.1007/11848035_11
- Yavuz, E., & Telatar, Z. (2007). SVD Adapted DCT Domain DC Sub-band Image Watermarking Against Watermark Ambiguity. In Y. Cho et al. (Eds.), *Proceedings of the 2007 ACM symposium on Applied computing: Vol. 4105* (pp. 1051-1055). New York: ACM Press.
- Zhang, X.-P., & Li, K. (2005). Comments on “An SVD-Based watermarking scheme for protecting rightful Ownership”. *IEEE Transactions on Multimedia*, 7(3), 593–594. doi:10.1109/TMM.2005.843357
- Zhou, B., & Chen, J. (2004). A geometric distortion resilient image watermarking algorithm based on SVD. *Chinese Journal of Image and Graphics*, 9(4), 506–512.
- Zhu, S., & Liu, J. (2009). A Novel Adaptive Watermarking Scheme Based on Human Visual System and Particle Swarm Optimization. In Bao, F., Li, H., & Wang, G. (Eds.), *Information Security Practice and Experience* (Vol. 5451, pp. 136–146). Berlin: Springer-Verlag. doi:10.1007/978-3-642-00843-6_13
- Zude, Z., Qingsong, A., & Quan, L. (2006). A SVD-based Digital Watermarking Algorithm for 3D Mesh Models. In *Proceedings of the 8th International Conference on Signal Processing: Vol. 4* (pp. 16-18).

KEY TERMS AND DEFINITIONS

Singular Value Decomposition (SVD):

Powerful numerical tool for factorizing rectangular matrices with complex or real values in the form: $SVD(A_{m \times n}) = [U_{m \times m}, S_{m \times n}, V_{n \times n}]$, where $S_{m \times n}$ is a diagonal matrix and $U_{m \times m}$ and $V_{n \times n}$ are unitary matrices, i.e., $U \cdot U^T = I_{m \times m}$, $V \cdot V^T = I_{n \times n}$, where $I_{m \times m}$ and $I_{n \times n}$ are the identity matrices. It has been extensively applied in information retrieval, recommender systems and signal processing, like image compression or data hiding.

Singular Values: The diagonal entries of $S_{m \times n}$ and related to the energy of the matrix A . If A represents an image, then modifying the magnitude of the singular values will affect the image luminance.

Singular Vectors: The columns of $U_{m \times m}$ and $V_{n \times n}$ that give the underlying structure of the image, i.e., the horizontal and vertical details.

Normal SVD: If the first component of left singular vectors is non-zero and the singular values of $S_{m \times n}$ are in decreasing order.

Ambiguity Problem: Inability to ensure the correct detection of hidden data and consequently the impossibility to certainly identify the ownership of a media.

Combined Domain: A series of different transforms, i.e., DCT, DWT, SVD, etc., applied to the original content. At each step, all (or some) features of the previous transform are retained

and further treated by the successive transform. In general, the features of the combined domain are more stable against common and geometrical attacks.

Segmentation: Partition of the digital content into blocks of variable or fixed size. The stability of the SVs is directly proportional to the segmentation size, i.e., increasing the segmentation size improves the robustness against attacks.

Quantization: Is a compression technique which compacts a range of values to a single value, i.e., quantized value. Specific applications include DCT data quantization in JPEG and DWT data quantization in JPEG 2000.

Chapter 12

Feature Based Watermarking

Hedley Morris

Claremont Graduate University, USA

Mohammad Eyadat

California State University, USA

Imad Muhi

New York Institute of Technology, Jordan

ABSTRACT

A digital media product must be protected with a watermark. This mark must be resilient yet transparent to legitimate users of the media. There are those who seek to cloud the ownership of digital media by tampering with the embedded marks. For example, a small rotation, scale change or cropping of an image can make it difficult, or impossible, for the legitimate owner to recover the watermark. This is called a geometric attack. The authors present a new paradigm for rendering any watermarking scheme resistant to such geometric attacks. This is done by means of a new image transform to a Rotation, Scaling, and Translation (RST) invariant domain based on ideas from shape theory. They also propose extensions of this technique to video watermarking. Finally, the authors provide an example of how these ‘shape based’ concepts can be extended to more general relational databases provided an abstract notion of shape is employed.

INTRODUCTION

The growth of the Internet has led to a massive distribution of digital multimedia data. This has spawned major concerns over intellectual property and ownership rights. By its nature digital data offers the possibility of mass duplication and the unfettered distribution of copyrighted materials. These concerns led to the Digital Millennium Copyright

Act in 1998. Watermarking involves embedding a hidden signal, a watermark, directly into digital data in an irreversible fashion. Such a watermark can be used for standard tasks such as the copyright protection of intellectual property, the tracking of illegal copies and copy protection, the direct control of duplication devices. Watermarks can also be used to test for data tampering, say of medical data. In this chapter we will consider mainly the watermarking of images and videos with a brief description of the watermarking of relational databases. This chapter

DOI: 10.4018/978-1-61520-903-3.ch012

demonstrates how an approach to watermarking based on ideas from shape theory provides a new set of methods that allow conventional watermarking methods for images to be extended to more general digital objects such as video streams and relational databases. The approach is to mark not individual elements such as pixels but identifiable subsets of the data. Shape theory (Kendall, 1999) is concerned with algorithms for the recognition of similar objects. Watermarking is concerned with the hiding of data in digital objects. Attacks distort such objects and so, to recover the watermark, it is necessary to be able to recognize deformations of objects as similar. Shape theory is all about algorithms for similarity testing (Goodall, 1999).

Hiding information in a multimedia data is easy. Doing so in a way that allows its retrieval or to prove its existence is a different matter. This is especially so when outside agents are trying their best to remove or replace your mark.

Geometric attacks alter the image in such a way that it is difficult to find where the mark is hidden. Watermarks that are invariant to geometric distortions can be designed, see for example (Bas et al., 2002) for the basic watermarking method.

Based on the well known algorithms and approaches we may summarize these approaches into 3 categories:

1. Using the Fourier-Mellin-Transform for the required invariance. An invariant vector is constructed from the slices of the log-polar mapped Fourier magnitude spectrum. A watermark is embedded by modifying this vector. Algorithms using the Fourier-Mellin transform suffer serious implementation difficulties. The log-polar and inverse log-polar mapping introduces errors during insertion. As they use the Fourier magnitude spectrum, interpolation performance is poor because interpolation only performs well with the sample values with the same scale.
2. There are many other implementation problems to consider. Watermarking algorithms

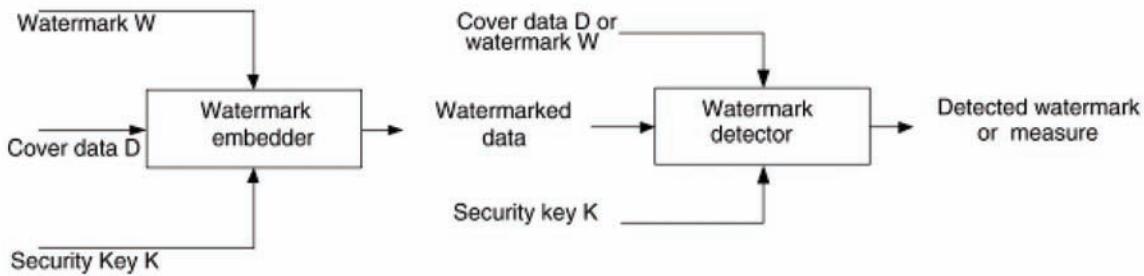
using a feature of an image were proposed as the second generation watermark. As features of the image have high invariance to distortions, they can be used as a key to find the insertion location. The features of the image have high invariance to distortions, and consequently determine where a mark has been inserted, see (Cox, et al., 2002).

3. In this chapter we propose a new feature-frame based image watermarking method that is resistant to geometrical attacks. Our approach is based on regions rather than points. A set of k-sided polygons in the plane is called a frame of k-ads. In order that our k-ads should be identifiable we use polygons whose vertices are image features. To give us the robustness required, the features chosen must be stable feature points. We must be able to identify and locate the equivalent k-ads in geometrically attacked images. Our methods do not depend on the feature point locator but we do require that the method not produce too many feature points. A regular Harris corner detector produces a huge number of features which change under rotations. A feature detector that is able to select mostly robust points that are preserved under geometric attack is needed. For our work we have selected the SIFT method, see (Ettinger, 2002)

We present a new watermarking scheme in which the watermarking is carried out in the spatial domain using robust feature points to aid in its embedding and extraction. These specific feature points are not only used to embed information, but also act as a geometrical reference. Our new method is based on embedding multiple copies of watermarks in regions around robust feature points and using shape theory to remediate the effects of affine attacks. In this chapter we show that:

- This new approach to watermarking that is based on a feature-frame in an image

Figure 1. A typical watermarking system



enhances the ability of any watermarking to resist geometric and digital image processing attacks. The development of a new image transform based on projective invariance leads to a new watermarking spaces we call universal images (UI's).

- Applying any known watermarking algorithm to the UI's of an image removes the need for the dyadic dimensions and at the same time imbues the watermark with affine invariance. This way of watermarking is an entirely new and is a promising watermarking approach, since it is designed to withstand severe affine attacks.
- Using distinguished k-aads allows us to control the area where we want to hide our watermark (WM).
- We construct an algorithm for watermark recovery based on results from shape theory. By using the results from Veronese-Whitney embedding theory we present a way to locate affine related k-aads in an image. This is used to locate hidden watermarking zones.

BACKGROUND

There are two principle objectives of media watermarking. The most obvious concerns the protection of digital rights. In this case our concern rests in information about content ownership and intellectual property rights (Cox, 2002). The em-

phasise in applications is on audio, image and video content. As important is content verification. The purpose in this case is to ensure that the original multimedia content has not been tampered with. The focus is on authentication. This is important for secure document transmission. Figure 1 shows the form of a typical watermarking system

There are two parts, a watermark embedder and a watermark detector. The inputs to the watermark embedder are the watermark, the cover media data and a security key. The watermark is usually a number sequence or a binary bit sequence. The key enhances the security of the whole system. The output of the watermark embedder is the watermarked data. The inputs to the watermark detector are the watermarked data, the security key and often the original watermark. There is considerable interest in reducing the retrievability of such a watermark. As a result digital watermarking needs to be robust against attempts, known as attacks, to remove or alter it. In the following sections we look at the watermarking process.

The Embedding Phase

There are several well-known algorithms, in the literature, to embed a watermark into a multimedia object. Each Watermarking method has its own requirements; however, these algorithms must possess the following essential **properties**:

1. **Invisibility** to avoid degrading the quality of the original (host) digital data. It is important

- that users should not notice the existence of the watermark.
2. **Robustness** against attacks and image processing operations. Robustness means that the watermark should be able to robust against any reasonable image processing or attacks. In some of the watermarking techniques, robustness is more a property and not a requirement.
 3. **Fidelity** the watermarked data must look, or sound, like the original. In other words, the degradation to the digital data after adding a watermark is very hard to discern by the observer.
 4. **Resistance** against legal image processing, such as signal distortions.
 5. **Effectiveness** is the probability of detecting the watermarking soon after it is completed with the embedding.
 6. **Computational Cost** is the how long time will it take for a watermark to be embedded and detected.
 7. **Security** of the encryption techniques.
 8. **Payload** refers to the amount of information that can be stored in the watermark.

The most common way to embed a watermark W into an image I is to use the additive $I' = I + \alpha W$ or the multiplicative $I' = I(1 + \alpha W)$ modification, where α is a parameter called the Watermark's strength and I' is the watermarked image. This method is most often applied in the transform domain and the inverse transform applied. As a result the watermark is spread throughout the original image. The most common transform is some type of wavelet

The Human Visual System (HVS) is less sensitive to changes near the edges of an image than it is in the smooth regions (Tovee, 2008). Therefore, we need to increase the strength of the watermark in the image around the edges and high-textured regions, and decrease it in the smooth regions of the image. In general, invisible-watermarking

schemes can be broadly classified into two categories or techniques:

1. **Spatial domain-based:** This technique is based on the modification of the intensity or the values of pixels in blocks. One tool used in the spatial domain includes bit-wise techniques such as the Least Significant Bit (LSB). Another technique involves noise insertion and manipulation.
2. **Frequency domain-based or Transform domain-based:** This technique can embed a larger number of bits without affecting the HVS. It is kind of an image adaptive Watermark (WM) embedding scheme: The common transforms are the Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT) or the Discrete Wavelet Transform (DWT). Here we first find the transform of the image and then insert the watermark in important frequency regions, such that the watermark is spread over all the pixels in the image.

The Wavelet Method

If a two-dimensional separable dyadic DWT (Strang & Nguyen, 1996) is applied to an image each level of decomposition produces four bands of data, one corresponding to the low pass band (LL), and three other corresponding to horizontal (HL), vertical (LH), and diagonal (HH) high pass bands. The decomposed image shows a coarse approximation image in the lowest resolution low pass band, and three detail images in higher bands. The low pass band can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached. Figure 2 shows a three level decomposition.

Most of the information in an image is located in the low-resolution block LLL, which represents the smooth parts of the image. It is also known that human visual system (HVS) is particularly

Figure 2. Three level decomposition

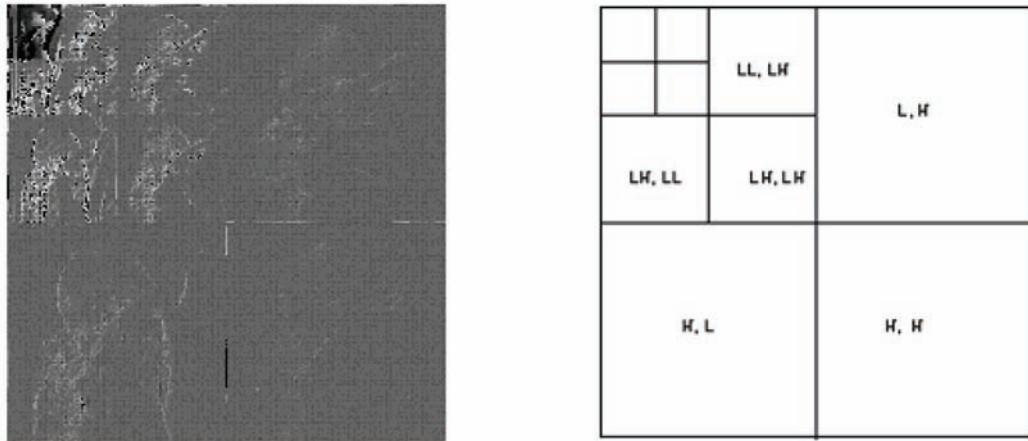
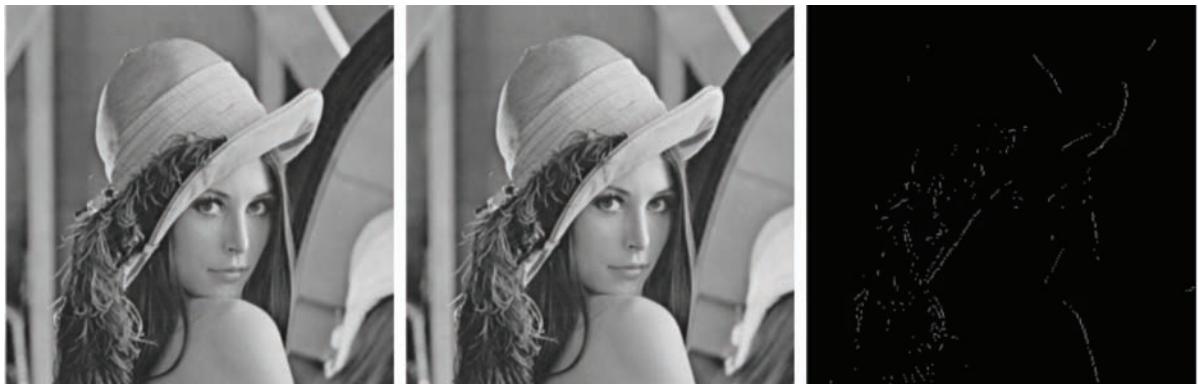


Figure 3. (a) Original image (b) watermarked image (c) the watermark



sensitive to small changes in this part of the image. Consequently, this block is often left unaltered. For example, a simple watermarking algorithm could consist of the following steps:

1. Compute the DWT coefficients with a wavelet filter.
2. Locate those coefficients that are above a given threshold in the sub-bands other than the low pass sub-band.
3. Modify each sub-band coefficient C_i (above the threshold) to $C'_i = C_i + \alpha |C_i| w_i$ where w_i is generated from a uniform distribution

of zero mean and unit variance and α is a constant.

Figure 3 shows the output of this algorithm when applied to lena.

We see that watermark is only added to the image edges because adding the watermark to significant coefficients in the high frequency bands is equivalent to adding the watermark to only the edge areas of the image. The watermark is the random sequence $\{w_i\}$.

The Extraction Phase

Watermark extraction can be divided into two phases. First involves locating the watermark, and second entails recovering the watermark information. The process can be done in many ways:

1. **Image independent (blind watermarking):** The watermark is placed in a linear way. The verification of the watermark can be performed without use of the original image. In this case, extracting is done without the existence of the original data
2. **Image dependent (non-blind watermarking):** The original image information is used in order to verify the existence of the watermark. The original data is needed for the extraction process in this case.
3. **Visible Watermark:** Designed to be easily seen by the viewers, and clearly identified by the owner. This method relies on some feature or data extractions process.

To detect the presence of a watermark a similarly measure is often employed to gauge the degree of similarity between two images. A common metric is given by

$$SM = \frac{\sum_{i=1}^m \sum_{j=1}^n [I(i, j) - I'(i, j)]^2}{\sum_{i=1}^m \sum_{j=1}^n [I(i, j)]^2} \quad (1)$$

where $I(i, j)$ refers to the original image, and $I'(i, j)$ refers to the watermarked one. Similarity also can be used as a criterion to measure the performance of the watermark embedding algorithm. Another criterion is Structure Similarity, which refers to the relationship between the distribution of the coefficients within the original image and those of the watermarked image. It can be quantified in the quantity SS defined by

$$SS = \frac{\sum_{i=1}^m \sum_{j=1}^n [I(i, j) * I(i, j)]}{\sum_{i=1}^m \sum_{j=1}^n [I'(i, j) * I'(i, j)]} \quad (2)$$

where again $I(i, j)$ refers to the original image, and $I'(i, j)$ refers to the watermarked image. The images that are compared this way are usually not the original images but rather the embedded watermark and recovered watermark represented as images.

Digital Watermarks and Attacks

As the distributions of digital data become more extensive, there is a considerable commercial incentive to protect and copyright these data. Digital watermarking techniques provide the solution for this problem (Voloshynovskiy et al., 2001). Dealing with attacks requires the development of watermark embedding methods robust against such attacks and the definition better benchmarks. The quality and the robustness of any algorithm used to embed digital watermark is measured by four criteria:

1. **Transparency:** The digital WM should not degrade the quality of images. In other words, the HVS will not be disturbed by embedded WM.
2. **Security:** Deals with who is capable of extracting the WM from marked data.
3. **Robustness:** Deals with how well the algorithm is able to withstand attacks. Hackers would try to modify or perform different kinds of attacks.
4. **Capacity:** Measures the amount of data a watermarking algorithm can embed before causing severe visual degradation. In general, one would like a high-capacity algorithm to embed more information.

It is important to note that, in general, a digital WM attack succeeds in defeating a watermarking scheme if it impairs the WM beyond acceptable limits while maintaining the perceptual quality of the attacked data. Based on the amount of knowledge the attacker has about the used watermarking scheme, we can introduce the following classification of attacks to watermarking systems.

Blind Watermarking Attacks

One categorization of the wide class of existing blind watermarking attacks contains four classes:

1. *Removal attacks.* These attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm. This category includes: Denoising; Quantization (e.g., for compression); Re-modulation.
2. *Geometric attacks.* Affine attacks attempt to destroy the synchronization of the watermark signals embedded in original image by introducing global and local changes to the image coordinates. The resynchronization is usually a necessary pre-processing step, in order to correctly extract the watermark. Some examples are: Rotation, Scaling, Translation (RST) and Compression. Watermarks must also be able to survive any reasonable digital filtering that may be applied to an image
3. *Cryptographic attacks.* Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded WM information.
4. *Protocol attacks.* Protocol attacks aim at attacking the entire concept of the watermarking system. They aim to create ambiguity with respect to the true ownership of the data..

Of these, Geometric attacks are the biggest problem. Watermarks should be RST invariant. This type of watermarking in which the pixel values, either in the spatial or a transformed space, are modified by a specific or random signal is called first generation watermarking. In second generation watermarking the emphasis is removed from individual pixels and transferred to image features.

THE FEATURE BASED APPROACH

The idea in second generation watermarking is to use salient image features. For these types of watermarking algorithms, also known as “Content aware methods”, specific knowledge of the image features at embedding time is used to maximize the robustness of the embedded watermark. Usable features must be:

1. Invariant under geometrical transformations
2. Invariant to noise like distortions

One way to cope with resynchronization problems after affine transforms is to embed the watermark in an invariant domain. (Ruanaidh & Pun, 1998) invented a transformation to an RST invariant domain. The method uses a log-polar coordinates

$$x_1 = \bar{x}_1 + e^\mu \cos(\theta), x_2 = \bar{x}_2 + e^\mu \sin(\theta), \quad \mu \in R^+, \theta \in [0, 2\pi] \quad (3)$$

located at the point (\bar{x}_1, \bar{x}_2) . Applying the Fourier transform after the log-polar mapping provides a translation, rotation, and scaling-invariant domain. This transform is named the Fourier–Mellin transform. In their scheme, watermark embedding is performed in this new RST invariant domain (Zheng et. al., 2003). Figure 4 shows the distorting effect of the log-polar part of the transform.

Figure 4. (a) The lena image (b) The log-polar transform of lena



A problem is the selection of the center of the new polar system. It is usually taken to be the center point of the image. In the Bas (2001) method circular patches are drawn around the most robust feature points. These are mapped to RST invariant domains which can be watermarked. In this chapter we present an alternative transform, using triangles rather than disks, to map regions of an image to a different type of RST invariant domain.

Feature Detectors

In order to be able to use features to locate watermarks it is essential for those features to be robust against geometrical attacks. There are a number of ways of finding such features. We examine two of them. The Harris detector and the scale-invariant feature transform (SIFT) detector.

The Harris Corner Detector

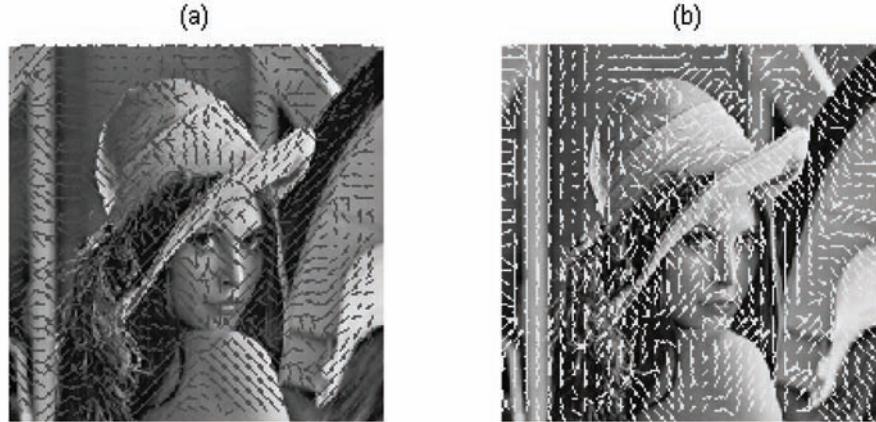
A robust feature is one that persists over a range of scales. In order to characterize such features and devise suitable feature detectors we must first understand image scale. The type of feature we are looking for is not an edge, but rather a corner

where two or more edges meet. Edges are detected by calculating the gradient of an image and are too numerous to be useful. A way must be found to single out from the edges those which comprise corners. How are corners characterized? Images are not smooth and so it is necessary to define what we mean by the derivatives of an image. One way is to convolve I with a Gaussian kernel

$$G_\sigma = \exp\left(-\frac{x^2 + y^2}{2\sigma^2}\right). \quad (4)$$

This gives a set of images $I^\sigma = G_\sigma * I$ where $*$ denotes convolution. This continuum of images I^σ is sometimes called the *scale space representation* of I . The gradient of I^σ is defined to be $\nabla I^\sigma = \nabla G_\sigma * I$. Similarly, higher derivatives can be defined by convolving with higher derivatives of the Gaussian. To find features like corners we study the gradient orientation and intensity at each point of an image. This leads us to look at what is known as the image *structure tensor*. Let us suppose we have selected a scale σ and we are examining an image I^σ . At each point in the image we construct the 2×2 matrix

Figure 5. Eigenvector field of (a) smallest eigenvalue, (b) largest eigenvalue



$$\nabla I^\sigma \nabla I^{\sigma t} = \begin{pmatrix} I_x^{\sigma 2} & I_x^\sigma I_y^\sigma \\ I_x^\sigma I_y^\sigma & I_y^{\sigma 2} \end{pmatrix}. \quad (5)$$

This is known as the Structure Tensor (Arseneau, 2008).

An additional smoothing operation with scale ρ is then applied to produce the structure tensor

$$J_\rho = G_\rho * \nabla I^\sigma \nabla I^{\sigma t} \quad (6)$$

There are therefore two distinct scales involved, σ and ρ . At each point in an image let J_ρ have eigenvalues λ_1, λ_2 with $|\lambda_1| > |\lambda_2|$ with the corresponding eigenvectors v_1, v_2 . The eigenvector v_2 determines the dominant orientation of an image at the given point. The quantity $\lambda_1 + \lambda_2$ is a measure of the intensity at the point.

Corner detectors attempt to devise a combination of λ_1 and λ_2 that can distinguish between plain edges and corners. The Harris detector (Harris & Stephens, 1988) is defined to be

$$C_{\text{Harris}} = \det(J_\rho) - k \operatorname{Tr}(J_\rho)^2 = \lambda_1 \lambda_2 - k(\lambda_1 + \lambda_2)^2 \quad (7)$$

where k is an empirically determined constant usually taken to lie in the range (0.04, 0.06). The term involving the trace is intended to suppress edges. The fact that k is arbitrary is unfortunate and a variant on the Harris detector that removes this aspect was proposed by Nobel in her thesis [Nobel 89]. The Noble detector is

$$C_{\text{Nobel}} = \frac{\det(J_\rho)}{\operatorname{Tr}(J_\rho)} = \frac{\lambda_1 \lambda_2}{\lambda_1 + \lambda_2 + a^2} \quad (8)$$

The parameter a is related to the noise level in the image and often taken to be zero. Another choice, due to (Shi & Tomasi, 1994) is $C_{\text{Shi-Tomasi}} = \min(\lambda_1, \lambda_2) > t$, for some threshold t .

Detectors of Harris type, based on the gradient field of an image, tend to produce a large number of corner candidates. One way to select the most dominant is to use a process called *non maxima suppression*. In this approach an edge point is defined to be a point whose strength a local maximum in the direction of the gradient. This should always be applied. If we use the Nobel measure then, after suppressing local maxima, we can obtain a result like that shown in Figure 7

Figure 6. The contours of the Shi-Tomasi detector superimposed on the lena image



Figure 7. Local maximum suppression



(a). But, as Figure 7 (b) shows, one can still find a huge number of corner points in some images.

Instead of basing our description of corner points on the image gradient we can use the idea of image curvature. The *isophote curvature* of an image is defined as

$$c_{iso} = \frac{2I_x^\sigma I_y^\sigma I_{xy}^\sigma - I_x^{\sigma 2} I_{yy}^\sigma - I_y^{\sigma 2} I_{xx}^\sigma}{(I_x^{\sigma 2} + I_y^{\sigma 2})^{3/2}} \quad (9)$$

In the curvature context, corners are defined as absolute maxima of c_{iso} . This is the Kitchen and Rosenfeld detector (Kitchen and Rosenfeld, 1982).

The SIFT Method

SIFT was developed by Lowe (Lowe, 2004) for image feature generation in object recognition.

Figure 8. The SIFT image pyramid

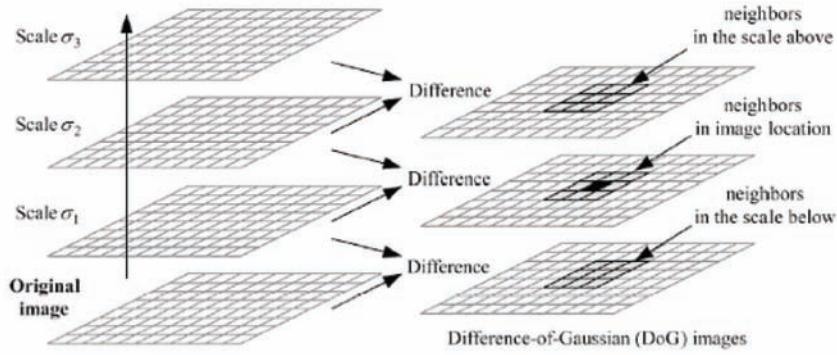


Figure 9. Typical output from SIFT

xloc	yloc	scale	size	edge tag	edge orientation	prominence
115.5243	210.3435	1.7346	2.0204	0	4.7124	-1.4349
124.9223	196.7486	2.1036	2.3465	1	0	-0.8935
156.2825	137.4315	2.1793	2.4197	0	1.5708	-1.1225
158.9022	158.6591	1.8683	2.133	0	4.7124	-0.9805
159.4298	179.2016	1.97	2.2228	0	5.4978	-1.8961
187.7796	159.7414	2.242	2.482	0	1.5708	-3.0167
213.5307	243.945	2.2539	2.494	1	4.3197	-2.5103
216.9852	223.9251	2.0416	2.2882	1	4.7124	-1.7238
217.7257	218.2623	2.1411	2.3824	0	1.5708	-1.5793
226.8712	197.5393	2.0801	2.3242	0	1.5708	-1.4637

In the SIFT method the difference

$$I^\sigma - I^{k\sigma} = (G_\sigma - G_{k\sigma}) * I \quad (10)$$

between two members of the scale space representation of an image I are examined. Key locations are selected at maxima and minima of these differences of Gaussians filtered images.

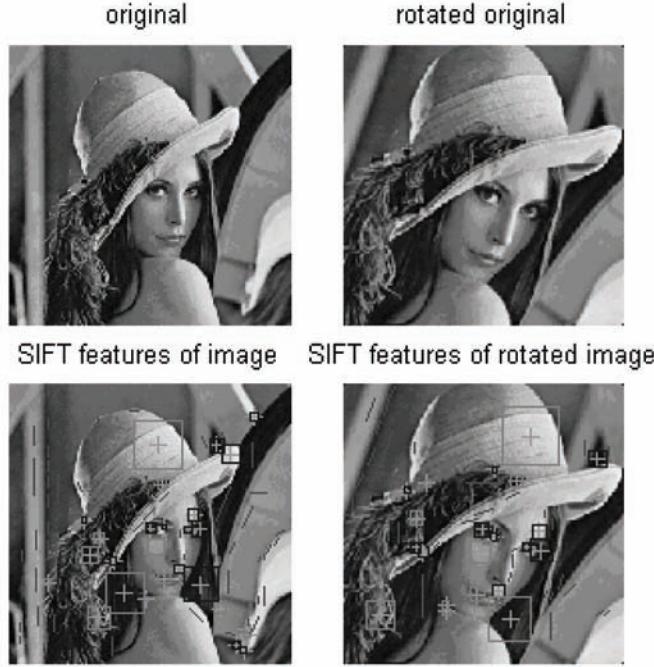
A sub-pixel image location, scale and orientation are associated with each SIFT feature. This additional information allows a classification of feature points according to their robustness across different scales. Candidate features that have a low contrast or are poorly localized along edges are

removed by using a robustness measure. Figure 9 shows typical output from SIFT.

The idea is that if we can find robust feature points they will be preserved under geometric (RTS) transformations. Figure 10 shows the application of the SIFT method to an image and a rotated version of it. Note that for the most part significant features are preserved. However, features can be lost and there prominence changed.

In Figure 10 lines indicate edge features and boxes represent prominent non-edge features. The size of the box is a measure of the particular feature's prominence. SIFT avoids the over-identification of features of standard Harris type

Figure 10. Feature points of lena and its rotated version



detectors producing a much smaller number of robust features. This is illustrated in Figure 11

SHAPE BASED WATERMARKING

In Morris and El-Ddin (2007, 2008) a feature based image watermarking method that is resistant to geometrical attacks has been proposed. The approach is based on regions rather than points. The key element of our construction, for a regular image, is a triangle. To give us the robustness required, the vertices chosen to be stable feature points. This is essential as it is necessary to be able to identify and locate the equivalent triangles in the geometrically attacked image. For our work we have selected the SIFT method (Lowe, 2004) to get stable features. However, our method is independent of the SIFT algorithm. The method generates triples of RST invariant image regions that we call watermarking zones.

Invariant Domains

Let R_1, R_2 and R_3 be any three non-collinear points and A is any fourth point in the plane, and let the point X be the intersection of the lines R_1R_2 and R_3A as shown in Figure 12.

From the triangles formed in Figure 12, we can construct two affine invariants (Sparr, 1996) as follows:

$$r_1 = \frac{\text{area}(R_1R_2R_3)}{\text{area}(XR_2R_3)} \quad \text{and} \quad r_2 = \frac{\text{area}(XR_2R_3)}{\text{area}(AR_2R_3)} \quad (11)$$

Each point $A = (x, y)$ is associated with a unique point (r_1, r_2) . Furthermore, the interior of the triad Δ maps to the rectangle $[1, \infty) \times [1, \infty)$.

$$X = R_2 + \frac{1}{r_1}(R_1 - R_2) \quad \text{and} \quad A = R_3 + \frac{1}{r_2}(X - R_3) \quad (12)$$

Figure 11. SIFT classified features for (a) lena (b) mandrill

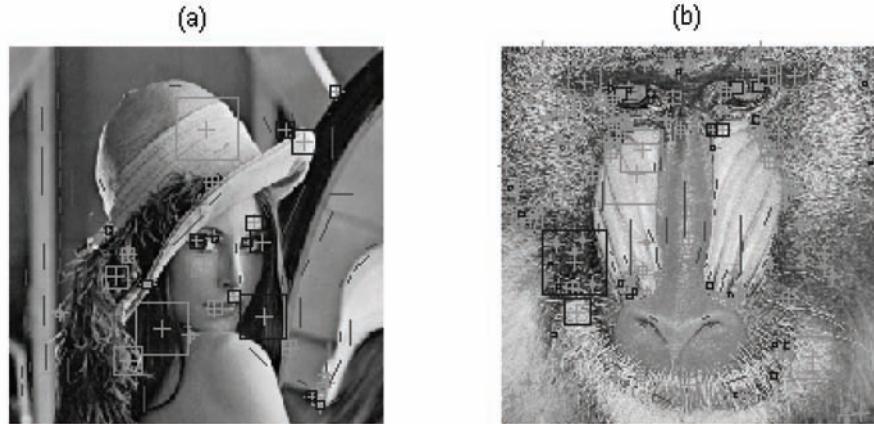
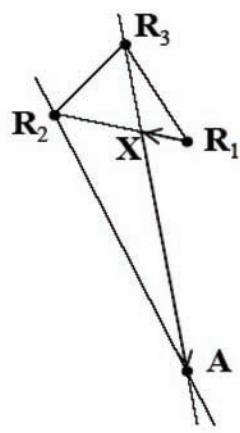


Figure 12. The basic triangle



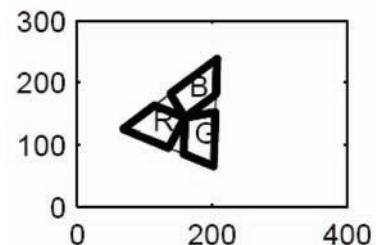
The mapping ϕ is a $1 - 1$ transformation with inverse

$$\phi^{-1} : [1, \infty) \times [1, \infty) \rightarrow \Delta \quad \text{with} \quad (r_1, r_2) \rightarrow A. \quad (13)$$

This inverse map has the explicit form:

$$r_1 = \frac{\det(A - R_3, R_2 - R_1)}{\det(A - R_3, R_2 - R_3)} \quad \text{and} \quad r_2 = \frac{\det(R_2 - R_3, R_1 - R_2)}{\det(A - R_3, R_1 - R_2)} \quad (14)$$

Figure 13. The three quadrilateral regions and the mapping zones



This mapping depends upon the choice of vertex R_3 and so, in order to avoid this restriction, we divide the triangle into three quadrilateral regions Q_i , $i = 1, 2, 3$ by adding the centroid of the triangle as an additional vertex, see Figure 13. In this way we obtain three watermarking zones, one for each vertex, R_1, R_2 and R_3 , of the triangle Δ . Then for each i , we define the map

$$\phi_i : Q_i \rightarrow U_i = \left[1, 2\right] \times \left[1, \frac{3}{2}\right], \quad i = 1, 2, 3 \quad (15)$$

These three watermarking zones are shown in Figure 13. Each rectangle corresponds to a vertex, and each zone Q_i is the pre-image of the same rectangle U .

In Figure 13, the upper left image shows the 3 watermarking zones, one for each vertex R_1, R_2 and R_3 , of the triangle Δ . The rest three images represent the three rectangles U_i , $i = 1, 2, 3$, (blue, green, and red), each one corresponds to one of the three vertices.

An $n \times m$ image $I(i, j)$ is defined on a rectangular grid. The set of 3-tuples is given by

$$\{ i, j, I(i, j) \mid 1 \leq i \leq m, 1 \leq j \leq n \} \quad (16)$$

Each of the mappings ϕ_i maps the image points in the i -th zone Q_i to an unstructured set of points in the rectangle U_i . We define an image on U_i by introducing a grid on U_i and then interpolating the unstructured data to that grid. In this work we use a 64×64 grid. Thus, whatever the size of the original image, it is mapped to three square images. We call each of these three resulting images a Universal Image (UI). The inverse of the mapping is implemented in a similar way. These are RST invariant domains.

Wavelet methods often require images of size $2^k \times 2^k$. This process makes it possible to use wavelet methods with reduced boundary effects. Having three Universal Images gives us choices of implanting the same watermark in each image or developing an error-correcting scheme.

These Universal images are affine invariant in the sense that, for any affine mapping T , the following relation holds

$$\phi_i(TI, T\Delta) = \phi_i(I, \Delta), \quad i = 1, 2, 3 \quad (17)$$

In the original image of lena we have selected three quadrilateral regions that map to three square Universal Images. Figures 14 and 15 below illustrate this.

Figure 16 shows an example of the invariant images obtained by using this process.

Figure 17 illustrates the invariance of these regions with respect to cropping and rotation.

Figure 14. Illustration of the 3 Watermarking zones for the lena Image



Shape Watermarking

Figure 18 shows our general paradigm. On the left we have the embedding phase and on the right the extraction phase.

The steps in the embedding phase are:

1. Using SIFT to find robust feature points.
2. Identify a stable triangle Δ in the image.
3. Construct a set of universal images from the triangle Δ .
4. Embed a watermark in each of the universal images.
5. Map the universal images back to get the watermarked image.

It is also possible to select a set of non-overlapping triangles each of which defines a set of invariant regions. As the watermark is embedded in the interiors of the triangles we are guaranteed that they will not interfere with each other. Any watermarking technique can be used to embed a mark into the invariant domains. Each of the three

Feature Based Watermarking

Figure 15. Illustration of the mapping from the watermarking zones to the Universal Images

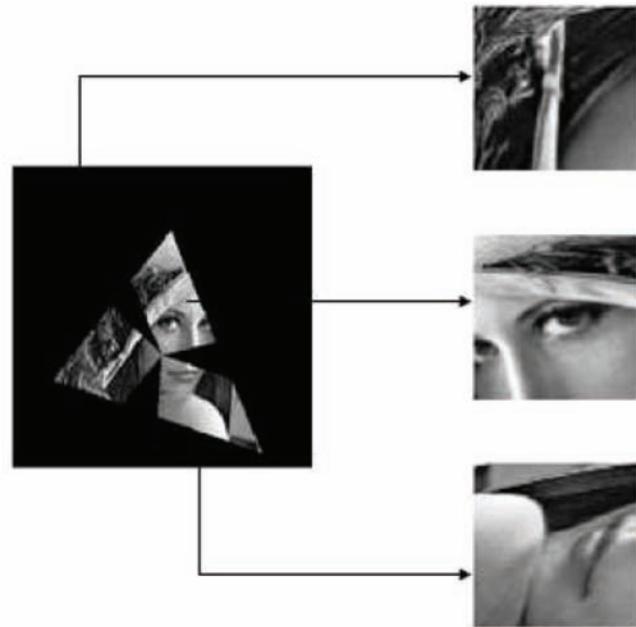


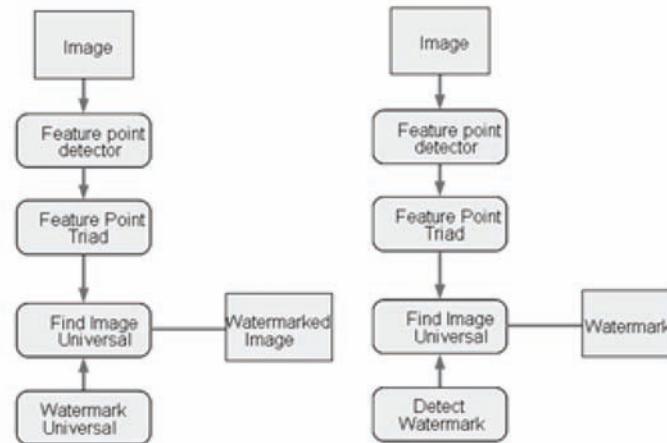
Figure 16. Illustration of the map from the watermarking zones to the Universal Images of lena



Figure 17. The UI's for a 40% cropping of lena (left) and a 15 degree rotation one (right)



Figure 18. The general paradigm



universal domains for each triangle can be given a different watermark.

Figure 19 shows an example of a watermark using a marking of lena using a simple block method. Our emphasis is not on any particular watermarking method but on the ability to endow any watermarking method with RST invariance. The more difficult step is the extraction phase.

The Extraction Phase consists of the following steps:

1. Using SIFT to get the Feature points.
2. Locate the watermarking triangle Δ .
3. Construct a UI from the triangle.
4. Extract the watermark
5. Validate the watermark.

In this phase we must be able to find the watermarking regions in an attacked image. If a geometric attack has been applied the basic triangle will have been rotated, scaled and translated. We need a method to identify two triangles, the

Figure 19. Illustration of using a simple block method



original and the attacked, that are related by an affine transformation. To do this we need to borrow some concepts from shape theory.

Shape Theory

Shape theory can be used in many areas, such as machine vision, image processing and computer vision. It is widely used in face recognition, tracking of regions and object boundaries in an image sequence. The basic idea of shape invariance can be described as follows: Shape invariants represent properties of geometric patterns, which remain unchanged while performing a class of transformations.

Consider a pattern or a set of k distinct points in the plane, where $k \geq 2$. Such a set is called a k -ad, where k -ads are considered to be on the d -complex plane \sum_d^k ; specifically, on the 2-di-

mensional complex space \sum_2^k . Hence, these k -ads will be denoted as k -complex numbers

$$z_j = (x_j + i y_j), \quad 1 \leq j \leq k. \quad (18)$$

We will now give some useful definitions and notes that are necessary for developing, understanding and utilizing the Shape Theory.

- **Definition:** The center or the centroid of a k -ad $z = (z_1, z_2, \dots, z_k) \in \sum_d^k$ is given by:

$$\bar{z} = \frac{1}{k} \sum_{i=1}^k z_i \quad (19)$$

- **Definition:** Translation of the k -ad z is done by moving its centroid to the origin.

- **Definition:** Rotation of the k -ad z by an angle θ and scaling it by a factor $\lambda > 0$ is achieved by multiplying $r = z - \bar{z}$ by the complex number $\lambda e^{i\theta}$.

Because the locations of the labels on the k -ad z are not important, we translate the k -ad z so that its centroid is located at the origin. Since the size of the k -ad z is not significant either, we may rescale it as $\frac{\bar{z}}{S}$ where:

$$S = \sqrt{\sum_{i=1}^k \|z_i - \bar{z}\|^2}. \quad (20)$$

- **Definition:** The space of k -ads is the space of complex lines on the complex hyper-plane:

$$T^{k-1} = \left\{ r \in C^k \setminus \{0\} : \sum_{j=1}^k w_j = 0 \right\} \quad (21)$$

The basic object for the translation and scaling is called the pre-shape.

- **Definition:** The quantity $u = \frac{z - \bar{z}}{\|z - \bar{z}\|}$ is called the *Pre-Shape* of the shape of k -ad z .
- **Definition:** The *shape* of the k -ad $z = (z_1, z_2, \dots, z_k)$ is the equivalence class, or the orbit, of z under translation, rotation and scaling. In other words, the shape of z is what it is left over after we remove the scaling, translation, and rotation of the k -ad z . The shape is denoted by

$$[z] = \{e^{i\theta} u \mid \theta \in [0, 2\pi]\} \quad (22)$$

- **Definition:** The *Shape Space* denoted by \sum_d^k consists of the set of all shape elements $[z]$. It is the space of all complex

lines through the origin in C^{k-1} . Hence, any two patterns of points or k -ads U_1 and U_2 will be considered to have the same shape if either of their pre-shapes can be transformed into the other by a rotation about their shared centroid. That means $[U_1] = [U_2]$.

Veronese-Whitney Mapping

In order to efficiently track the distinguished triangle Δ in the image under different affine attacks, such as rotation, cropping, or scaling, we utilize the idea of Veronese-Whitney Mapping (Bhattacharya & Bhattacharya, 2008). First, we give some useful definitions:

- **Definition:** Let V be a vector space with a Hermitian form $h : V \times V \rightarrow \mathbb{C}$. Then the space $H = (h, V)$ is called a *Hermitian Space*.
- **Definition:** The Veronese-Whitney embedding or mapping of \sum_2^k is given by:

$$\psi : \sum_2^k \rightarrow H \quad \text{defined by} \quad \psi([z]) = uu^*, \|u\| = 1 \quad (23)$$

where H is the space of all Hermitian matrices and:

$$u = \frac{z - \bar{z}}{\|z - \bar{z}\|} = \frac{r}{\|r\|}. \quad (24)$$

This maps the space of k -ads \sum_2^k to the space of Hermitian matrices H .

- **Definition:** The *Distance Function* ρ on \sum_2^k between U_1 and U_2 is given by

$$\rho(U_1, U_2) = \|U_1 U_1^* - U_2 U_2^*\|_H \quad (25)$$

where $\|\bullet\|_H$ is the standard Frobenius norm defined by

Figure 20. Matching triangles using the images of the triangles



$$\|M\|_H = \text{trace} (MM^*) \quad (26)$$

on the space of Hermitian matrices.

Locating the Watermark Δ

To locate the image of the basic triangle in a RST attacked image we use the following steps on the watermarked image.

1. Determine the prominent feature points
2. Construct all triangles with feature points as vertices
3. Use the Veronese-Whitney distance function to compare each triangle with Δ

Figure 20 illustrates how to find the image of a triangle in an original image.

We compute its image H under the Veronese-Whitney map together with the Veronese-

Whitney images H_i of the feature point triangulations of the rotated image. However, it is surprising how many nearly similar triangles can be formed from all the feature point vertices in an image. This is not a problem as one can check each triangle for watermarks. It is easier if the triangle is unique. One possible way to make this happen is to utilize a second triangle associated with the watermarking triangle. We

Figure 21. The triangle pair for lena, watermarking and ghost



define the “ghost triangle” \hat{H}_i to be the triangle with vertices that consist of the nearest feature point to each vertex of the watermarking triangle outside that triangle. The pair of “dual” triangles $D_i = (H_i, \hat{H}_i)$, $D_i = (H_i, \hat{H}_i)$ is much more likely to be unique than the single watermarking triangle. Figure 21 show a triangle pair for the lena image.

The normal distance algorithm is applied to the watermarking triangle to generate all candidate

Figure 22. The watermarking and ghost triangles identified for the lena image



triangles. The set of ghost triangles is then tested in the same way to see if they too are similar. This double requirement will usually result in the identification of a unique watermarking triangle candidate.

Figure 22 shows the recovery of both the watermarking triangle and its ghost in the watermark extraction stage. The algorithm is

$$H = \arg \min_i \hat{d}(H, H_i) \quad (27)$$

Where $\hat{d}(H, H_i) = d(H, H_i) + d(\hat{H}, \hat{H}_i)$ is the lift of the Veronese-Whitney distance the space of dual triangles. This allows the automation of the process of triangle recovery. Once the triangle has been located we apply the extraction procedure appropriate to the embedding method used. This is usually a similarity based method.

FUTURE RESEARCH DIRECTIONS

Video watermarking involves embedding cryptographic information derived from frames of digital video into the video itself. Ideally, a user viewing the video cannot perceive a difference between the original, unmarked video and the marked video, but a watermark extraction ap-

plication can read the watermark and obtain the embedded information. Because the watermark is part of the video, rather than part of the file format or Digital Rights Management (DRM) system, this technology works independently of the video file format or codec.

This watermarking algorithm optimizes for three separate factors:

1. **Robustness:** the ability of the watermark to resist attempts by an attacker to destroy it by modifying the size, rotation, quality, or other visual aspects of the video.
2. **Security:** the ability of the watermark to resist attempts by a sophisticated attacker to remove it or destroy it via cryptanalysis, without modifying the video itself.
3. **Perceptual fidelity:** the perceived visual quality of the marked video compared to the original, unmarked video.

Attackers commonly use geometric attacks against watermarked videos. Rotation is a common geometric attack. Rotating a marked video by 1° or 2° can render the watermark unreadable while not appreciably changing a user's viewing experience. Other geometric attacks include random bending, cropping, changes in contrast, time compression or expansion, or re-encoding

at a low bit rate. Sophisticated geometric attacks may include several or all of these.

There are also types of attack that are specific to video. For example there are the following attacks:

1. **Noise attack:** The watermarked video is corrupted by adding the uniform distributed noise with different intensity.
2. **Cropping attack:** Video watermark has similar cropping attack like image watermark. In our experiment, a part of each frame in the video has been cropped.
3. **Frame dropping attack:** For the existence of the inherent redundancy in video data, there is little change between frames in a shot. So, the frame dropping (frame cutting), which are some frames are removed from the video shot, is often used as an effective video watermark attack, since it leads little or no damage to the video signal.
4. **Frame averaging attack:** Frame averaging is another significant video watermarking attack. It is clear that the average of multiple frames will remove the dynamic composition of the watermark.
5. **Frame swapping attack:** Frame swapping can also destroy some dynamic composition of the video signal and video watermark.
6. **MPEG compression attack:** MPEG compression is one of the most basic attacks to video watermark. The video watermarking scheme must be robust against it.

In this section we will propose a way in which our image approach can be extended to the video realm. Video sequences are composed of consecutive still images, which can be independently processed by various image watermarking algorithms. Three-dimensional (3D) wavelet transforms are a good choice (Zhu et. al., 1999). There are three steps

Step 1: First the video is segmented into scenes. This is done with a scene-change detection algorithm (Doulaverakis, 2004). Figure 23 shows

some scene changing frames from the public domain video sample ‘foreman.avi’.

For example, if we take the bottom left frame we can determine watermark zones and universal images for it. These are shown in Figure 24.

By running through the frames in the scene we can automatically generate a set of base triangles one for each frame. This is done by a modification of our triangle location algorithm. We select in each frame the feature point triangle nearest in size to the triangle in the previous frame. Figure 25 shows an example of such process.

By selecting N frames from a single scene we can construct N triples of universal images. This gives us three image rectangles. Each is $L \times L \times N$ where $L \times L$ is the size of each universal image. These three image blocks are defined by an N -tuple of triangles $\{\Delta_i\}_{i=1}^N$. The dimensions L and N can be chosen to be dyadic powers.

We have constructed a transformation $\Phi_\alpha(S, \Delta) = (\varphi_\alpha(S_1, \Delta_1), \dots, \varphi_\alpha(S_N, \Delta_N))$ that maps a video scene S onto three rectangular prisms. We call these *universal video watermarking prisms*. We assemble these prisms into videos. Thus each video is reduced to a set of three small videos. These *universal videos* are what we watermark. They are a generalization of RST invariant universal images. The mapping from S to a triple of watermarking prisms is invertible as each of the maps φ_α is invertible. Any watermarking method can be applied. However, wavelet methods are well suited.

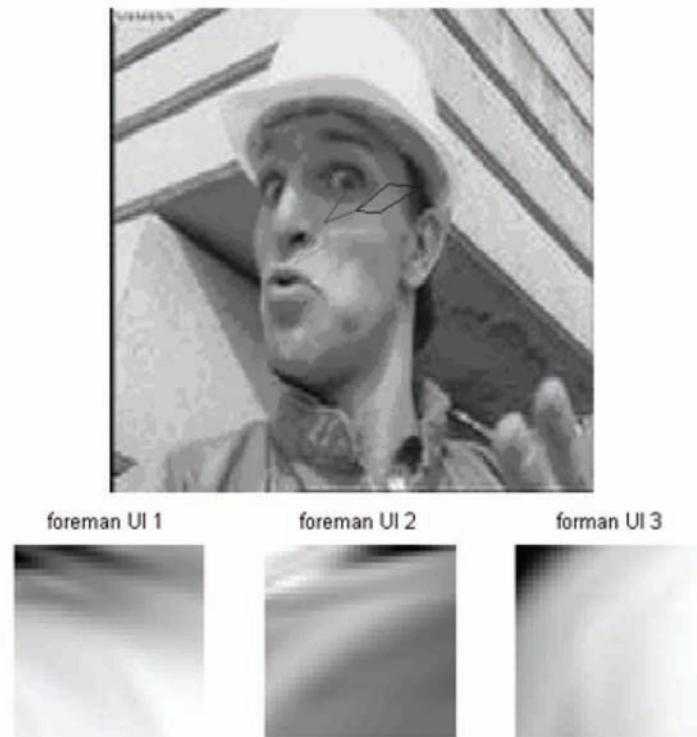
Step 2: Embed a watermark in each frame. For simplicity we use the simple watermarking method used in Eyadat, and El-Ddin, (2005).. The position of the watermark is approximately constant when there is little change in the video frames. Figure 27 shows some watermarked frames from the video sample ‘suzie.avi’.

In general, when there is more activity in a scene, the watermark move about the image. This is shown in Figure 28.

Figure 23. Scene breaks from 'foreman.avi'



Figure 24. The watermarking zones and universal images of a single from forman.avi



Feature Based Watermarking

Figure 25. An automated triangle allocation for a set of frames from 'foreman.avi'



Figure 26. The universal images of three frames from 'foreman.avi'



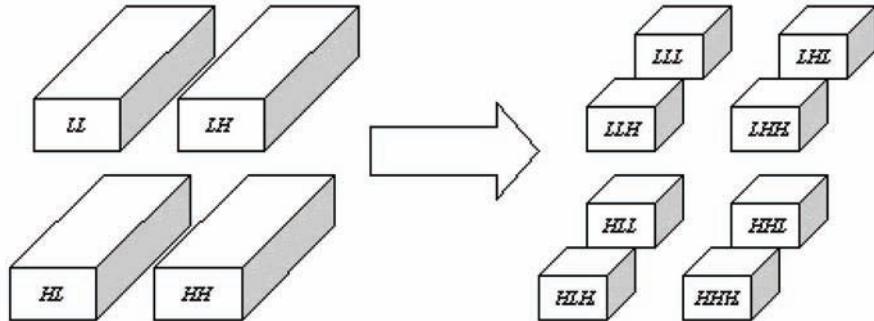
Figure 27. The frame, the watermarked frame and the watermark



Figure 28. The frame, the watermarked frame, and the watermark



Figure 29. The dyadic break up of a watermarking prism



3D Wavelets

To defend against non geometric attacks we have to move away from the picture of a video as a series of frames. We need to use its temporal nature. In this section we present an application of a 3D wavelet method applied to the *universal video watermarking prisms*. We use the 3D wavelet basis introduced by (Selesnick et al, 2001).

The situation is similar to the 2D case with subbands represented by rectangular prisms rather than planar squares. The filter bank is shown in Figure 30. In the 3D case, the 1D analysis filter bank is applied in turn to each of the three dimensions. In our example the universal pyramids are of size 64 by 64 by 128. After applying the 1D analysis filter bank to the first dimension we have two subband data sets, each of size 32 by 32 by 64. After applying the 1D analysis filter bank to the second dimension we have four sub-band data sets, each of size 32 by 32 by 128. Applying the 1D analysis filter bank to the third (temporal) dimension gives eight sub- band data sets, each of size 32 by 32 by 64. Figure 31 shows a slice of the wavelet transform of one universal pyramid of the ‘foreman.avi’ video.

In the 3D case, the 1D analysis filter bank is applied in turn to each of the three dimensions.

In our example the universal pyramids are of size 64 by 64 by 128. After applying the 1D analysis filter bank to the first dimension we have

two subband data sets, each of size 32 by 32 by 64. After applying the 1D analysis filter bank to the second dimension we have four sub-band data sets, each of size 32 by 32 by 128. Applying the 1D analysis filter bank to the third (temporal) dimension gives eight sub-band data sets, each of size 32 by 32 by 64. Figure 32 shows a slice of the wavelet transform of one universal pyramid of the ‘foreman.avi’ video.

The watermark can be embedded by the spread spectrum method in any of the rectangular prism subbands. The LLL subband is not used so as to decrease the visibility of the mark. We use the subbands HLH, HHL and HHH. Each of the subbands is divided into 8×8 blocks. In each block the watermark is embedded by using an additive spread spectrum method (Eyadat, 2005). Each wavelet coefficient w_i is replaced by w_i' given by $w_i' = w_i^k + \alpha_k r_i$ where $k \in \{HLH, HHL, HHH\}$. The quantity r_i is generated from a uniform distribution of zero mean and unit variance and the α_k are a constants. Computing the inverse wavelet transform completes the embedding in the original image. To extract the mark we compute the 3D wavelet transform of the watermarked image and extract the HLH, HHL and HHH subbands. From the 8×8 blocks we can extract the watermarking sequence r_i^* . The sequences $\{r_i^*\}$ and $\{r_i\}$ are compared using the standard similarly measure. If $SM(r, r^*) > T$ for some threshold T the

Figure 30. The 3D wavelet filter bank

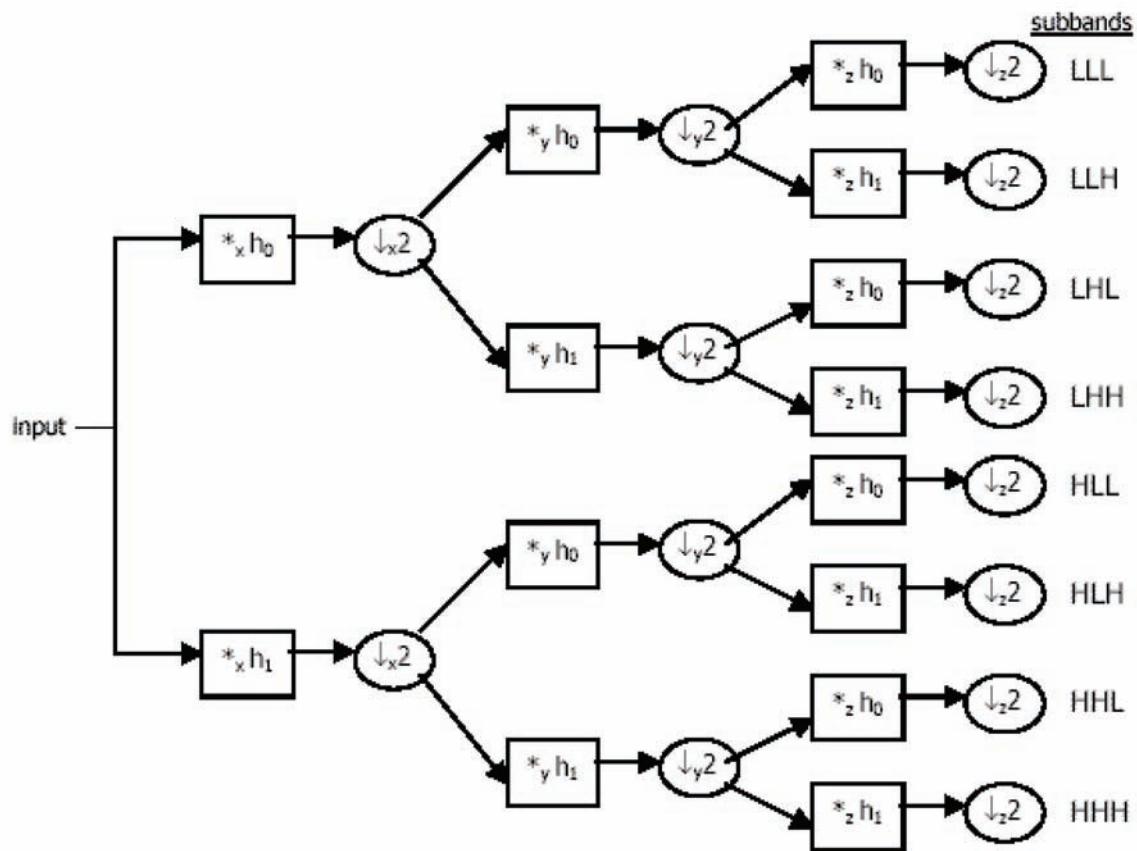


Figure 31. The 3D wavelet subbands of one slice of a universal pyramid

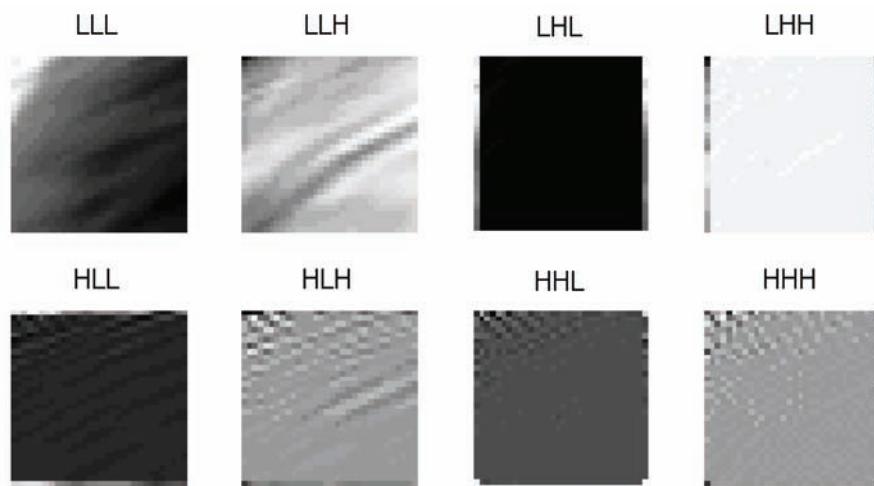
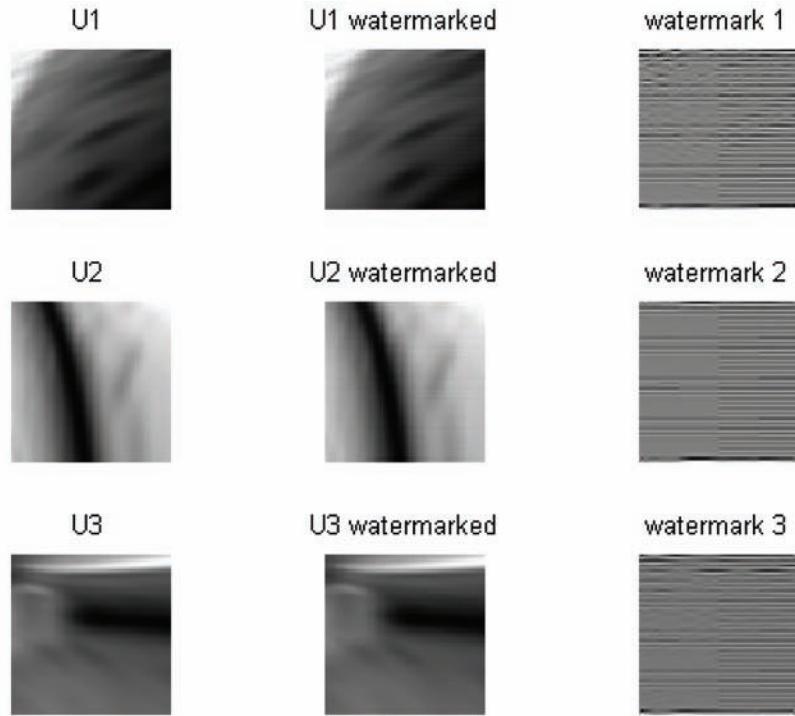


Figure 32. The watermark in a slice from the universal domain



watermark is found. Figure 32 shows how the watermark looks in the universal domain. When translated back to the original image domain the watermark appears as it does in Figures 27 and 28. The watermark is spread both spatially and temporally. There are three watermarks, one for each of the universal prisms. The presence of the watermark is determined with high accuracy with a threshold $T < 0.8$.

Watermarking a Relational Database

A video can be viewed as an image database containing the frames of the video. We are able to mark the individual entries because of their redundancy. The insensitivity of the HVS to certain types of information is heavily exploited. In a general relational database the problem is more difficult as we must be very cautious when altering entries as each one may need to stand alone. However, if we are cognizant of these problems we can use the

techniques from image and video watermarking and apply them to more general databases. In this section we will show this can be accomplished. As in the regular image and video situation there are those that will attack the watermark in order to cloud ownership. The primary attacks on database containing numeric data are:

1. **Subset Selection:** A subset of the data is randomly selected and subjected to attack.
2. **Subset Addition:** The attacker adds a set of numbers to the original data without altering the useful properties of the original data.
3. **Subset Alteration:** In this case the attacker alters a subset of the items in the original data set such that there is still value associated with the resulting set.

An essential capacity is to be able to identify a database element as having been changed either by a watermark or an attack. How do we charac-

terize the shape of a database component in order to locate a shape change?

1. Embedding Phase:

- a. Select a maximal number of unique, nonintersecting subsets of the original set, using some sort of secret key. This is the analog of selecting a set of robust feature triangles in a set of frames in a video scene. In the video case the specific triangles are the keys.
- b. For each considered subset, embed a watermark into it using some encoding convention. This is the analog of watermarking each of triangles we embedded in frames of a video scene.
- c. Check for data usability bounds. If usability bounds are exceeded, retry different encoding parameter variations or, if still no success, try to mark the subset as invalid. In the video case we check whether the watermarks can be recovered from which scenes. Those which are sensitive to recovery can be eliminated or marked as such.
- d. Repeat these steps until no more subsets are available for encoding. This results in multiple embeddings in the data.

2. Recovery Phase:

- a. Using the secret keys from embedding step (a), recover a majority of the subsets considered in (a), (or all if no attacks were performed on the data).
- b. For each considered subset, reconstruct watermarks.. The result of this is a set of copies of the same watermark with various potential errors.
- c. Use a set of error correcting mechanisms, such as majority voting schemes, to recover the highest likelihood initial mark from the results of step (b).

Watermarking an image or a collection of video frames requires us to have a process for

rediscovering those objects for recovery. We accomplished that in our feature based approach by using robust triangles. Watermarking a collection of data items also requires a similar ability to identify the relevant subsets before and after watermarking or security attack. This produces a resilient watermarking process. Consider the following simple example (Sion, 2004). Let S be a set of n real numbers $S = \{s_1, s_2, \dots, s_n\} \subset R$. The watermarking of S can be viewed as the problem of finding a transformation of S to another set \hat{S} such that, given all possible imposed usability metrics sets $G = \bigcup G_i$ for any subsets $S_i \subset S$ the metrics should hold also for \hat{S} . We call \hat{S} the watermarked version of S . In this example $\hat{S} = \{\hat{s}_1, \hat{s}_2, \dots, \hat{s}_n\} \subset R$ is obtained by making minor alterations to its content. Let a string of bits w of length $m \ll n$ be the desired watermark to be embedded into the data ($|w| = m$). Let $K = \{k_1, k_2, \dots, k_m\}$ be a set of m keys of n bits each. If we have secret key k_s we can segment the database S into subsets, S_i by sorting according to a cryptographic keyed hash of the most significant bits (MSB)

$$\text{index}(s_i) = H(k_s, \text{MSB}(\text{NORM}(s_i)), k_s)$$

Subsets S_i can now be constructed from “chunks” of the database, a “chunk” being a set of adjacent items in the sorted version of the collection. This provides resilience against the attacks by dispersing their effect throughout the data, as a result of the secret ordering. Like the triangles of our image and video techniques keys determine watermarking zones within the database. Once these zones have been identified a watermark can be embedded by an appropriate random algorithm. Suppose we want to embed a single bit b of the string w into a segment S_i . Let $v_{\text{false}}, v_{\text{true}}, c \in (0, 1)$, $v_{\text{false}} < v_{\text{true}}$ be real numbers. The number c is called a *confidence factor* and the interval $(v_{\text{false}}, v_{\text{true}})$ *confidence*

violators hysteresis. The triple (c, v_{false}, v_{true}) is part of the watermark definition. Let $avg(S_i)$ and $\delta(S_i)$ be the average and standard deviation, respectively, of S_i . Given S_i and the real number $c \in (0,1)$ define $v_c(S_i)$ to be the number of elements in S_i that are greater than $avg(S_i) + c \delta(S_i)$. Given a triple (c, v_{false}, v_{true}) define $mark(S_i) \in \{true, false, invalid\}$ by

$$mark(S_i) = \begin{cases} true & if \quad v_c(S_i) > v_{true} \times |S_i| \\ false & if \quad v_c(S_i) < v_{false} \times |S_i| \\ invalid & if \quad v_c(S_i) \in (v_{false} \times |S_i|, v_{true} \times |S_i|) \end{cases}$$

In other words, the watermark is modeled by the percentage of positive “confidence violators” present in S_i for a given confidence factor c and confidence violators hysteresis (v_{false}, v_{true}) . Encoding the single bit b , into S_i is achieved by making minor changes to some of the data values in S_i such that the number of positive violators $v_c(S_i)$ is such that $v_c(S_i) < v_{false} \times |S_i|$ if $b = 0$ and $v_c(S_i) > v_{true} \times |S_i|$ if $b = 1$. The chunks S_i are analogs of the 8×8 sub-images of an image watermarking method and the embedding method is clearly a variant of the spread spectrum Cox procedure.

CONCLUSION

This chapter surveyed existing methods and introduced a new alternative that called shape based watermarking.

There are two principle objectives of media watermarking. The most obvious concern is the protection of digital rights. In this case our concern rests in information about content ownership and intellectual property rights. The focus is on authentication which ensures that the original multimedia content has not been tampered with.

A fundamental basic of a typical watermarking system consists of two parts, a watermark embedder and a watermark detector. First gen-

eration watermarking schemes involve altering individual pixels values, either in the spatial or transformed data space. Common transforms are the discrete cosine transform and various wavelets transforms. The watermark is embedded in a series of sub-bands of the transform. The final watermark is spread over the entire data space of the original source. Consequently, these are known as spread-spectrum methods. These watermarks are subject to a number of watermark attacks. A class of attacks known as geometric, in which the source date is subject to signal processing methods such as compression, has proved to be difficult to defend against. Second generation watermarking has shifted attention away from individual data values to robust features in the data such as corner points. Processes that tamper with such features damage the content of the data and become easier to detect.

In shape based watermarking we emphasize new local coordinate systems based on polygonal shapes whose vertices are chosen from a set of robust features. We survey various ways in which a suitable set of feature points can be detected. Both the Harris detector and the SIFT approach are presented. Once we have a method of locating robust feature points we can introduce a new image transformation that is robust against geometric attacks. In so doing we introduce a number of results from mathematical shape-theory that have not previously be used in the watermarking realm. These methods are illustrated for images. This new methods also is applied to standard image processing based on a new image transform into an RST invariant domain. The new paradigm is for rending any watermarking scheme resistant to geometric attacks.

Furthermore in this chapter we proposed extensions of our technique to video watermarking and more general types of digital media by introducing an RST invariant map from a video scene to a set of *universal video watermarking prisms*. In this invariant domain we can embed a watermark by any method and assure RST invariance. Examples

of the new methods and how it can be generalized to the video realm are presented.

Recently, there has been an increasing interest in the extension of the watermarking audio, image, and video applications to relational databases. We survey the state of the art in this area and identify ways in which our new techniques might be applied. A generalized concept of shape is a clear direction in which the subject of watermarking is evolving.

REFERENCES

- Abdelnour, A. F., & Selesnick, I. W. (2001). Nearly symmetric orthogonal wavelet bases. In *Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing* (ICASSP).
- Arseneau, S. (2008). *Junction-Analysis*. Nevada, USA: VDM Verlag.
- Bas, P., Chassery, J., & Macq, B. (2002). Geometrically invariant watermarking using feature points. *IEEE Transactions on Image Processing*, 11(9). doi:10.1109/TIP.2002.801587
- Bhattacharya, A., & Bhattachary, R. (2008). Nonparametric statistics on manifolds with applications to shape spaces pushing the limits of contemporary statistics: contributions in honor of J.K. Ghosh. *IMS Collections*, 3, 282–301. doi:10.1214/074921708000000200
- Cox, I., Killian, J., Leighton, T., & Shamoon, T. (1996). Secure spread spectrum watermarking for images, audio and video. In *Proceedings of the IEEE Int. Conf. on Image Processing ICIP-96*, (pp. 243–246).
- Cox, I., Miller, M., & Bloom, J. (2002). *Digital Watermarking*. San Francisco: Morgan Kaufmann Publishers.
- Doerr, G., & Dugelay, J.-L. (2003). A guided tour to video watermarking. *Signal Processing Sig. Proc.: Image Comm.*, 18, 263–282. doi:10.1016/S0923-5965(02)00144-3
- Doulaverakis, C., Vagionitis, S., Zervakis, M., & Petrakis, E. (2004). Adaptive methods for motion characterization and segmentation of MPEG compressed frame sequence. In *1st Intern. Conference on Image Analysis and Recognition* (ICIAR'2004), *Proc. Part I*. Porto, Portugal. (LNCS 3211, pp. 310-317). Berlin: Springer Verlag.
- Eyadat, M., & El-Ddin, I. (2005). Compression Standards Roles in Image processing: Case Study. In *ITCC'05 (Vol. II*, pp. 135–140). Washington, DC: IEEE.
- Goodall, C., & Mardia, K. (1999). Projective shape analysis. *Journal of Computational and Graphical Statistics*, 8(2), 143–168. doi:10.2307/1390631
- Harris, C., & Stephens, M. (1988). A combined corner and edge detector. In *Proceedings Fourth Alvey Vision Conference*, (pp. 147-151).
- Jung, H.-S., Lee, Y.-Y., & Lee, S. (2004). Scene-based RST-resilient videowatermarking technique. *EURASIP Journal on Applied Signal Processing*, 14, 2113–2131. doi:10.1155/S1110865704405046
- Kendall, D., Barden, D., Carne, T., & Le, H. (1999). *Shape and Shape Theory*. New York: Wiley.
- Kitchen, L., & Rosenfeld, A. (1982). Gray-level corner detection. *Pattern Recognition Letters*, 1(2), 95–102. doi:10.1016/0167-8655(82)90020-4
- Kundur, D., Su, K., & Hatzinakos, D. (2004). Digital Video Watermarking: Techniques, Technology and Trends. In Pan, P. J.-S., Huang, H.-C., & Jain, L. (Eds.), *Intelligent Watermarking Techniques* (pp. 265–314). Singapore: World Scientific Publishing Company.

- Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, 60(2), 91–110. doi:10.1023/B:VISI.0000029664.99615.94
- Morris, H., & Muhi El-din, I. (2008). A new image transform. In *Proceedings of IPV08*.
- Morris, H., & Muhi El-Ddin, I. (2007). Feature frame watermarking. In *Proceedings of the 41 st Annual Asilomar Conference on Signals, Systems, and Computers*, (pp. 565-569).
- Muhi El-Ddin, I., Morris, H., & Eyadat, M. (2008). Watermarking: Anew approach. In *Proceedings of the Fifth International Conference on Information Technology: New Generations*, (pp. 795-800).
- Petitcolas, F., Anderson, R., & Kuhn, M. (1998). Attacks on copyright marking systems. In *Proceedings of the Second International Workshop on Information Hiding*, (LNCS1525, pp. 219–239).
- Ruanaidh, J. J. K., & Rotation, T. P. (1998). Scale and translation invariant spread spectrum digital image watermarking. *Signal Processing*, 66(3), 303–317. doi:10.1016/S0165-1684(98)00012-7
- Shi, J., & Tomasi, C. (1994). Good features to track. In *Proceedings of the IEEE Conference of ComputerVision and Pattern Recognition (CVPR '94)*.
- Sion, R., & Atallah, M. (2004). *Fellow, Rights Protection for Relational Data* (Vol. 16). IEEE Transactions on Knowledge and Data Engineering.
- Sparr, G. (1996). *Proceedings of the 13th International Conference on Pattern Recognition (Vienna)*, (pp. 328-333). Washington, DC: IEEE Compute. Soc. Press.
- Strang, G., & Nguyen, T. (1996). *Wavelets and Filter Banks*. New York: Wellesley-Cambridge Press.
- Tovée, M. J. (2008). *An Introduction to the Visual System Edition: 2*. Cambridge, UK: Cambridge University Press.
- Voloshynovskiy, S., Pereira, S., Iquise, V., & Pun, T. (1988). Attack modeling: towards a second generation watermarking benchmark. *Signal Processing*, 81, 1177–1214. doi:10.1016/S0165-1684(01)00039-1
- Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J., & Su, J. (2001). Attacks on Digital Watermarks: Classification, Estimation-based Attacks and Benchmarks. *IEEE Communications Magazine (Special Issue on Digital watermarking for copyright protection: a communications perspective)*, 39(8), 118-127.
- Zheng, D., Zhao, J., & El Saddik, A. (2003). RST invariant digital image watermarking based on log-polar mapping and phase correlation. *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Authentication, Copyright Protection and Information Hiding*, 13(8), 753–765.
- Zhu, W., Xiong, Z., & Zhang, Y.-Q. (1999). Multiresolution watermarking for images and video. *IEEE Trans. Circuits and Systems for Video Technology*, 9(4), 545–550. doi:10.1109/76.767121

ADDITIONAL READING

- Al-Haj, A., & Odeh, A. (2008). Robust and blind watermarking of relational database systems. *Journal of Computer Science*, 4(12), 1024–1029. doi:10.3844/jcssp.2008.1024.1029
- Bas, P., Chassery, J., & Macq, B. (2002). Geometrically invariant watermarking using feature points. *IEEE Transactions on Image Processing*, 11(9), 1014–1029. doi:10.1109/TIP.2002.801587

- Belkacem, S., Dibi, Z., & Bouridane, A. (2007). A masking model of HVS for image watermarking in the DCT domain. *14th IEEE International Conference on Electronics, Circuits and Systems*. Volume, 330 – 334
- Bhattacharya, A., & Bhattacharya, R. (2006) “Statistics on Riemannian Manifolds with applications to the Planer shape space”.
- Blanco-Silva, F. (2007) “The Curvelet Transform. A generalized definition and approximation properties”. Doctoral dissertation, Purdue University, Indiana, USA.
- Call, B., Beardy, R., & Taylor, C. (2006) “Obstacle avoidance for unmanned air vehicles using image feature tracking’. *AIAA Guidance, Navigation, and Control Conference*.
- Campisi, P., & Neri, A. (2005). Video watermarking in the 3D-DWT domain using perceptual masking. *IEEE International Conference on Image Processing*, Volume 1, 997-1000
- Candès, E. J. (2003). What is a curvelet? *Notices of The AMS*, 50, 1402–1403.
- Candès, E. J., & Demanet, D. L. (2005). The curvelet representation of wave propagators is optimally sparse. *Communications on Pure and Applied Mathematics*, 58(Issue 11), 1472–1528. doi:10.1002/cpa.20078
- Candès, E. J., Demanet, D. L., Donoho, D., & Ying, L. (2006). “Fast discrete curvelet Transforms”. Multiscale modeling & simulation (MMS). *Society for Industrial and Applied Mathematics*, 5(Issue 3), 861–899.
- Candès, E. J., & Donoho, D. L. (2005). Continuous curvelet transform: II. Discretization and frames. *Applied and Computational Harmonic Analysis*, 19(Issue 2), 198–222. doi:10.1016/j.acha.2005.02.004
- Candès, E. J., & Donoho, D. L. (2005). Continuous curvelet transform: I. Resolution of the wave-front set. *Applied and Computational Harmonic Analysis*, 19(Issue 2), 162–197. doi:10.1016/j.acha.2005.02.003
- Chen, Q., & Huang, T. S. (2000). Blind digital watermarking for images and videos and performance analysis. *In Proc. ICME*, 178. New York
- Choong-Hoon Lee, C.-H., Lee, H.-K., & Deajon, Y.-G. (2005). Geometric attack resistant watermarking in wavelet transform domain. *Optics Express*, 13(4), 1321.
- Coria, L., Nasiopoulos, P., & Rabab, W. (2006). A Robust Content-Dependent Algorithm for Video Watermarking, *Proceedings of the ACM workshop on Digital rights management*. 97-101. ACM.
- Cox, I. Miller, M., & Bloom, J. (2002). Digital Watermarking. New Jersey: Morgan Kaufmann.
- Demanet, L., & Yingz, L. (2007). *Curvelets and Wave Atoms for Mirror-Extended Images* (Vol. 6701). Proceeding SPIE.
- Dugelay, J., Roche, S., Rey, C., & Doerr, G. (2006). Still-image watermarking robust to local geometric distortions. *IEEE Transactions on Image Processing*, 15(9). doi:10.1109/TIP.2006.877311
- Elbasi, E. (2008). *Multimedia Security: Digital Image and Video Watermarking*. New York: VDM Verlag.
- Ettinger, S. 2002. SIFT Matlab Implementation, Intel. <http://robots.stanford.edu/cs223b/Matlab-SIFT.zip>
- Eyat, M. “unpublished Ph.D. Thesis” Claremont Graduate University, Claremont Graduate University, May 2005.
- Forssén, P.-E., & Lowe, D. G. (2007). “Shape descriptors for maximally stable extremal regions”, *International Conference on Computer Vision (ICCV)*, Rio de Janeiro, Brazil.

- Goswami, J. C., & Chan, A. K. (1999). *Fundamentals of Wavelets Theory, Algorithms, and Applications*. New York: John Wiley & Sons, Inc.
- Inglis, L. A. (1999). *Video Engineering*. New York: McGraw-Hill.
- Kejariwal, A., Gupta, S., Nicolau, A., Dutt, N., & Rajesh Gupta, R. (2004). Proxy-based task partitioning of watermarking algorithms for reducing energy consumption in mobile devices. *Proceedings of the 41st annual conference on Design automation*. 166-174.
- Kenney, C. S., Zuliani, M., & Manjunath, B. S. (2005) “An Axiomatic Approach to Corner Detection”. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)* - Volume 1, 191-197.
- Kwok, S. H., Yang, C. C., & Tam, K. Y. (2007). “Watermark Design Pattern for Intellectual Property Protection in Electronic Commerce Applications”, *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Vol. 2.
- Lu, W., Lua, H., & Fu-Lai Chung, F.-L. (2006). Feature based watermarking using watermark template match. *Applied Mathematics and Computation*, 177(Issue 1). doi:10.1016/j.amc.2005.11.015
- Luther, A., & Inglis, A. (1999). *Video Engineering*. New York: McGraw-Hill.
- Majumdar, A. (2007). “Bangla Basic Character Recognition Using Digital Curvelet Transform”. *Journal of Pattern Recognition Research*, (1) 17-26.
- Manay, S., Cremers, D., & Hong, B.-W. Yezzi, A. J. & Soatto, S. (2006). “Integral Invariants for Shape Matching”. *IEEE Transactions On Pattern Analysis And Machine Intelligence*, Vol. 28, No. 10.
- Mizuki Tone, M., & Hamada, N. (2005). “Affine Invariant Digital Image Watermarking Using Feature Points”. *RISP International Workshop on Nonlinear Circuit and Signal Processing (NCSP'05)*, Hawaii, USA.
- Ng, K. S., & Cheng, L. M. (1999). “ Selective block assignment approach for robust digital image watermarking”, *Proceedings of the SPIE/IS&T International Conference on Security and Watermarking of Multimedia Contents*, vol. 3657, San Jose, CA.
- Nunziati, W., Sclaroff, S., & Bimbo, A. D. (2005) “An Invariant Representation for Matching Trajectories across Uncalibrated Video Streams”. *International Conf. on Image and Video Retrieval*.
- Omer, I., & Werman, M. (2006). “Image Specific Feature Similarities”. *In Proceedings of ECCV* (2). 321-333.
- Parameswaran, L. (2008). *Content-based watermarking for image authentication using independent component analysis*.
- Pröfrock, D., Schlauweg, M., & Müller, E. (2007). *Content-Based Watermarking by Geometric Warping and Feature-Based Image Segmentation* (Vol. 37). Signal Processing for Image Enhancement and Multimedia Processing.
- Qian, S. (2002). *Introduction to Time-Frequency and Wavelet Transforms*. New Jersey: Prentice Hall.
- Qiang, C., & Huang, T. S. (2000) Blind digital watermarking for images and videos and performance analysis. *IEEE International Conference on Multimedia*. Volume 1,389 – 392.
- Raghavan, S. V., & Tripathi, S. K. (1998). *Networked Multimedia Systems concepts, Architecture, and Design*. New Jersey: Prentice Hall.

- Rao, K. R., Bojkovic, Z. S., & Milovanovic, D. A. (2002). *Multimedia Communication Systems Techniques, standards, and networks*. New Jersey: Prentice Hall.
- Sharda, N. K. (2002). *Multimedia Information Networking*. New Jersey: Prentice Hall.
- Solari, S. J. (1997). *Digital Video and Audio Compression*. New York: McGraw-Hill.
- Symes, P. (2001). *Video Compression Demystified*. New York: McGraw-Hill.
- Taylor, F., & Mellott, J. (1998). *Hands-On Digital Signal Processing*. New York: McGraw-Hill New York.
- Vinod, P., Gwenaël, D., & Bora, P. K. (2006). Assessing Motion-Coherency in Video Watermarking. *Proceedings of the 8th workshop on Multimedia and security*. 114-119. ACM.
- Vladimir Balan & Vic Patrangenaru. (2006). “Geometry of Shape Spaces”. *The Fifth Conference of Balkan Society of Geometers*, 28-33. Mangalia, Romania.
- Weinheimer, J. (2006). “Towards A Robust Feature-Based Watermark”. *IEEE International Conference on Image Processing*, Atlanta, GA, 1401-1404.
- Zheng, S. Zhu, Y. & Wang, X. (2008). A New RST-Invariant Watermarking Scheme Based on Texture Features. *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia*. ICST
- Ziad Sakr, Z., & Georganas, N. D. (2007). Robust Content-Based MPEG-4 XMT Scene Structure Authentication and Multimedia Content Location. *Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP)*, Volume 3 Issue 3, article, 18, 1-23. ACM.
- Zou, F., Lu, Z., & Ling, H. (2004). A Multiple Watermarking Algorithm Based on CDMA Technique. *Proceedings of the 12th annual ACM international conference on Multimedia* 424-427. ACM.

KEY TERMS AND DEFINITIONS

Cryptographic Hash: A cryptographic hash function is an irreversible procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. Hashes, compile a stream of data into a small summarized form. Hashes are different from encryption in that hashing cannot be reversed. Their role is to provide an indication of whether a data stream has been tampered with.

Feature Points: Locations that have properties that allows them to be identified in a digital object even when it ha been subjected to attacks. For example, in an image, it is features such as corners, line intersections. Feature points are categorized according to their robustness.

Geometric Attacks: Affine attacks attempt to destroy the synchronization of the watermark signals embedded in original image by introducing global and local changes to the image coordinates. Image processing techniques such as rotation, scaling, cropping and compression are examples.

Invariant Domain RST: An acronym for Rotation Scaling and Translation. These are the primary geometric attacks on images where they appear as image rotation, resizing and cropping.

Shape Theory: This is the analysis of geometric shapes. It is concerned with algorithms to detect similarly shaped objects represented in digital form. Examples are boundary representation of an object in an image or video frame; specific subsets in a segmentation of a relational database; point cloud representations.

SIFT: An acronym for Scale-invariant feature transform SIFT is an algorithm to detect and describe local features in images. It is based on a Difference of Gaussian (DOG) image pyramid technique.

Spatial Domain: This term comes from Digital Signal Processing (DSP) where it refers to the measurement space of the signal, usually a set of intensity values. Its primary use is to distinguish that representation from say the Frequency Domain in which the signal is represented by its frequency content. For example, a grayscale image is changed from its Spatial Domain (pixel values) to its Frequency Domain (image frequencies) description by a Fourier Transform.

Transform Domain: The coordinate space in which a signal is measured (Spatial Domain) is not

the best for extracting particular characteristics. Often a transform such as a Fourier or Wavelet Transform is applied. The spaces of Fourier or Wavelet coefficients are examples of Transform Domains.

Universal Domain: This is a Transform Domain in which is invariant with respect to particular types of transformation (attacks) are applied to the Spatial Domain of a digital object.

Watermarking Schema: A process inserts a pattern of bits inserted into a digital data of image, audio or video file for authentication purposes and it must be robust against any attacks such image processing, etc

Chapter 13

Techniques for Multiple Watermarking

Abdellatif Zaidi
Université Catholique de Louvain, Belgium

1. ABSTRACT

The watermarking problem is relatively well understood in the single watermark case, but it lacks theoretical foundation in the multiple watermarks case. The goal of this chapter is to provide important technical insights as well as intuitive and well developed discussions onto how multiple watermarks can be embedded efficiently into the same host signal. The authors adopt communication and information theoretic inclinations, and they argue that this problem has tight relationship to conventional multiuser information theory. Then they show that by virtue of this tight relationship design and optimization of algorithms for multiple watermarking applications can greatly benefit from recent advances and new findings in multiuser information theory.

2. INTRODUCTION

Digital media has become an integral part of modern lives. Whether surfing the web, watching satellite television, playing a digital video disc, or listening to digital music, a large part of our professional and leisure time is filled with all things digital. This is the basis for modern scientific and economic developments which is centered around the distribution of digital data to a worldwide audience. However, the replacement of analog media by their digital

counterparts together with the explosion of the high speed internet and wireless networks has had also a perhaps unintended consequence. It has also become relatively easy to illegally use and redistribute media at will. Securing the data exchanged in a networked media environment against copyright violation, unauthorized usage and illegal redistribution is thus a central and at time critical issue. This is because traditional means of network security consisting, e.g., in firewalls, virtual private networks and intrusion detection systems can hardly cope with security issues when used as stand-alone technologies. Additional security-assisting functionalities relying on

DOI: 10.4018/978-1-61520-903-3.ch013

watermarking and data hiding and techniques are highly instrumental in this trend (Voloshynovskiy, Deguillaume, Koval, and Pun, 2003).

Watermarking consists in inserting unperceived data in a signal (referred to as cover or carrier signal) in an attempt to establish ownership, usage rules or track media redistribution. It gained importance in the mid 1990s mainly as a potential solution for digital rights management. The key aspects of watermarking that make it attractive are the imperceptibility of the embedded data, its statistical covertness and its ability to withstand channel degradations, including several cycles of digital-to-analog and analog-to-digital conversions and various signal processing operations. These two conflicting requirements are often called *robustness* and *transparency* requirement, respectively.

Much of prior work on watermarking and data hiding concentrated on designing one single watermark with prescribed requirements. This is suitable for applications such as copyright protection where the embedding of just a few bits of information expected to be detectable with very low probability of false alarm is sufficient to serve as an evidence of copyright (Swanson, Kobayashi, and Tewfik, 1998). However, in many other practical situations this might be not sufficient and one might need to embed more than one watermark into the same host. Such situations are referred to as **multiple watermarking**. The problem of inserting multiple watermarks into a digital media has been introduced in the literature in the pioneering work by Mintzer and Braudaway (1999). Then, there has been a growing body of works focusing on multiple watermarking techniques, algorithms and limitations (see, e.g., Cox et al., 1997; Liu et al., 2004; Khisti et al., 2007; Zaidi et al., 2007, 2009).

The problem of watermarking is relatively well understood in the single watermark case (Chen and Wornell, 2001; Moulin and O’Sullivan, 20003), but it lacks theoretical foundation in the multiple watermarks case. The goal of this chapter is to

provide technical ground and insights onto how multiple watermarks can be embedded efficiently into the same host signal. We adopt communication and information theoretic inclinations, and we argue that this problem has tight relationship to conventional multiuser information theory. Then we show that by virtue of this tight relationship design and optimization of algorithms for multiple watermarking applications can greatly benefit from recent advances and new findings in multiuser information theory. Harnessing information-theoretic tools to the investigation of the problem of multiple watermarking not only provides a yardstick by which the efficiency of this technique can be measured, but in fact provides the right guidance to the appropriate design of efficient embedding schemes in practice.

This chapter is organized as follows. After introducing the notation we give a brief review of existing literature in Section II. Then we describe in Section III the formal statement of the watermarking problem viewed as a communication problem with side information known only at the transmitter; in this section we also review some sub-optimal but practical coding schemes which are by now well known for the single watermark case. In Section IV we turn to present, and discuss, two mathematical models for multiple watermarking. In Section V, we discuss coding in practice for the studied models and we analyze the corresponding performance. Finally, we close with some concluding remarks in Section VI.

NOTATION

Throughout the paper, boldface fonts denote vectors. We use uppercase letters to denote random variables or vectors (e.g., $\mathbf{X} = (X_1, X_2, \dots, X_n)$), lowercase letters for their realizations (e.g., $\mathbf{x} = (x_1, x_2, \dots, x_n)$) and calligraphic fonts for sets (e.g. \mathcal{X}). Unless otherwise specified, vectors are assumed to be in the n-dimensional Euclidean space ($\mathbb{R}^n, \|\cdot\|$) where $\|\cdot\|$ denotes the Euclidean

norm of vectors. For a random vector \mathbf{X} , we use $E_{\mathbf{X}}[\cdot]$ to denote the expectation taken with respect to \mathbf{X} and $P_{\mathbf{X}}(\cdot)$ to denote the probability distribution of \mathbf{X} . A random vector \mathbf{X} with conditional probability distribution given \mathbf{S} is denoted by $\mathbf{X} | \mathbf{S}$. The Gaussian distribution with mean μ and square deviation σ^2 is denoted by $\mathcal{N}(0, \sigma^2)$. The identity matrix is denoted by I . For random vectors, \mathbf{X}, \mathbf{U} and \mathbf{S} , the notation

$$\begin{aligned}\mathbf{U} | \mathbf{S} &\sim \mathcal{N}(\alpha\mathbf{S}, PI) \\ \mathbf{X} &= \mathbf{U} - \alpha\mathbf{S},\end{aligned}$$

is used to mean that \mathbf{X} is i.i.d. Gaussian with power P , i.e., $\mathbf{X} \sim \mathcal{N}(0, PI)$, independent of \mathbf{S} and \mathbf{U} is generated as $\mathbf{U} = \mathbf{X} + \alpha\mathbf{S}$ for some scalars α and P . Throughout the paper, the logarithm function is to the base 2.

3. BACKGROUND ON MULTIPLE WATERMARKING

For long time, the use of watermarking techniques has been restricted to the embedding of one single watermark. The idea of inserting multiple watermarks into a digital media has been first proposed and discussed by Mintzer and Braudaway (1999). In that work, Mintzer and Braudaway ask: “if one watermark is good, are more better?”. The question is relevant indeed as it is not clear whether different watermarks can be embedded into the same media without altering each other. Cox et al. (1997) extend algorithms that are designed for the embedding of one watermark to the case of multiple watermarks which are chosen to be nearly orthogonal. Wong et al. (2004) study embedding different watermarks sequentially using the same key. For a comprehensive overview of the earliest multiple watermarking techniques, which are mostly derived from the designer’s experience, the reader may refer to the work by Wong et al.

(2003). More systematic recent studies with a deeper emphasis on embedding aspects from a coding angle have appeared recently (Liu et al., 2004; Khisti et al., 2007; Zaidi et al., 2007, 2009).

In multiple watermarking, different watermarks can be used for different purposes, i.e., intended for different usages. These watermarks may or may not have different robustness and transparency requirements. Thus, each watermark can be asked to be robust, *semi-fragile* or *fragile* depending only on the desired usage and not on other watermarks. In the scope of watermarking of medical images, we may wish to store the patient information into the corresponding image in a secure and private way (this information is sometimes called the “annotation part” of the watermark and, hence, is required to be sufficiently robust) together with a possibly fragile “tamper detection part” which serves to detect tampering. Also, in the scope of proof-of-ownership applications, we may wish to use two watermarks: one watermark is destined to convey ownership information and so it should be robust, and the other one is used to check for content integrity and so it should be semi-fragile or even fragile.

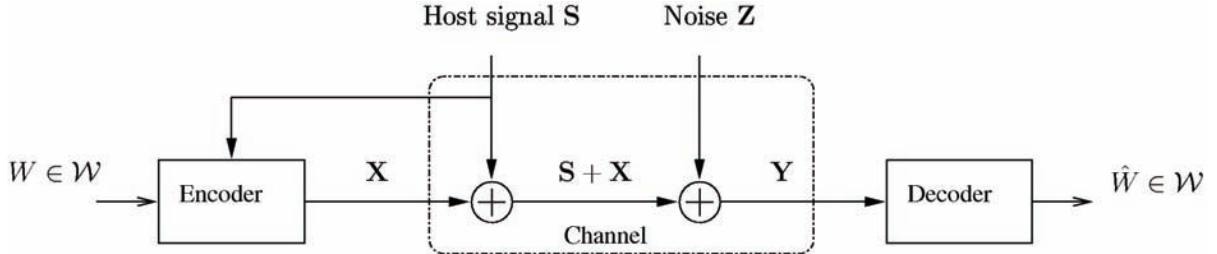
4. WATERMARKING AS DIRTY PAPER CODING

In this section, first we give a brief review of the additive Gaussian watermarking problem viewed as dirty paper coding. Next, we briefly review the now well-known practical implementations scalar Costa scheme (SCS), (Eggers, Bauml, Tzschoppe, and Girod, 2003) and quantization index modulation (Chen and Wornell, 2001).

Watermarking Viewed as Side-Informed Communication

Figure 1 depicts a block diagram of the problem of blind watermarking. An embedder embeds

Figure 1. Blind watermarking viewed as dirty paper coding over a Gaussian channel (©IEEE 2007. Used with permission)



some data (or message) m into the host signal S in an imperceptible manner, so as to serve as watermark. The watermarked content may then be transmitted, stored, or simply processed in some way, intentionally (i.e., by an attacker) or non-intentionally. The decoder does not know the host signal and has to decode the embedded message from the received signal. The message m can be represented by a sequence $\{W\}$ of M -ary symbols, $W \in \{1, \dots, M\}$, so that the embedding of message m amounts to that of the sequence of symbols $\{W\}$. Thus, in the rest of this chapter, we will loosely refer to each symbol W as being a “message”.

The embedding process consists in encoding the message W into a signal called the “embedded signal” or “watermark”, which the embedder then adds to the host signal. The embedding rate R , expressed in number of bits per host sample that the encoder can embed reliably, is such that $M \approx 2^{nR}$. For imperceptibility reasons, embedding should not introduce any perceptible distortion to the host signal; and this imposes an embedding power constraint of the form $E[\|X^2\|] \leq nP$. Also, the embedded signal must survive certain channel degradations, including some common incidental and intentional attacks

The watermarking problem shown in Figure 1 can be viewed as a communication problem with side information (SI) known non-causally at the transmitter but not at the receiver (Cox, Miller, and McKellips, 1999); the **side information**

being the cover signal, the transmitter being the embedder and the transmission rate being given by the embedding rate. In this model, the SI acts as interference for the transmission of the message. For the i.i.d. Gaussian case, the relevant work is Costa’s “writing on dirty paper”, adeptly known as **dirty paper coding** (DPC), (Costa, 1983). More specifically, if the SI S and the noise Z are independent and i.i.d. Gaussian, with $S \sim \mathcal{N}(0, QI)$ and $Z \sim \mathcal{N}(0, QI)$. Costa was the first to show the remarkable result that the additive Gaussian interference S which is known non-causally only to the transmitter, incurs no loss in capacity relative to the standard interference-free additive white Gaussian noise (AWGN) channel, i.e.

$$C = \frac{1}{2} \log(1 + \frac{P}{N}). \quad (1)$$

The achievability proof is based on a random binning argument for general channels with non-causal state information (Gel’fand and Pinsker, 1980). It uses a random construction of a Gaussian codebook and a random partition of the codewords of this codebook into “bins”. Costa showed that with the choice of the input distribution as

$$\begin{aligned} \mathbf{U}|S &\sim N(\alpha S, PI) \\ \mathbf{X} &= \mathbf{U} - \alpha S \end{aligned} \quad (2)$$

where \mathbf{U} is an auxiliary random vector and $\alpha = P / (P + N)$, one achieves the interference-free capacity (1) regardless of the power of the interference \mathbf{S} . This DPC, however, is not feasible in practice due to the huge random codebook which is needed to perform binning. Earlier DPC-based implementations sub-optimally set the signal \mathbf{S} to be an appropriate scaled version of the quantization error of the host signal \mathbf{S} . Quantization can be scalar-valued (Chen and Wornell, 2001; Eggers et al., 2003) or vector-valued (Zamir, Shamai and Erez, 2002; Fischer, 2005).

Review of Some Embedding Schemes for One Watermark

Following Costa's ideal DPC, Chen and Wornell (2001) proposed the use of structured quantization-based codebooks. The resulting embedding scheme is referred to as quantization index modulation (QIM). Also, Eggers et al. (2003) designed a practical "scalar Costa scheme" (SCS) where the random codebook \mathbf{U} is chosen to be a concatenation of dithered scalar uniform quantizers. The watermark signal is a scaled version of the quantization error, i.e,

$$x_k = \tilde{\alpha} \left(Q_{\Delta} \left(s_k - \frac{W}{M} \Delta \right) - \left(s_k - \frac{W}{M} \Delta \right) \right), \quad (3)$$

with $\Delta = \sqrt{12P} / \tilde{\alpha}$, $\tilde{\alpha} = \sqrt{P / (P + 2.71N)}$ and Q_{Δ} is the uniform scalar quantizer with constant step size Δ . The decoding also is based on scalar quantization of the received signal $\mathbf{y} = \mathbf{x} + \mathbf{s} + \mathbf{z}$ followed by a thresholding procedure. More precisely, the estimate \hat{W} of the embedded message W is the closest integer to $r_k M / \Delta$, with $r_k = Q_{\Delta}(y_k) - y_k$; and the optimum choice for the inflation parameter $\tilde{\alpha}$ is $\tilde{\alpha} = \sqrt{P / (P + 2.71N)}$, obtained by numerically maximizing Shannon mutual information $I(W; r)$

With this setting, SCS performs close to the optimal DPC. Comparatively, the aforementioned QIM, which corresponds to the inflation parameter set to unity, is less efficient, especially at high noise levels. This QIM embedding function is referred to as *regular* QIM and can be slightly modified so as to increase its immunity to noise. The resulting scheme, called *distortion-compensated* QIM (DC-QIM), corresponds to $\pm = P / (P + N)$ and performs very close to SCS.

5. MATHEMATICAL MODELS FOR MULTIPLE WATERMARKING

In what follows, referring to conventional communication, we loosely use the term "multiple user" to refer to the situation in which several messages $\{W_i\}$ have to be embedded into the same cover signal \mathbf{S} . The embedding may or may not require different robustness and transparency requirements. This means that the embedding of each of these messages can be independently asked to be *robust*, *semi-fragile* or *fragile*. Also, depending on the target application, the watermarking system may require either joint or separate decoding. For joint decoding, think of one single *trusted* authority checking for several watermarks at once. For separate, or distributed, decoding, think of several authorities each checking for its own watermark; or the same authority checking for the same watermark but using different noisy contents (e.g., think of a watermarked image being transmitted over a mobile network, with watermarking verification performed at different nodes of this network). Also, like the decoding process, we may wish that the encoding of the different messages be performed either jointly or separately. Simple practical situations where joint/separate encoding is preferred may be obtained by just reversing the roles of the embedders and the decoders in the aforementioned examples.

We will consider two scenarios of multiple watermarking which we will recognize as being equivalent to communication over a degraded broadcast channel (BC) and a multiaccess channel (MAC) respectively. These scenarios are relevant in practice.

A Broadcast Setup for Multiple Watermarking

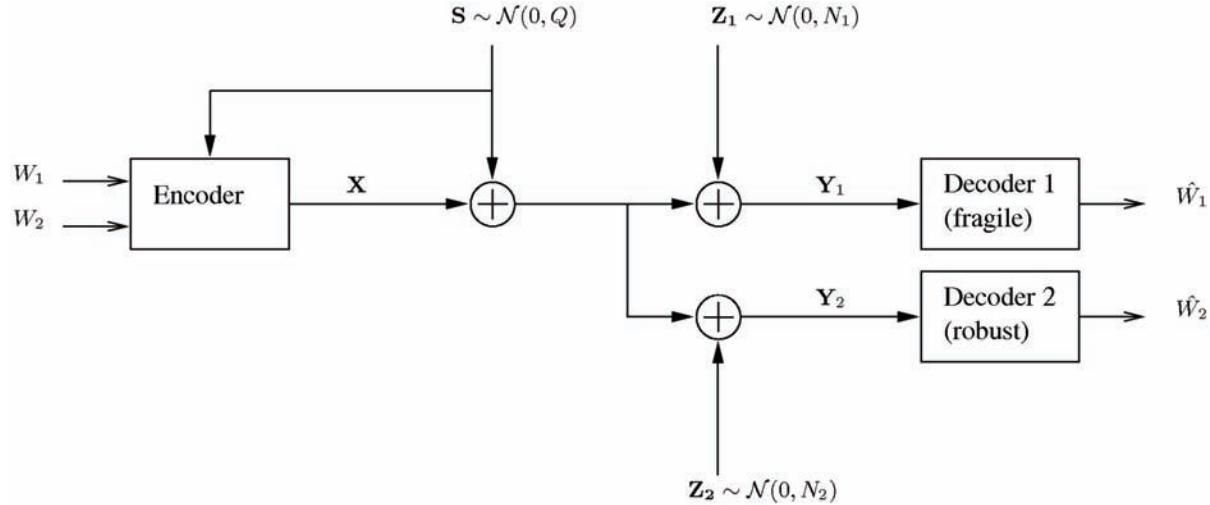
Consider a watermarking system aiming at embedding two messages W_1 and, W_2 assumed to be M_1 -ary and M_2 -ary respectively, into the same cover signal $\mathbf{S} \sim \mathcal{N}(0, QI)$. We suppose that one single *trusted authority* (i.e., the same encoder) has to embed these two messages; and that embedding should be performed in such a way that the two watermarks are used for two different purposes. For example, the watermark \mathbf{X}_2 (carrying W_2) should be very robust whereas the watermark \mathbf{X}_1 (carrying W_1) may be of lesser robustness. This means that watermark \mathbf{X}_2 must survive channel degradations up to some noise level $N_2 \gg N_1$. Furthermore, the transparency requirement implies that the two watermarks put together must have total power P , at most (i.e., $E_{\mathbf{X}}[\|\mathbf{X}\|^2] = nP$ where $\mathbf{X} = \mathbf{X}_1 + \mathbf{X}_2$). Assuming statistically independent watermarks \mathbf{X}_1 and \mathbf{X}_2 we suppose that $E_{\mathbf{X}_1}[\|\mathbf{X}_1\|^2] = n\gamma P$ and $E_{\mathbf{X}_2}[\|\mathbf{X}_2\|^2] = n(1 - \gamma)P$, where $\gamma \in [0, 1]$ may be arbitrarily chosen to share power between both watermarks.

In practice, this multiple watermarking scenario can model a variety of practical situations. In the scope of watermarking of medical images for example, we may wish to store the patient information into the corresponding image in a secure and private way (this information is sometimes called the “annotation part” of the watermark and, hence, is required to be sufficiently robust) and, in addition, to use a possibly fragile “tamper detection part” to detect tampering. Another example from proof-of-ownership applications is

as follows: we may wish to use one watermark to convey ownership information (should be robust) in addition to a second watermark to check for content integrity (should be semi-fragile or fragile). A third example concerns watermarking for distributed storage. In this example, a watermark embedded into a multimedia content which has to be stored in different storage devices may experience different alteration levels depending on the storage and extraction processes on each of the devices. Consequently, embedding must be such that reliable decoding be possible whatever the actual alteration level is (as long as this alteration is below some prescribed level). Many other examples and applications can be listed and, in fact, the model at hand covers all the situations in which a single watermarking authority (i.e., the same embedder) has to simultaneously embed several watermarks into the same host in such a way that these watermarks satisfy different robustness requirements.

Assuming Gaussian channel noises $\mathbf{Z}_i \sim \mathcal{N}(0, N_i I)$, with $i = 1, 2$, a simplified block diagram of the embedding scheme is shown in Figure 2. Decoder i checks for message W_i embedded at rate R_i , using signal $\mathbf{Y}_i = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{S} + \mathbf{Z}_i$. Decoding is unsuccessful if the estimate of message W_i is equal to the transmitted message. Functionally, this is the very transmission diagram of a two users **degraded Gaussian broadcast channel (D-GBC) with side information** available at the transmitter but not at the receivers. The watermark \mathbf{X}_2 which has to be robust plays the role of the message directed to the “degraded user”. Conversely, the watermark \mathbf{X}_1 plays the role of the message directed to the “better user”. We close this section by noting that similarity with a L -user BC will be retained if, instead of just two watermarks, L watermarks were to be simultaneously embedded by the same so-called trusted authority.

Figure 2. Embedding two watermarks at the same encoder viewed as communication over a two-user Gaussian broadcast channel (©IEEE 2007. Used with permission)

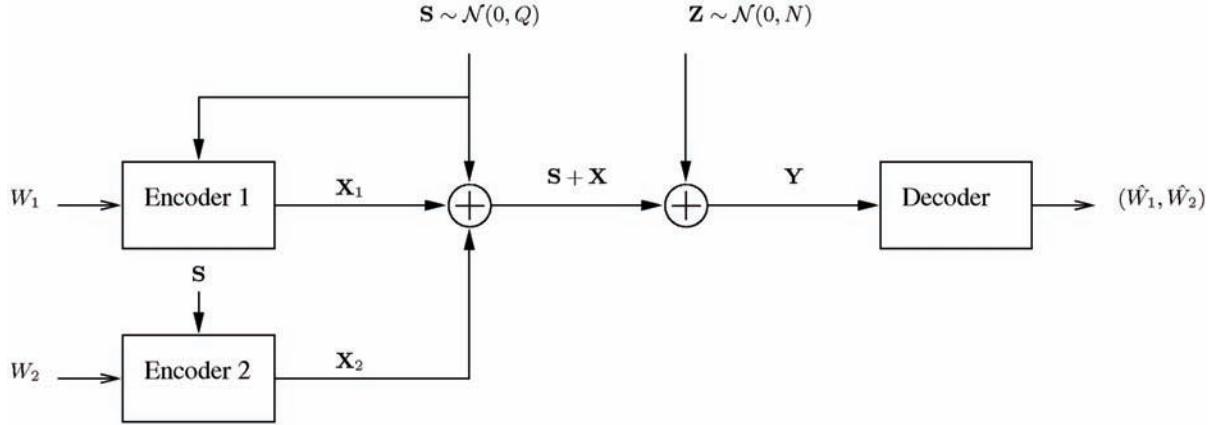


A Multiaccess Setup for Multiple Watermarking

We now consider another situation. Again, the watermarking system aims at embedding two independent messages W_1 and W_2 into the same cover signal S . However, the present situation is different in that, this time, 1) embedding is performed by two different authorities, each having to embed its own message with given power requirement and 2) at the receiver, a single trusted authority checks for both watermarks. We assume no particular cooperation between the two embedding authorities, meaning that the watermarks X_1 (carrying W_1) and X_2 (carrying W_2) should be designed independently of each other and should satisfy independent power constraints $E_{X_i}[\|X_i\|^2] \leq nP_i$, $i = 1, 2$. Note that, in addition, the composite watermark $X_1 + X_2$ with power at most equal $P = P_1 + P_2$ must satisfy the fidelity criterion to the non-watermarked content. However, the power constraint here is fundamentally different from that in the aforementioned BC setup, since individual power constraints must be satisfied independently.

In practice, this multiple watermarking scenario can be used to serve multiple purposes. Loosely speaking, every watermarking system addressing the same application multiple times is concerned. An example stemming from proof-of-ownership applications is as follows. Consider two different creators independently watermarking the same original content S , as it is common for large artistic works such as feature films and music recordings. Each of the two watermarks may contain private information. A common trusted authority may have to check for both watermarks. This is the case when an authenticator agent needs to track down the initial owner of an illegally distributed image, for example. A second example is the so-called hybrid in-band on-channel digital audio broadcasting (Chen and Wornell 2001). In this application, we would like to simultaneously transmit two digital signals within the same existing analog (AM and/or FM) commercial broadcast radio without interfering with conventional analog reception. Thus, the analog signal is the cover signal and the two digital signals are the two watermarks. These two digital signals may be designed independently. One digital signal may be used as an enhancement to refine the analog

Figure 3. Embedding two watermarks at separate encoders viewed as communication over a two-encoder multiaccess channel (MAC) (©IEEE 2007. Used with permission)



signal and the other as supplemental information such as station or program identification. A third application concerns distributed (i.e., at different places) watermarking: some fingerprinting can be embedded right at the camera, while possible annotations can be added next to the storage device.

Assuming a Gaussian channel noise $Z \sim \mathcal{N}(0, NI)$ corrupting the watermarked content $S + X$, a simplified diagram is shown in Figure 3. Embedder i , $i = 1, 2$ embeds W_i into the host S at rate R_i ; and the decoder checks for both watermarks. Decoding is unsuccessful if both messages are decoded correctly. Functionally, this is the very transmission diagram of a two users **Gaussian multiaccess channel (MAC)** with **side information** available at the transmitters but not at the receiver. We close this section by noticing that, similarity with a K -user MAC will be retained if, instead of just two authorities, K different embedding authorities, each encoding its own message were considered.

The previous discussion indicates that there are strong similarities between multiple watermarking and conventional multiuser communication. In the sequel, in our attempt to further highlight these similarities, we will sometimes use the terms “multiple users”, “degraded user” and “better user”

to loosely refer to “multiple watermarks”, “the receiver decoding the more noisy watermarked content” and “the receiver decoding the less noisy watermarked content”, respectively.

6. MULTIPLE WATERMARKING: PERFORMANCE ANALYSIS

In this section, we rely on the aforementioned similarity between multiuser watermarking and multiuser communication and, in fact, on recent findings in multiuser information theory (see, Kim, Sutivong and Sigurjonsson, 2004) for the Gaussian BC with SI and the Gaussian MAC with SI, to design efficient multiuser embedding schemes, for each of the two situations considered in Section IV. We refer to these schemes or coding strategies as being **broadcast-aware**’ and **multiaccess-aware**, respectively. Awareness imposes some joint-design and offers substantial improvement (over straightforward, rather intuitive, embedding schemes obtained by simple super-imposition of single user embedding techniques). This improvement is illustrated through both achievable embedding rate regions and BER curves in the sequel.

Broadcast-Aware Coding for Multiple Watermarking

In Section IV-A, we have shown that the communication scenario depicted in Figure 2 is basically that of a **degraded GBC** with state information non-causally known to the transmitter but not to the receivers. Kim et al. (2004) have shown that the capacity region C_{BC} of this channel is given by

$$\begin{aligned} C_{BC}(P) = \bigcup_{0 \leq \gamma \leq 1} \{(R_1, R_2) : & R_1 \leq \frac{1}{2} \log_2 \left(1 + \frac{\gamma P}{N_1} \right), \\ & R_2 \leq \frac{1}{2} \log_2 \left(1 + \frac{(1-\gamma)P}{\gamma P + N_2} \right) \}, \end{aligned} \quad (4)$$

which is that of a GBC with no interfering signal S . This region can be attained by an appropriate successive encoding scheme that uses two well designed DPCs, as follows:

- 1) Use a first DPC (denoted by DPC2) considering the host S as known state and the watermark X_1 (carrying W_1) and X_2 as unknown noise (i.e., total noise $X_1 + Z_2$ to form the most robust watermark X_2 intended to the degraded user. By using (2), DPC2 is given by $X_2 = U_2 - \pm_2 S$ with

$$U_2 | S \sim \mathcal{N}(\alpha_2 S, (1-\gamma)P), \text{ with } \alpha_2 = \frac{(1-\gamma)P}{(1-\gamma)P + (N_2 + \gamma P)}. \quad (5)$$

- 2) Use a second DPC (denoted by DPC1) considering $S + X_2$ as known state, sum of the cover signal S and the already formed watermark X_2 and Z_1 as unknown noise to form the less robust watermark X_1 intended to the better user. By using (2), DPC1 is given by $X_1 = U_1 - \pm_1(S + X_2)$ with

$$U_1 | U_2, S \sim \mathcal{N}(\alpha_1(S + X_2), \gamma P I), \text{ with } \alpha_1 = \frac{\gamma P}{\gamma P + N_1}. \quad (6)$$

- 3) Finally, transmit the watermarked content $S + X$ over the watermark channel, where $X = X_1 + X_2$ is the composite watermark. The decoders checking for the fragile and the robust watermarks receive $Y_1 = X + S + Z_1$ and $Y_2 = X + S + Z_2$, respectively.

Note that watermark X_2 should be embedded first here, because of the following intuitive reason. When considering the extreme case in which watermark X_1 is fragile, this watermark should be, by design, damaged by any operation that alters the cover signal S . Since robust embedding is such an operation, the fragile watermark should be embedded last. Also, we emphasize that the key point in the embedding system here is to consider the unknown watermark X_1 as noise in the design of watermark X_2 which, in turn, will be used as non-causal side information in the design of watermark X_1 . We refer to this by saying that, for the design of watermark X_i , $i = 1, 2$, the encoder is “aware” of the existence of the other watermark X_j ($j = 1, 2; j \neq i$) and takes it into account, either as unknown noise or as side information (thus imposing some joint design of DPCs). Hence, we call the embedding scheme here “**broadcast-aware**”. In order to emphasize the improvement brought by this “awareness” note that, when watermark X_2 is designed independently of watermark X_1 (which is assumed to be designed as above), one is able to embed only $R(\alpha_2, (1-\gamma)P, Q, \gamma P + N_2)$ bits of information W_2 at most, where:

$$R(\alpha, P, Q, N) = \frac{1}{2} \log_2 \left(P(P+Q+N) / (PQ(1-\alpha)^2 + N(P+\alpha^2Q)) \right)$$

Then, the corresponding 2-user embedding scheme simply super-imposes two independent DPCs. We refer to this straightforward scheme as being “broadcast-unaware”, by reference to the lack of the aforementioned joint design.

We close this section by noticing that DPC1 - as given by (6) - is optimal in that embedding rate R_1 corresponds to that of a channel with not only no interfering cover signal \mathbf{S} but also no interfering watermark \mathbf{X}_2 . Thus, message W_2 can be embedded at its maximal rate, as if there were no other watermark W_1 . From “Decoder 1” point of view, the channel from W_1 to \mathbf{Y}_1 is functionally equivalent to a single-user channel $W_1 \rightarrow \mathbf{Y}'_1$, where $\mathbf{Y}'_1 = \mathbf{Y}_1 - \mathbf{U}_2 = \mathbf{X}_1 + (1 - \alpha_2)\mathbf{S} + \mathbf{Z}_1$ contains no \mathbf{X}_2 . Yet, it is not that \mathbf{Y}_1 is a single-user channel, but rather that the amount of reliably decodable information W_1 is exactly the same as if W_1 were to be embedded alone. Also, even though the interference due to \mathbf{X}_1 is not removed (in the embedding of W_2), DPC2 is optimal too, since it allows to attain the maximal rate $R_2^{(\max)} = \frac{1}{2} \log_2 (1 + (1 - \gamma)P / (\gamma P + N_2))$ at which message W_2 can be embedded when message W_1 has a nonzero embedding rate.

Feasible Embedding Rate Region

Consider now a scalar implementation of this Joint DPC scheme consisting in two successive SCSs. DPC2 can be implemented by a scalar scheme SCS2, quantizing the cover signal \mathbf{s} and outputting the watermark \mathbf{x}_2 as an appropriate scaled version of the quantization error. We denote by $\tilde{\alpha}_2$ and Δ_2 the corresponding scale factor and quantization step size, respectively. DPC1 can be implemented by a scalar scheme SCS1, quantizing the newly available signal $\mathbf{s} + \mathbf{x}_2$ and outputting the watermark \mathbf{x}_1 as an appropriately scaled version of the quantization error. We denote by $\tilde{\alpha}_1$ and Δ_1 the corresponding scale factor and

quantization step size, respectively. The **embedding rate region** $\widetilde{\mathcal{R}}_{BC}$ feasible with this practical coding is given by

$$\begin{aligned} \widetilde{\mathcal{R}}_{BC}(P) = \bigcup_{0 \leq \gamma \leq 1} \{(\widetilde{R}_1, \widetilde{R}_2) : & \quad \widetilde{R}_1 \leq \max_{\alpha_1 \in [0,1]} I(W_1; Q_{\Delta_1(\alpha_1, \gamma)}(\mathbf{y}'_1) - \mathbf{y}'_1), \\ & \quad \widetilde{R}_2 \leq \max_{\alpha_2 \in [0,1]} I(W_2; Q_{\Delta_2(\alpha_2, \gamma)}(\mathbf{y}_2) - \mathbf{y}_2) \}. \end{aligned} \quad (7)$$

The scale factors pair $(\tilde{\alpha}_1, \tilde{\alpha}_2)$ maximizing the right hand side terms of (7) is given by

$$(\tilde{\alpha}_1, \tilde{\alpha}_2) = \left(\sqrt{\frac{\gamma P}{\gamma P + 2.71N_1}}, \sqrt{\frac{(1 - \gamma)P}{(1 - \gamma)P + 2.71(\gamma P + N_2)}} \right) \quad (8)$$

The region (7), obtained through Monte-Carlo based integration, is depicted in Figure 4 and is compared to the region \mathcal{C}_{BC} given by (4), for two choices of channel parameters: weak channel noise [Figure 4(c) and 4(d)] and strong channel noise [Figure 4(a) and 4(b)]. The latter may model, for example, a channel attack with is as strong as the two watermarks considered together. Note that for the evaluation of the mutual information involved in (7) (and in fact, the computation of conditional probabilities $p_{\mathbf{r}'_1}(\mathbf{r}'_1 | W_1)$ and $p_{\mathbf{r}_2}(\mathbf{r}_2 | W_2)$), we assumed that the high resolution quantization assumption $Q \gg P$ holds, which is relevant in most watermarking applications

Improvement over the simple “broadcast-unaware” scheme is made possible by increasing the rate at which the robust watermark can be reliably embedded at. It is precisely the aforementioned “awareness” that allows this improvement. However, observe this gain is more visible at high SNR as shown in Figure 4(c). At low SNR however, this gain, though still theoretically possible as shown in Figure 4(a), is very limited and is almost not visible for scalar codebooks. From a communication point-of-view, this can be interpreted as follows: “awareness”, which can be viewed as a power saving technique for the

Figure 4. The improvement brought up by "BC-awareness" (with binary inputs) is depicted for (a) $P / N_1 = 5 \text{ dB}$, $P / N_2 = 0 \text{ dB}$ and (c) $P / N_1 = 12 \text{ dB}$, $P / N_2 = 9 \text{ dB}$. Solid line corresponds to the embedding rate region of the BC-aware scheme achievable theoretically (upper) and practically (lower). Dashed line corresponds to the embedding rate region of the BC-unaware scheme achievable theoretically (upper) and practically (lower). Left Subfigures: achievable embedding rate region of the BC-aware scheme for M_1 -ary and M_2 -ary alphabets depicted for (b) $P / N_1 = 5 \text{ dB}$, $P / N_2 = 0 \text{ dB}$ and (d) $P / N_1 = 12 \text{ dB}$, $P / N_2 = 9 \text{ dB}$ (© IEEE 2007. Used with permission)

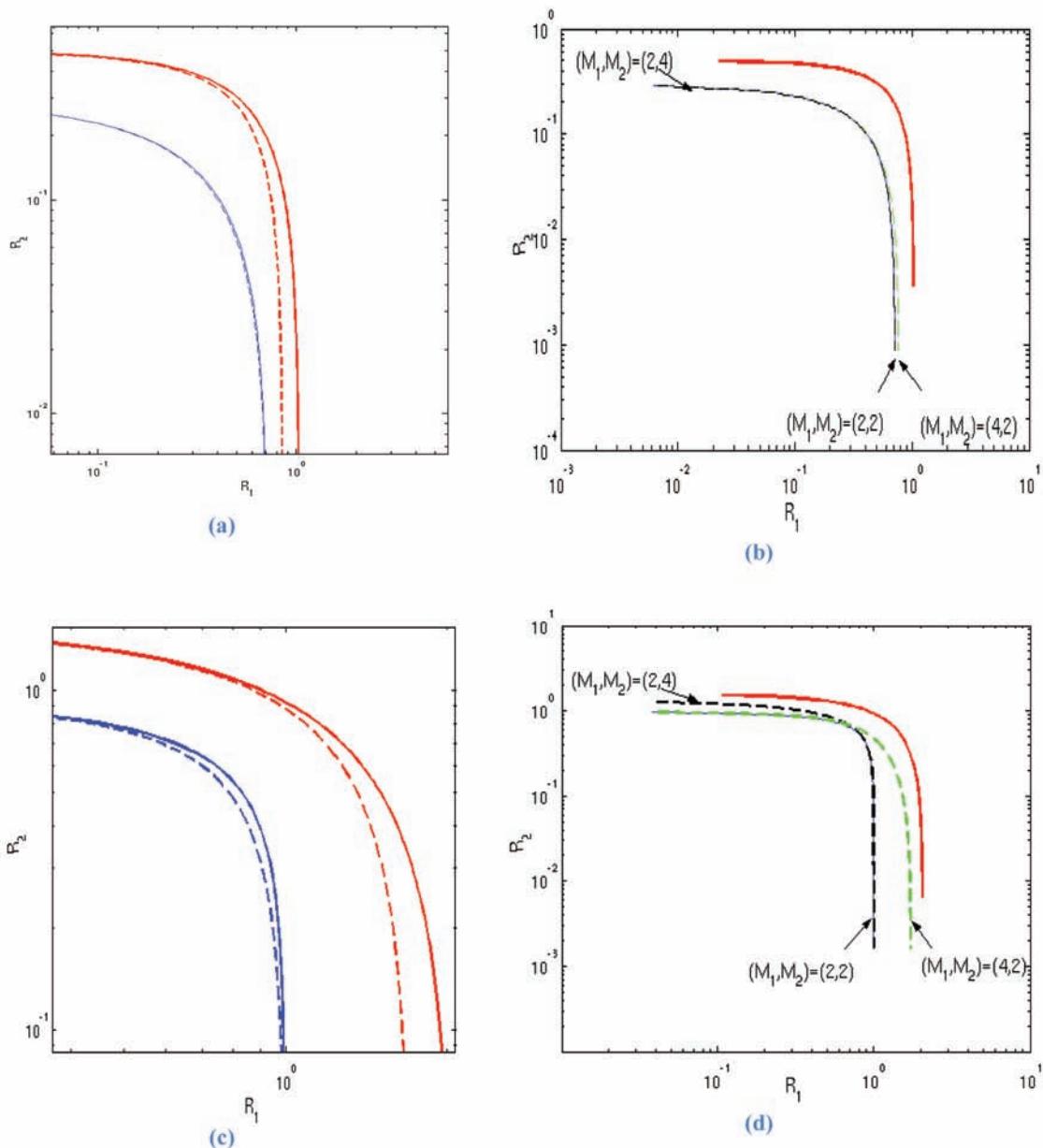
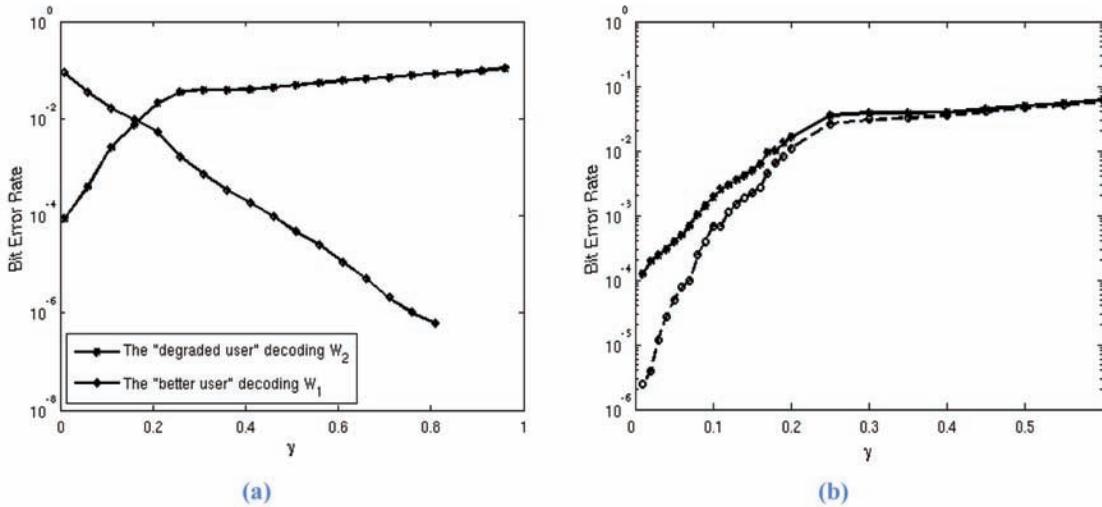


Figure 5. Broadcast-aware multiple watermarking. (a): bit error rates for embedding using repetition coding. (b): Each decoder can only decode "his" own watermark. Though much less noisy, the "better user" performs only slightly better than the "degraded user" in decoding message W_2 . The messages W_1 and W_2 are repeated 4 times each, i.e., $(\rho_1, \rho_2) = (4, 4)$ and channel parameters are such that $P / N_1 = 12 \text{ dB}$ and $P / N_2 = 9 \text{ dB}$. (©IEEE 2007. Used with permission)



"degraded user", does not sensibly improve the overall communication when the channel is very bad. Both theoretical and feasible embedding rate regions of the BC-aware scheme are also depicted for no binary inputs in 4(d) and 4(b). It can be seen that, depending on the SNR, the practically feasible embedding rate region (7) can more-or-less approach the theoretical capacity region C_{BC} by increasing the sizes M_1 and M_2 of the input alphabets \mathcal{M}_1 and \mathcal{M}_2 .

Bit Error Rate Analysis and Discussion

Another performance analysis is based on measured BERs for hard decision based decoding of binary scalar DPC. Results are obtained with Monte Carlo based simulation and are depicted in Figure 5. Note that the set of channel parameters chosen in Figure 5 may model a wide range of admissible channel attacks on the individual watermarks, since the individual SNRs, $\text{SNR}_1 = 10\log_{10}(\gamma P / N_1)$

and $\text{SNR}_2 = 10\log_{10}((1-\gamma)P / (\gamma P + N_2))$, vary from -8 dB to 12 dB and from -15 dB to 9 dB respectively as the power-sharing parameter γ varies from 0 to unity. However, this may be not a good choice to model a strong attack on the composite watermark $X_1 + X_2$ (e.g., one such that $P / N_2 = 0 \text{ dB}$). For such an attack, the individual rates are very low and the BERs are very bad. In principle, it would be possible to use any provably efficient error correction code for each of the channels Y_1 and Y_2 taken separately. However, at low SNR ranges, it is well known that repetition coding is almost optimal. The curves in Figure 5(a) are obtained with $(\rho_1, \rho_2) = (4, 4)$, meaning that W_1 and W_2 are repeated 4 times each.

We observe that as $\gamma \in [0, 1]$ increases, the power part of the signal X allocated to the watermark carrying W_1 becomes larger and that allocated to the watermark carrying W_2 becomes smaller. This causes the corresponding BER curves to monotonously decrease and increase,

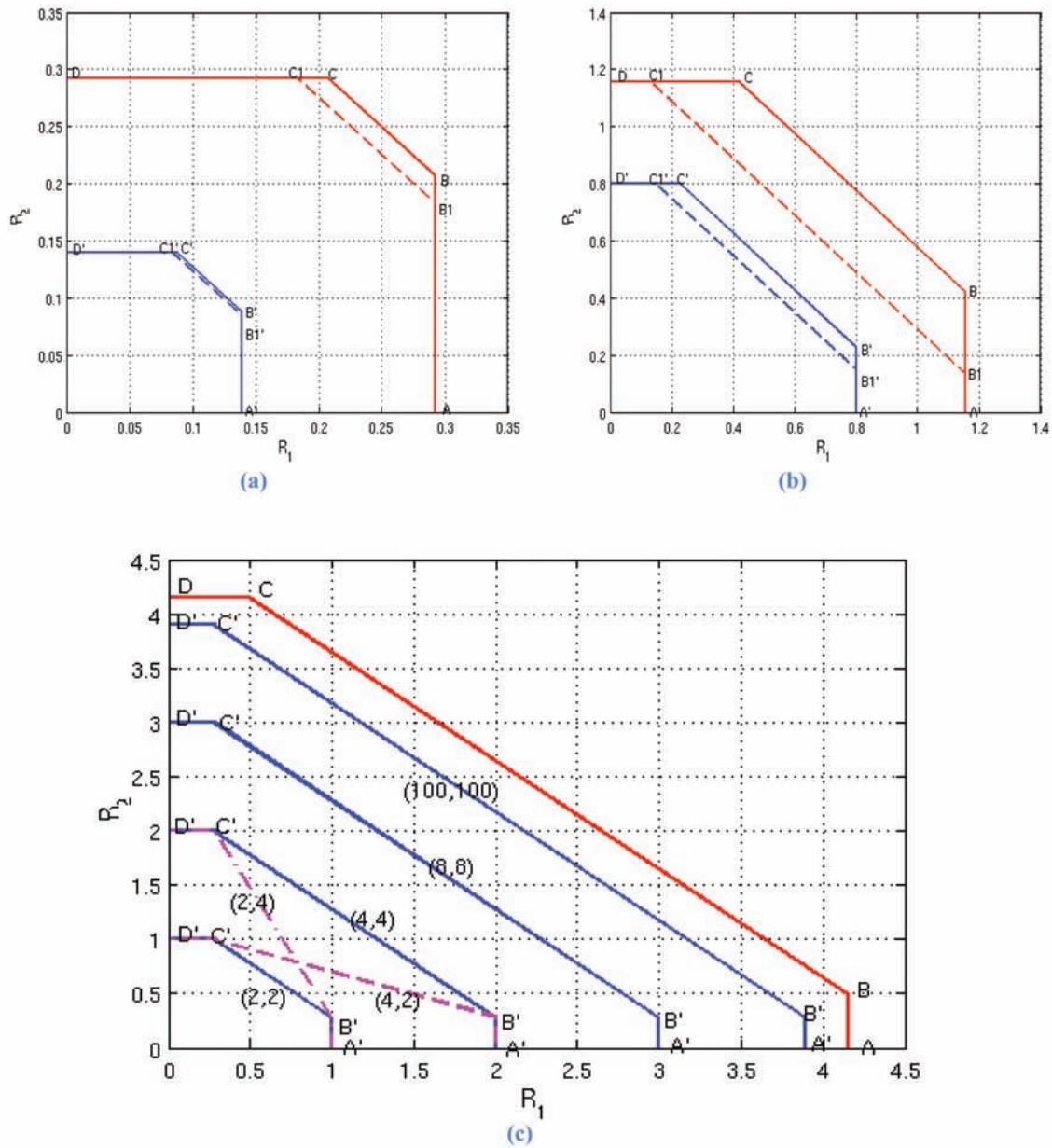
respectively. The curves depicted in Figure 5 also motivate the following discussion.

1. In practical situations, the repetition factors ρ_1 and ρ_2 should be chosen in light of the desired embedding rates and also the desired robustness requirements. The choice $(\rho_1, \rho_2) = (4, 4)$ made previously should be taken just as a baseline example. Channel coding as a means of providing additional redundancy obviously strengthens the watermark immunity to channel degradations. However, such a redundancy inevitably limits the embedding rate. This means that for equal target embedding rates R_1 and R_2 , the repetition factors ρ_1 and ρ_2 should satisfy $\rho_2 \geq \rho_1$.
2. The scalar DPC considered here is conceived using insights from coding for broadcast channels (Cover, 1972), as mentioned previously. Interestingly, in such channels the user who experiences the better channel (less noisy) has to reliably decode the message assigned to the (degraded) user who experiences the worst channel (more noisy). In a watermarking context, this means that the robust watermark, which is supposed to survive channel degradation levels up to N_2 , should be reliably decodable if, actually, the channel noise is less powerful. However, this feature, which is inherently related to the principle of superposition coding at the transmitter combined with successive decoding (peeling-off technique) at the “better user” (Decoder 1) (Cover, 1991), makes more sense in the situations where the “better user” is unable to reliably decode its own message unless it primarily subtracts off the interference due to the message assigned to the “degraded user”. The DPC-based scheme considered here is fundamentally different, in that the interference is already subtracted off at the encoder. As a by-product of this

design, the “better user” does not need to decode the message of the degraded user.¹

3. There could, however, be advantages and disadvantages for the DPC-based scheme described previously to not satisfy the aforementioned broadcast feature. An obvious advantage is that it is more secure. Clearly, the user checking for the fragile watermark needs not (and should not) be able to reliably decode the robust watermark in systems where security is of prime concern. By opposition, an obvious disadvantage is as follows. If channel conditions come to be improved (e.g., less stringent attacks than expected) resulting in better SNR for message W_2 , the user checking for the robust watermark (and expecting bad channel conditions) should not only still reliably decode this watermark, but in principle, be able to perform it even if there were more information W_2 embedded into the host signal.
4. The present DPC scheme, as is, does not fully satisfy this feature. From Figure 5(b) we observe that, even if he were allowed to (i.e., if security issues were not considered), the user checking for the fragile watermark (i.e., the “better user”) would decode almost as much information W_2 as what the user checking for the robust watermark (i.e., the “degraded user”) actually does. This shows that he does not fully exploit the fact of decoding a much less noisy watermarked content. The improvement in BER upon the “degraded user” is very small and is even negligible, as shown in Figure 5(b). And even though this improvement seems to behave like the improvement in SNR (which is maximal at $\gamma = 0$), it is actually smaller than the one, $10 \log_{10} \left((\gamma P + N_2) / (\gamma P + N_1) \right)$ dB, which should be visible if the “better user” were really able to decode message W_2 as in superposition coding.

Figure 6. MAC-aware multiple watermarking. The improvement brought by "awareness" is depicted for (a) strong channel noise, $P_1 = P_2$, $(P_1 + P_2) / N = 0$ dB and (b) weak channel noise, $P_1 = P_2$, $(P_1 + P_2) / N = 9$ dB. Solid line delineates the capacity region of the MAC-aware scheme achievable theoretically (upper) and practically (lower). Dashed line delineates the embedding rate region of the MAC-unaware scheme achievable theoretically (upper) and practically (lower). (c) Capacity region of the MAC-aware scheme with $(M_1$ -ary, M_2 -ary) input alphabets for very high SNR. (©IEEE 2007. Used with permission)



MAC-Aware Coding for Multiple Watermarking

In this section, we are interested in designing implementable multiple watermarking schemes for the situation described in Section IV-B. Paralleling the development made in Section IV-A, we provide performance analysis for two MAC-aware and unaware coding strategies.

Let $\mathbf{Y} = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{S} + \mathbf{Z}$ denote the received signal. Upon reception, the receiver should reliably decode both watermarks. In Section IV-B, we argued that the embedding scenario depicted in Figure 3 is equivalent to communication over a Gaussian multiaccess channel (GMAC) with side information non-causally known to the transmitters but not to the receiver. Kim et al. (2004) established the capacity region \mathcal{C}_{MAC} of this channel as

$$\begin{aligned} \mathcal{C}_{\text{MAC}}(P_1, P_2) = \left\{ (R_1, R_2) : \quad R_1 &\leq \frac{1}{2} \log_2 \left(1 + \frac{P_1}{N} \right), \\ R_2 &\leq \frac{1}{2} \log_2 \left(1 + \frac{P_2}{N} \right), \\ R_1 + R_2 &\leq \frac{1}{2} \log_2 \left(1 + \frac{P_1 + P_2}{N} \right) \right\}, \end{aligned} \quad (9)$$

which is that of a GMAC with no interfering signal \mathbf{S} . This region is represented by the region with corner points (A), (B), (C) and (D) in Figure 6; and can be attained by an appropriate successive encoding scheme that uses well designed DPCs. For example, the corner point (B) can be attained as follows.

1. Embedder 2 (i.e., Encoder 2) uses a DPC (denoted here by DPC2) considering the host \mathbf{S} as known state and signal $\mathbf{X}_1 + \mathbf{Z}$ as unknown total channel noise, to form the watermark \mathbf{X}_2 of power P_2 and carrying W_2 as $\mathbf{X}_2 = \mathbf{U}_2 - \alpha_2 \mathbf{S}$, where

$$\mathbf{U}_2 \sim \mathcal{N}(\alpha_2 \mathbf{S}, P_2 I), \text{ with } \alpha_2 = \frac{P_2}{P_2 + (P_1 + N)}. \quad (10)$$

At reception, the decoder first decodes W_2 and then cleans up the channel by subtracting the interference penalty \mathbf{U}_2 that the embedding of W_2 causes to that of W_1 .² Thus, the watermark channel for W_1 is made equivalent to $\mathbf{Y}_1 = \mathbf{Y} - \mathbf{U}_2 = \mathbf{X}_1 + (1 - \alpha_2) \mathbf{S} + \mathbf{Z}$. This “cleaning up” step is inherently associated with *successive decoding* and is sometimes referred to as the *peeling-off* technique. Hence, Embedder 1 (i.e., Encoder 1) can use a second DPC (denoted here by DPC1) to embed message W_1 .

- 2) Embedder 1 forms \mathbf{X}_1 as $\mathbf{X}_1 = \mathbf{U}_1 - \alpha_1 \mathbf{S}$, where

$$\mathbf{U}_1 | \mathbf{S} \sim \mathcal{N}(\alpha_1 \mathbf{S}, P_1 I), \text{ with } \alpha_1 = (1 - \alpha_2) \frac{P_1}{P_1 + N} = \frac{P_1}{P_1 + P_2 + N}. \quad (11)$$

The rates pair $(R_1, R_2) \in \mathcal{R}_{\text{MAC}}$ achieved by the considered two DPCs are represented by the corner point (B) in Figure 6 and are given by

$$\begin{aligned} R_1(B) &= \frac{1}{2} \log_2 \left(1 + \frac{P_1}{N} \right), \\ R_2(B) &= \frac{1}{2} \log_2 \left(1 + \frac{P_2}{P_1 + N} \right), \end{aligned} \quad (12)$$

which is easily obtained by evaluating the achievable region

$$\begin{aligned} \mathcal{R}_{\text{MAC}}(P_{U_1 U_2 | S}) = \left\{ (R_1, R_2) : \quad R_1 &\leq I(U_1; Y | U_2) - I(U_1; S | U_2) \\ R_2 &\leq I(U_2; Y | U_1) - I(U_2; S | U_1) \\ R_1 + R_2 &\leq I(U_1, U_2; Y) - I(U_1, U_2; S) \right\}, \end{aligned} \quad (13)$$

with the choice of

$$p(u_1, x_1 | s) p(u_2, x_2 | s)$$

given by (10) and (11).

Similar DPC schemes allowing attaining the corner points (A), (C) and (D) can be designed by following the same principle. The corner point (A) corresponds to the watermark \mathbf{X}_1 (i.e., message W_1) being embedded at its maximum rate whereas the watermark \mathbf{X}_2 (i.e., message W_2) not embedded at all. The two corner points (C) and (D) correspond to the points (B) and (A), respectively, with the roles of the watermarks \mathbf{X}_1 and \mathbf{X}_2 reversed. Any rate pair lying on the lines connecting these corner points can be attained by time sharing.

We emphasize that the key point for DPC2 in (10) and DPC1 in (11) is to consider watermark \mathbf{X}_1 as noise in the design of watermark \mathbf{X}_2 and to use successive decoding (i.e., a peeling-off technique) at the decoder. We refer to this by saying that Embedder 2 is “aware” of the existence of watermark \mathbf{X}_1 and takes it into account; and that Embedder 1 is “aware” that the decoder is using a peeling-off technique and acts accordingly. Hence, we call the embedding scheme here “**multiaccess-aware**”, or, simply, MAC-aware. This awareness imposes some joint design of DPCs as stated above. In order to bring out the improvement offered by this “awareness”, note that when watermark \mathbf{X}_2 is designed independently of watermark \mathbf{X}_1 (which is still conceived as above), one is able to embed only:

$$R_2(B1) = 0.5 \log_2 \left(P_2 (P_2 + Q + N + P_1) / (P_2 Q (1 - \alpha_2)^2 + (N + P_1)(P_2 + \alpha_2^2 Q)) \right)$$

bits of information W_2 at most. Then, the corresponding 2-user embedding scheme simply super-imposes two independent DPCs. We refer to this straightforward scheme as being “MAC-

unaware”, by reference to the lack of the aforementioned joint design. It achieves the region with corner points (A), (B1), (C1) and (D), which is strictly contained in the region with corner points (A), (B), (C) and (D) as shown in Figure 6.

Feasible Embedding Rate Region

We consider now a practical implementation for this joint scheme. Concentrate, for example, on the corner point (B). This can be performed by using two SCSs, SCS1 and SCS2, consisting of scalar versions of DPC1 and DPC2. The uniform scalar quantizers \mathcal{Q}_{Δ_1} and \mathcal{Q}_{Δ_2} have step sizes $\Delta_1 = \sqrt{12P_1} / \tilde{\alpha}_1$ and $\Delta_2 = \sqrt{12P_2} / \tilde{\alpha}_2$, where the optimal choice

$$(\tilde{\alpha}_1, \tilde{\alpha}_2) = \left(\frac{P_1 + N}{P_1 + P_2 + N} \sqrt{\frac{P_1}{P_1 + 2.71N}}, \sqrt{\frac{P_2}{P_2 + 2.71(N + P_1)}} \right) \quad (14)$$

for scale factors conforms the codebooks choice in (10) and (11). Note that the signal \mathbf{S} is assumed to be flat-host here, as we mentioned previously. These implementable scalar schemes SCS1 and SCS2 perform close to optimality. The allowed embedding rates \tilde{R}_1 and \tilde{R}_2 for watermarks W_1 and W_2 are obtained by maximizing mutual information $I(W_1; r_1)$ and $I(W_2; r_2)$, respectively, where $r_1 = \mathcal{Q}_{\Delta_1}(y_1) - y_1$ and $r_2 = \mathcal{Q}_{\Delta_2}(y_2) - y_2$. The maxima are achieved with the choice of scale factors chosen as in (14). The embedding rate pair $(\tilde{R}_1, \tilde{R}_2)$ is represented by the corner point (B') in Figure 6 for two examples of channel conditions: weak noise [shown in Figure 6(b)] and strong noise modeling a strong channel attack on the composite watermark $\mathbf{X} = \mathbf{X}_1 + \mathbf{X}_2$ [shown in Figure 6(a)]. More generally any rate pair on the region frontier delimited by the corner points (A'), (B'), (C') and (D') can be achieved by subsequent time-sharing. When only message $W_i, i = 1, 2$, is embedded (i.e.,

embedding rate zero for the other message W_j , $j \neq i$), the equivalent watermark channel for message W_i is $\mathbf{Y}_i = \mathbf{Y} - \mathbf{U}_j$. Hence, message W_i can be embedded at its maximum feasible rate, given by $\max_{\alpha_i \in [0,1]} I(W_i; r_i)$ where $\mathbf{r}_i = \mathcal{Q}_{\Delta_i}(\mathbf{y}_i) - \mathbf{y}_i$. When both messages are embedded at non zero rates, the maximum embedding rate for the composite watermark is obtained by embedding one of the two (e.g., W_1) at its maximal feasible rate (i.e., as if it were *alone* on the watermark channel) and the other (W_2) at the embedding rate obtained by considering the first watermark as noise (i.e., total channel noise $\mathbf{z} + \mathbf{x}_1$). Of course, we can reverse the roles of W_1 and W_2 , and the maximum feasible embedding rate for the composite watermark remains unchanged. Consequently, the **embedding rate region** practically feasible here by the two SCSs is given by:

$$\begin{aligned} \tilde{\mathcal{R}}_{\text{MAC}}(P_1, P_2) = \{(\tilde{R}_1, \tilde{R}_2) : & \quad \tilde{R}_1 \leq \max_{\alpha_1 \in [0,1]} I(W_1; \mathcal{Q}_{\Delta_1(\alpha_1, P_1)}(\mathbf{y}_1) - \mathbf{y}_1), \\ & \quad \tilde{R}_2 \leq \max_{\alpha_2 \in [0,1]} I(W_2; \mathcal{Q}_{\Delta_2(\alpha_2, P_2)}(\mathbf{y}_2) - \mathbf{y}_2), \\ & \quad \tilde{R}_1 + \tilde{R}_2 \leq \max_{\substack{\alpha_1 \in [0,1] \\ \alpha_2 \in [0,1]}} I(W_1; \mathcal{Q}_{\Delta_1(\alpha_1, P_1)}(\mathbf{y}_1) - \mathbf{y}_1) \\ & \quad + \max_{\alpha_2 \in [0,1]} I(W_2; \mathcal{Q}_{\Delta_2(\alpha_2, P_2)}(\mathbf{y}) - \mathbf{y})\}. \end{aligned} \quad (15)$$

Figure (6) shows the improvement in achievable embedding rate region brought by the joint design of the two scalar schemes (over the aforementioned “MAC-unaware” scheme). This improvement, which is more visible at high SNR (i.e., weak channel noise), is larger when both watermarks are embedded at non zero rates. In such cases, for a given embedding rate \tilde{R}_2 for message W_2 for example, the joint design allows more information to be embedded for the other watermark (i.e., higher embedding rate \tilde{R}_1 for message W_1). From Figure 6 we see also that the gap to the theoretical limit \mathcal{C}_{MAC} can be reduced by use of larger size alphabets, which of course, would be achieved at the cost of some increase in embedding and decoding complexities.

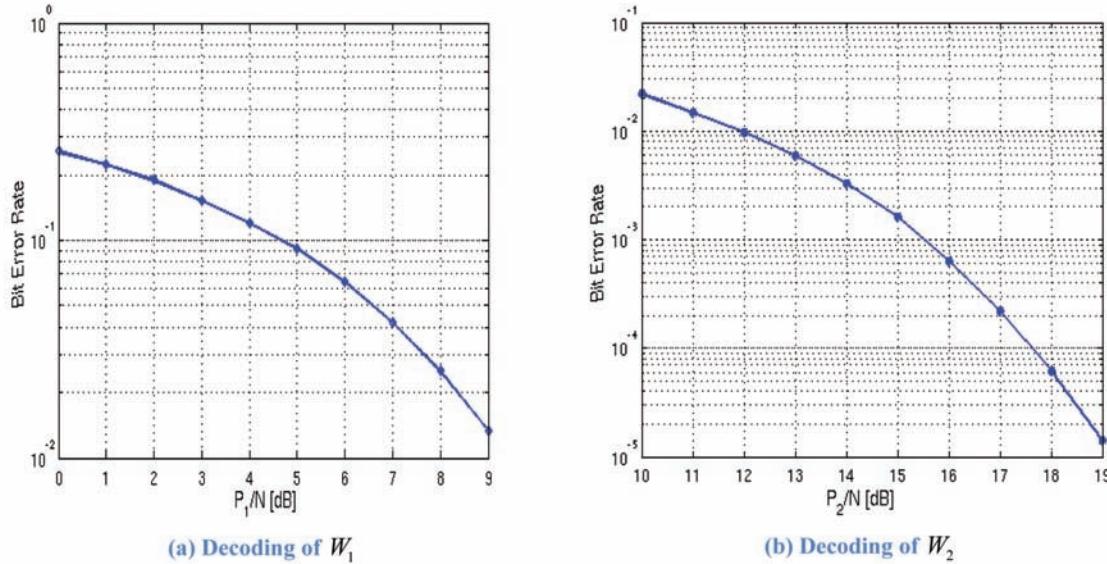
Bit Error Rate Analysis and Discussion

Consider the coding scheme given by (10) and (11). The peeling-off technique aims to clean up the channel before decoding W_1 , by subtracting the codeword \mathbf{U}_2 . This is good for performance evaluation and to prove theoretically the achievability of corner point (B) in the embedding rate region curve. However, in practice, the decoder does not know the exact codeword \mathbf{U}_2 that Embedder 2 had selected, basically because it does not know the host signal \mathbf{S} . Instead, the decoder determines an estimate $\hat{\mathbf{U}}_2$ of \mathbf{U}_2 , as the reconstruction vector of a scaled version of the received signal \mathbf{Y} . Of course, the accuracy of this estimation (and thereby that of decoding message W_1) depends on the value of SNR2 (i.e., the SNR for message W_2). For instance, bad SNR2 likely cause decoding of W_2 to fail. Thus, the estimate $\hat{\mathbf{U}}_2$ does not resemble the exact \mathbf{U}_2 and it would be seen rather as an additional noise source. However, at good (high) SNR2, the estimate $\hat{\mathbf{U}}_2$ of codeword \mathbf{U}_2 is accurate and the peeling-off technique is more efficient as shown in Figure 7. Note that the curves in Figure 7 are obtained using scalar codebooks and with respective powers P_1 and P_2 for the two watermarks such that $P_2 = 10P_1$. In the simulations, second watermark (i.e., message W_2) is decoded first, corresponding codeword $\hat{\mathbf{U}}_2$ is subtracted and then the other watermark is decoded.

7. CONCLUSION

In this chapter, we first investigated the tight relationship between multiple watermarking and conventional multiuser information theory. For instance, two different scenarios of embedding several watermarks into the same cover signal are emphasized. The first scenario concerns the situations in which different watermarks are to

Figure 7. MAC-aware multiple watermarking bit error rates using scalar codebooks. The two messages W_1 and W_2 are sent at rates $(\tilde{R}_1, \tilde{R}_2)$ corresponding to the corner point (B') in the capacity region diagram shown in Figure 6. Successive decoding is implemented by first decoding message W_2 , subtracting its corresponding codeword $\hat{\mathbf{u}}_2$ and then decoding message W_1 . (©IEEE 2007. Used with permission)



be embedded jointly (e.g., by the same trusted authority) and checked for separately (e.g., by different authorities, or spatially distributed verification for the same watermark). This scenario is recognized to be equivalent to communication over a Gaussian broadcast channel (GBC) with state information non-causally known at the transmitter but not at the receivers. The second scenario concerns the situations in which different watermarks are to be embedded separately (e.g., by different authorities each embedding its own watermark as it is common for large artistic works such as films and music recordings) and checked for or decoded jointly; and is argued as to be analog to communication over a Gaussian multiaccess channel (MAC) with state information known non-causally at the transmitters but not at the receiver. Next, based on this equivalence and heavily relying on a recent work by Kim et al. in which the authors extend the single-user Costa's DPC to the multiuser case, two practically feasible

scalar schemes for simultaneously embedding two messages into the same host signal are proposed. These schemes carefully extend the initial QIM and SCS schemes that were originally conceived for embedding one watermark, to the 2 watermarks case. The careful design concerns the joint encoding as well as the appropriate order needed so as to reliably embed the different watermarks. A central idea for the joint design is “awareness”. The improvement brought by this awareness is shown through comparison to the corresponding rather intuitive schemes, obtained through superimposition, as many times as needed, of the single user schemes QIM and SCS. Performance is analyzed in terms of embedding rate region and bit error rate.

Finally, we close this chapter by noticing that the proposed schemes can be straightforwardly extended to the arbitrary number of watermarks case and also to the vector case through lattice-based codebooks.

REFERENCES

- Chen, B., & Wornell, G. (2001). Quantization Index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, *47*, 1423–1443. doi:10.1109/18.923725
- Costa, M. H. M. (1983). Writing on dirty paper. *IEEE Transactions on Information Theory*, *29*, 439–441. doi:10.1109/TIT.1983.1056659
- Cover, T. M. (1972). Broadcast Channels. *IEEE Transactions on Information Theory*, *18*, 2–14. doi:10.1109/TIT.1972.1054727
- Cover, T. M., & Thomas, J. A. (1991). *Elements of Information Theory*. Mahwah, NJ: John Wiley & Sons, Inc. doi:10.1002/0471200611
- Cox, I., Miller, M., & McKellips, A. (1999). Watermarking as communication with side information. *IEEE Int. Conference on Multimedia Computing and Systems*, (pp. 1127-1141).
- Cox, I. J., Kilian, J., Leighton, T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, *51*, 1673–1678. doi:10.1109/83.650120
- Eggers, J. J., Bauml, R., Tzschoppe, R., & Girod, B. (2003). Scalar Costa Scheme for information Embedding. *IEEE Transactions on Signal Processing*, *1003–1019*. doi:10.1109/TSP.2003.809366
- Fischer, R. F. H., (2005). The Modulo-Lattice Channel: The key Feature in Precoding Schemes. *International Journal of Electronics and Communications*, *244–253*.
- Gel'fand, S. I., & Pinsker, M. S. (1980). Coding for channel with random parameters. *Problems of Control and Information Theory*, *9*, 19–31.
- Khisti, A., Erez, U., Lapidot, A., & Wornell, G. (2007). Carbon Copying Onto Dirty Paper. *IEEE Transactions on Information Theory*, *53*, 1814–1827. doi:10.1109/TIT.2007.894693
- Kim, Y.-K., Sutivong, A., & Sigurjonsson, S. (2004). Multiple User Writing on Dirty Paper. *IEEE Int. Symp. Information Theory*, *534*.
- Liu, Y.-W., & Smith, J. O. (2004). Multiple Watermarking: is power sharing better than time sharing? In *IEEE Int. Conf. on Multimedia and Expo, ICME*, (pp. 1939-1942).
- Mintzer, F., & Braudaway, G. W. (1999). If one watermark is good, are more better? In *IEEE Int. Conf. on Acoustics, Speech and Signal Processing, ICASSP*, (pp. 2067-2069).
- Moulin, P., & O'Sullivan, J. A. (2003). Information-theoretic analysis of information hiding. *IEEE Transactions on Information Theory*, *49*, 563–593. doi:10.1109/TIT.2002.808134
- Swanson, M. D., Kobayashi, M., & Tewfik, A. H. (1998). Multimedia data-embedding and watermarking technologies. In *IEEE International Conference on Communications*, *2*, 823-827.
- Voloshynovskiy, S., Deguillaume, F., Koval, O., & Pun, T. (2003). Information-Theoretic Data-Hiding for Public Network Security, Services Control and Secure Communications. *IEEE Int. Conf. on Telecomm. in Modern Satellite, Cable and Broadcasting Service*, *1*, 3-17.
- Wong, P. H. W., Au, O. C., & Yeung, Y. M. (2003). A novel blind multiple watermarking techniques for images. *IEEE Trans. on Circuits and Systems for Video Technology*, *13*, 813–830. doi:10.1109/TCSVT.2003.815948
- Zaidi, A., Piantanida, J. P., & Duhamel, P. (2007). Broadcast- and MAC-aware coding strategies for multiple user information embedding. *IEEE Transactions on Signal Processing*, *55*, 2974–2992. doi:10.1109/TSP.2007.893973
- Zaidi, A., & Vandendorpe, L. (2009). Coding schemes for relay-assisted information embedding. *IEEE Transactions on Information Security and Forensics*, *4*(1), 70–85. doi:10.1109/TIFS.2008.2009588

Zamir, R., Shamai (Shitz), S., & Erez, U. (2002). Nested linear/lattice codes for structured multi-terminal binning. *IEEE Transactions on Information Theory*, 48, 1250–1276. doi:10.1109/TIT.2002.1003821

Zaidi, A., & Duhamel, P. (2009). On Rate and BER Analysis for Finite-Dimensional Lattice Coding for the Dirty Paper Channel. International Journal of Electronics and Communications. doi:10.1016/j.aeue.2009.02.010

ADDITIONAL READING

Giakoumaki, A., Pavlopoulos, S., & Koutsouris, D. (2004). A multiple watermarking scheme applied to medical image management. IEEE Int. Conf. on the Engineering in Medicine and Biology Society, 3241-3244.

Liu, T., Moulin, P., & Koetter, R., (2004). On Error Exponents of Nested Lattice Codes for the AWGN Channel. IEEE Information Theory Workshop, 348-352.

Wong, P. H. W., Chang, A., & Au, O. C. (2004). A sequential multiple watermarks embedding technique. IEEE Int. Conf. On Acoustics, Speech and Signal Processing, ICASSP, 393-396.

ENDNOTES

¹ Note that by opposition to superposition coding, there is an important embedding ordering at the encoder. The benefit of such ordering is a decoupling of the receivers and hence a more scalable system. Each receiver needs only know its own codebook to extract its message.

² Note that, theoretically, the decoder looks for the (unique) codeword U_2 such that (U_2, Y) is jointly typical. In practice W_2 however, the decoder only knows an estimate \hat{U}_2 of the codeword U_2 even if W_2 is decoded perfectly, since the host S is unknown at the receiver (see discussion in Section V-B.2).

Chapter 14

Copyright Protection in the Distribution of Multimedia Digital Objects in Internet

Mariví Higuero

University of the Basque Country, Spain

Purificación Saiz

University of the Basque Country, Spain

Marina Aguado

University of the Basque Country, Spain

ABSTRACT

This chapter shows the most significant approaches developed so far for the distribution of digital contents with copyright protection, highlighting their most interesting features. These proposals may be classified into two categories: on the one hand systems that try to prevent unauthorized uses of the contents, and on the other hand systems whose purpose is to detect unauthorized uses of the contents and to identify involved offenders. This chapter is focused on the systems that fit in the second of these strategies, most of which are based on the use of watermarking techniques. However, watermarks cannot provide a suitable answer to this issue by themselves, but they must be framed into more complex systems, involving the participation of different entities and the use of well defined protocols which establish the exchange of data and contents among these entities. It is important to point out that cryptography is also a key element in all of these systems and protocols.

INTRODUCTION

The protection of the copyright in the marketing and distribution of digital materials is a challenge faced by different participants in the sector during

the last years (Digital Rights Management, n.d; Ianella, 2001).

The copyright management in traditional activities, in general, has taken advantage of the physical nature of products to prevent unauthorized uses of them. It was almost always more interesting for users to buy a new object than to make copies of it, due to several reasons: making copies may involve

DOI: 10.4018/978-1-61520-903-3.ch014

considerable time, sometimes a copy can be not much cheaper than a new object, and the quality of the copies may not be attractive. This situation changed significantly when digital technologies and materials were introduced into markets. Digital contents can be easily copied and transmitted through communication networks, and the quality of the materials remains identical regardless of the number of copies made.

The increasing number of technical tools available to users for the processing of digital materials at affordable prices in last years, along with the ease of publication and transmission of digital information through Internet, has resulted in a market where piracy has become a common practice. This situation has revealed the need to protect intellectual property rights of authors of digital contents, as they are easily vulnerable without the use of specific protection measures.

The development of protection measures in the distribution of products in such environments was tackled when the level of piracy began to increase significantly. These activities especially reached significant levels in the 70s; software was the affected product. Later, in the 90s, the deployment of Internet led to the spread of piracy to other types of contents, especially music and video, although any copyrighted digital object may be affected, such as books, databases, confidential business information, etc.

The various efforts made to prevent these attacks to copyright have not been successful so far, mainly due to the lack of robust solutions for most of the situations, and because the different approaches have not been widely accepted by the different parties involved. The fact that Internet has traditionally been considered by most users as a scenario where information can be freely distributed, adds a greater difficulty to the acceptance and implementation of solutions.

The use of watermarking techniques for copyright protection in distribution of digital contents has driven a significant amount of efforts. In most of the proposals the application of these techniques

has been bound to the identification of offenders, although some schemes for protection against copying have also incorporated these technologies.

It is interesting to highlight that watermarks by themselves cannot provide a suitable answer to the above-mentioned issue (Mintzer *et al.*, 1997; Craver *et al.*, 1998), but they must be framed in more complex systems based, in general, on the use of TTP (Trusted Third Parties) (Qiao *et al.*, 1998) or register entities (Petitcolas *et al.*, 1998), and using well defined protocols.

It is also important to highlight the need for standardization (Craver *et al.*, 1998), and legal support of technical solutions for the practical viability of such systems.

This chapter presents the main approaches suggested so far for protecting the copyright of digital contents when they are distributed in Internet; systems based on watermarking will be fitted in them. The chapter includes an analysis of the most important requirements to be taken into account by these systems, and a description of the most relevant approaches developed so far, including an assessment of their main advantages and shortcomings.

STRATEGIES FOR COPYRIGHT PROTECTION

Most systems developed so far for copyright protection of digital contents can be classified into two broad categories corresponding to two different strategies: systems that try to avoid unauthorized uses of contents, and those that try to detect unauthorized uses.

The approaches in line with the first strategy usually involve the use of devices or mechanisms for protection against copying, in order to limit the access to protected materials, or simply to prevent the making of copies. Examples of such systems include systems for censored television broadcasting, or devices to avoid making copies in DVD players and recorders.

On the other side, systems for detection of unauthorized uses do not try to restrict the use of the material; instead they attempt to identify offenders when they carry out unauthorized actions. These approaches usually include techniques to identify offenders when suspicious materials are met. They basically enable the identification of users “source” of fraud, who illegally distribute copies of lawfully acquired contents. Most systems of this type are based on the use of watermarking techniques.

Systems developed following both strategies have faced several problems, which have not yet been completely solved. Nevertheless, nowadays, the advantages and disadvantages of the two approaches seem to tip the scales in favour of detection systems. Most of these systems are based on watermarking techniques.

Problems of the Strategies for Copyright Protection

The systems that try to avoid unauthorized uses of contents raise several problems of different nature, mainly technical problems but also political and commercial.

Among the technical problems, the following ones are highlighted:

- Such systems are usually broken up after a while, losing at that moment any possibility of protection against the making of copies, as Maillet *et al.* (2003) state.
- Another issue in this line is cited by Schneier (2000). He points out that in most systems a decryption key is required to carry out any operation over a content (e.g. viewing the content, or any other process). This fact implies that, as the key is used in the system at some point, it is always possible to develop powerful debug tools to access both the key and the clear content, so the system would become violated.

Other non technical problems are the following ones:

- It is difficult to persuade manufacturers to include devices for copy control on their computers, among other reasons due to the following:
 - The addition of these devices make equipment more expensive without providing buyers with any additional benefit in terms of service, which means a difficulty in the marketing of the equipment.
 - Those devices would not be compatible with current formats, which is not usually advisable when new equipment or content formats have to be introduced.
- Furthermore, the law in many countries is ambiguous. While it prohibits the unauthorized reproduction and sale of copyrighted materials, it also explicitly states that their use for personal enjoyment or educational or research environments (usually within certain limits) is permitted. However, most of the copy control technologies prevent this type of legal uses.

Regarding the systems focused on the detection of unauthorized uses or unauthorized copies, which are mostly based on watermarking techniques, they also present several problems, such as:

- These systems usually make use of a register authority, which may also cause several problems. This entity could be a source of fraud, calling into question the global system. Moreover the register authority can constitute a bottleneck if the number of required operations is high. And sometimes, a conflict resolution implies the disclosure of the secret key of an innocent user, making the rest of his contents vulnerable (Adelsbach *et al.*, 2002).

- It is also often pointed out that systems based on fingerprinting, tracking and analysis of copies make difficult to protect buyers' privacy, as these systems usually entail the storage of information related to buyers (IBM, 2001). In fact the processes involved in fraud detection often entail the identification of buyers, thus preventing anonymity. This problem has almost disappeared in recent years, through the development of several approaches, like the use of aliases (Maillet *et al.*, 2003).
- Another significant problem is related to the standardization and development of a legal framework to support the technical solutions (Qiao and Nahrstedt, 1998; Craver and Katzenbeisser, 2001). It is obvious that a system capable of identifying offenders is not very useful if these violations cannot be punished in any way. As already mentioned these approaches usually provide means to identify illegal use of protected contents, but do not avoid them. Penalty actions would also act as a deterrent to prevent future offenses.
- In this line there are also arguments pointing out that the systems that identify offenders do not assure that actions can be punished, since offenders can argue that the illegally distributed material may previously have been stolen (Atallah *et al.*, 2004).

Bloom *et al.* (1999) mention two practical measures to penalize systems developed to break the protections. The first one is the use of really robust watermarking techniques. A more practical solution consists in the development of a tool to modify or to delete inserted watermarks for the watermarking system used by a company, and the register of a patent for that tool. This way, any software or hardware that uses patented technology to manipulate the material could be punished for a patent infringement.

The remainder of this chapter focuses on systems following the second strategy. Therefore the features and protocols involved in the most relevant copyright protection systems for unauthorized use detection are described hereafter. Systems included are based on watermarking techniques since they are the most significant approaches following this strategy.

SYSTEMS FOR COPYRIGHT PROTECTION BASED ON WATERMARKING TECHNIQUES

The systems for digital contents distribution that enable the detection of illicit copies are based on the use of mechanisms for identifying offenders. Offenders are usually legal buyers that illegally distribute copies of the acquired contents, as mentioned above. The operation of most of these systems is based on the use of watermarking techniques, and more specifically on fingerprinting techniques.

It is important to point out that cryptography is an essential technique in all proposals for contents distribution systems. However, cryptography cannot constitute a solution by itself: it allows secure transmissions of the contents (avoiding unauthorized access) as the contents are encrypted, but it cannot avoid the realization of copies or manipulations on the contents after they have been decrypted by an authorized party.

Watermarking does not constitute either a solution by itself. The mere insertion and detection of a code into a digital material does not provide a guarantee about the identity of the entity that has inserted that code, or about the order of mark insertion if several watermarks are found in a content, etc.

For these reasons most of the approaches presented so far are based on the combination of cryptography and watermarking, and they are usually integrated in complex distributed systems. These systems often define specific operation

frameworks, including features regarding the participants, as well as procedures regarding the processes and information exchanges to make in transactions.

This section starts with an approach to the desirable requirements in a scenario like this, which are: anonymity, low computational cost, ability to detect fraud, and so on. Next, the origin and evolution of the watermarking systems for copyright protection in the distribution of materials are reviewed, and the most significant schemes suggested so far are described. This description includes an analysis and an assessment of the compliance of the requirements by the different protocols, and their main shortcomings.

Requirements

Different systems and protocols presented in recent years exhibit different characteristics that make them attractive for the scenarios where they are presented.

This subsection describes and analyzes the most desirable requirements and features for the practical viability of systems for digital contents distribution with copyright protection. Later, in the description of the most significant systems and protocols, a reference about the requirements met for each system will be included.

Some of the most important requirements are listed below:

- **Anonymity:** Anonymity is a key feature, especially for certain types of contents, so that users are not reluctant to use these distribution systems.
- **Security:** The actions of users should not be traceable by any entity. At the same time the correct identification of offenders should be ensured.
- **Asymmetry:** Operation of the system should not lead to ambiguities in the identification of offenders. This fact implies that the protocols should not provide the same

version of a marked content to two different users or entities.

- **Simplicity for users:** If the use of the system is too complex, or requires many resources, or requires a great expertise from users, the probability of success of the system decreases significantly. The system should not either involve the acquisition and installation of new hardware or software in the users' equipment. These considerations can be summarized by indicating that the complexity of the global system should lie on the side opposite the client, as far as possible.
- **Fraud detection:** The system should provide a detection level as high as possible.
- **Feasible business model:** The business model involved in the distribution system should not be too much complex or too simple; it should not be too different from current business models. Not fulfilling this factor could hinder the practical feasibility of the system.
- **System performance perceived by end users:** The distribution system should be fast in carrying out transactions. Thus customers would not be discouraged to use this type of legal distribution schemes for the purchase of digital material. The penalty introduced by the use of the system is a relevant factor. It may be measured as the difference between the amount of time involved in a downloading of a content making use of a distribution system, and the time involved in a direct downloading of the same content directly from the provider, without using any specific system.

In most cases it is necessary to establish a compromise among different requirements. For example, the techniques introduced to provide security and asymmetry usually penalize performance. In the same way, procedures for anonymity sometimes involve additional operations to

be carried out by users, increasing this way the complexity of a system for them.

It is also important to highlight some requirements related to the watermarking subsystem. The most relevant are the following ones:

- **Robustness:** The watermarking technique used in the system should be as robust as possible. This means that the inserted watermarks should be resistant to different types of attacks.
- **Imperceptibility:** The insertion of a watermark into a digital content must be imperceptible. This feature is dependent on the content type.
- **Security in the detection process:** The operation of the detection process should not affect the security of the system. This means that this process should not entail the disclosure of sensitive information such as private keys of users, etc.
- **Insertion of appropriate watermarks:** The watermarking technique should support the insertion of codes of a length appropriate for each system and content.

Another feature to be taken into account in any distribution system is that buyers who use properly acquired contents should enjoy an adequate service, without being disturbed by these mechanisms. In fact, even though users usually receive information about the transactions they make (e.g. in the form of a ticket), they should not be unfairly penalized if they do not store that information properly (e.g. they may lose or unintentionally destroy the file containing that information). It is also desirable that the buyers could make operations by means of the interaction with only one entity, the vendor.

Protocols for Distribution of Digital Contents with Copyright Protection

This section reviews the main features and the operation of the most relevant distribution models presented so far, and the associated protocols. Some approaches take their name from the corresponding protocol, because its operation is the key part of the model.

First it should be mentioned that all these approaches implement fingerprinting which, as such, was introduced by Wagner (1983). The first basic implementations of this concept not only have various shortcomings such as lack of anonymity for buyers, etc., but also pose a major problem, that is explained in the following paragraph.

A basic scheme of fingerprinting generally involves the realization of slightly different copies of a digital content for each buyer (although the copies are perceptually equal). Thus, from the analysis of one copy, a seller could identify the owner or buyer of that copy. However in the first digital content distribution models based on fingerprinting, both buyer and seller are provided with the same fingerprinted version of the content, which has been generated for the transaction. If a fraudulent distribution of the copy occurred, even if the vendor could identify the buyer responsible for the action, he would not be able to prove to a third party (e.g. a judge) the guilt of the buyer, as it might be argued that it is the seller who distributed illegally the analyzed copy (which could also be true). Such approaches are called symmetric fingerprinting schemes. This feature, the symmetry, is also often called customer's right problem by some authors because they consider that customers' rights are not well protected.

On the other hand, models based on asymmetric fingerprinting only provide buyers with the final fingerprinted version of the digital content. Thus sellers could not access the final version of contents, and there would not be ambiguity in the process for identifying offenders.

Before describing the main features of the related protocols, it is interesting to describe the objectives and operation of a mathematical tool widely used in several proposals for distribution protocols that implement asymmetry. This mathematical tool is the homomorphism.

A function f is defined as homomorphic, or it is said to have the property called homomorphism for an operation op , if it fulfills the following expression:

$$f(x \ op \ y) = f(x) \ op \ f(y)$$

where x and y are two variables from the set of variables for the function f . The operation op is typically an algebraic operation over these data: addition, subtraction, multiplication or division.

The homomorphism of a function f is defined for the operation to be performed (a function can be homomorphic for the addition or subtraction, but not for the multiplication, or it can be homomorphic for all operations, etc...).

A homomorphic operation, in the context of this work, is called a privacy homomorphism, and it enables the making of operations directly over encrypted data. This concept of privacy homomorphism was introduced by Rivest, Adleman and Dertouzos (1978).

The privacy homomorphism in copyright distribution systems implies that the application of encryption to two separate components (in this scenario a digital content V , and the watermark W) and the later realization of the homomorphic operation over both of them, is equivalent to making the homomorphic operation with both components first (what is watermarking the digital content), and then encrypting the result (the watermarked material).

This can be expressed as follows:

$$\{ (V)_K \oplus (W)_K \} = \{ V \oplus W \}_K$$

where V is the content, W the watermark, K the encryption key, and \oplus the operation for inserting the watermark in the content. In this context Λ is the homomorphic operation. The result of this operation:

$$(V \oplus W) \text{ is usually expressed as } V_w.$$

This may be briefly expressed as follows: the application of the homomorphism to the watermarking operations involved in this context consists in the carrying out the watermarking in the ciphered domain. As an application example, a seller could insert a ciphered watermark (he has been provided with somehow) into a ciphered content, so this watermarked content could only be deciphered by the buyer.

This feature is thus what provides the asymmetry in the transactions, avoiding the access to the same watermarked version of a content (deciphered) by two different entities. By means of this asymmetry sellers usually can access all watermarked contents, but those contents are ciphered, so sellers cannot access the final versions of the contents obtained by buyers.

It is important to highlight that not all watermarking techniques support this homomorphism, so a watermarking technique that supports it must be used in the global system.

Asymmetric Fingerprinting Protocols

The development of asymmetric protocols arises from the consideration described just above about the problem faced by symmetric fingerprinting schemes: the ambiguity in resolving the identity of offenders between buyers and sellers.

Pfitzmann and Schunter (1996), and Pfitzmann and Waidner (1997) presented the asymmetric fingerprinting approaches to resolve this problem.

The first of these approaches consists in the use of secure multiparty computation to provide asymmetry to a symmetric protocol, like the approach presented by Wagner (1983), creating this

way an asymmetric fingerprinting protocol. By the use of this technique vendors could not gain access to the final fingerprinted copies obtained by buyers. Thus, when an illicit copy is found only the buyer can be the source of fraud (another different issue is the allocation of guilt in practice, since a buyer could argue that the copy has been stolen to him). Using this technique, the distributors cannot have access to final fingerprinted copies derived by different buyers. After these first works on the development of asymmetry, anonymity was added to these approaches.

The general operation of these systems makes use of four subprotocols: key generation, fingerprinting, identification, and dispute subprotocols, which carry out the functions suggested by their names.

The secure multiparty computation techniques used in these approaches consist in the use of *bit commitment schemes* which are based on the works of Brassard *et al.* (1988). An approach of ‘bit-commitment’ would be a protocol in which an entity A commits itself to providing another entity B with certain information. This information is initially provided in a hidden way, and it only serves as a commitment about the clear information that will be sent in the future. Then, when A reveals the information, B will be able to verify that the received information is exactly what A had previously committed to.

A simple bit-commitment approach could be a protocol between A and B, where A has a message M which B wants to possess. A would send M to B but in a hidden way. For this purpose, A chooses a random string R, and concatenates R with M. Then A would apply a hash function over the concatenated data, and the obtained digest would be sent to B. From that point B already has a proof of what M is, but B does not possess M because hash functions are unidirectional. After a while, A could reveal M, by sending B both the message M and the string R. B would then be able to check if the received M is the previously committed one. In order to perform this verification,

B has to perform the same operation previously performed by A, by concatenating M and R and calculating the digest. If the result coincides with the original proof received from A, M is the committed information.

The bit-commitment approaches proposed by Brassard, Chaume and Crèpau (1988) support the feature of the homomorphism regarding the multiplication of bits, and this is the technique used by Pfitzmann and Schunter (1996) to insert the watermark in a hidden way for the seller.

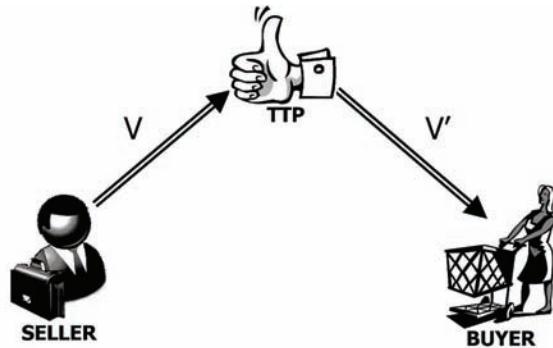
Later Pfitzmann and Waidner (1997) modified this approach to provide anonymity as well. This protocol also makes use of a ‘bit-commitment’ approach to avoid ambiguity in identifying offenders, and uses a zero knowledge proof for verification of signatures.

Details of the homomorphic bit commitment schemes and of the zero-knowledge proof system used in these approaches, which are computationally complex, are provided by Pfitzmann and Schunter (1996), and by Pfitzmann and Waidner (1997).

In subsequent works, Pfitzmann and Sadeghi (1999) presented an approach for asymmetric fingerprinting which employs ideas from the digital cash approach developed by Brands (1999), which is based on a blind signature scheme used by Chaum and Pedersen (1993). This approach is very costly in terms of implementation; moreover, as mentioned by Goi *et al.* (2004), since the system makes use of Boneh and Shaw (1995) codes to strengthen the system against collusion attacks, the scheme does not become practical to implement because of the length of these codes.

Among the most significant subsequent proposals related to these approaches, it is worth highlighting the work presented by Biehl *et al.* (1997) based on the use of the so-called c-secured codes, and the works by Ferrer *et al.* (1998, 1999, 2000). The first of the Ferrer’s approaches (1998) also makes use of the secure multiparty computation tool, based on the proposal by Chaum *et al.* (1988), so its implementation does not result viable

Figure 1. The operation of the TTP Watermarking protocol



from a practical point of view. Later Maillet *et al.* (2003), members of the same working group, state that the approach by Ferrer *et al.* (1999) makes use of a committed oblivious transfer tool which, despite being theoretically correct and feasible, involves such a high computation and communication cost for large objects that the system also becomes impractical. Another proposal presented by Ferrer *et al.* (2000) uses a zero knowledge cryptographic primitive, whose practical implementation is also doubtful.

The TTP Watermarking Protocol

This protocol, proposed by Qiao and Nashrstedt (1998) uses the services of a trusted entity or TTP, independent of content owners and buyers. This TTP acts as an intermediate between sellers (who can also be the owners of the contents) and buyers and avoid a direct contact between them. Its operation, which is summarized below, is shown in the following figure (Figure 1).

In this system, when an owner or seller wants to send any fingerprinted material (V_w) to a buyer, he will just have to send the original material (V) to the TTP, which is the entity responsible for the operation of inserting a watermark in the content (the watermark should be unique for each distributed copy), and for the sending of that copy to the buyer. In addition the TTP must

store some information about the transactions and the involved parties, in order to carry out the corresponding checks, in case of a later conflict.

This protocol guarantees that no fraud based on the watermarking and registration services of the TTP will occur. The TTP provides trust between the parties, and serves as an arbiter when required. The TTP must also validate the identity of participants in transactions, through authentication services and the use of certificates.

The following are the main advantages of this basic protocol with a TTP:

- The services of the TTP allow assuring that every distributed content have a unique watermark. In order to check whether a user who has a material is an authorized customer or not, the TTP will have to check only previously stored data about the corresponding transaction.
- The TTP can use standardized watermarking schemes, trying to guarantee the security of watermarking services.

On the other hand, among the major shortcomings arisen from the operation of this protocol the following ones can be highlighted:

- The reliability and operation of this system is supported by a single entity, in this case the TTP, with the drawbacks this fact can bring. First, the vulnerability of the system is highly dependent on the vulnerability of this TTP. And secondly the TTP in these approaches is a single point of failure and can become a bottleneck because of the need for its participation in all operations, and the magnitude of these operations (checks, watermarking, data storage, etc.), which can be a major problem if the number of operations is high.
- The architecture of this system leads to a too simplified business model. For example if the vendors and the authors of the

digital contents are separate entities, at least another entity should be included in the approach.

- The TTP watermarking protocol does not provide a true anonymity. It is easy to get that the identity of the buyers is not known by the sellers, but the TTP will know the materials the buyers want to buy (along with their identity). Depending on the type of contents being distributed, the anonymity may be a requirement of the system.
- In this scenario the TTP stores all the original contents to be distributed. This means that if the security of the TTP is jeopardized, equally the rights of owners and buyers will be jeopardized, as well as all the stored contents.

The Buyer-Seller Protocol

The Buyer-Seller protocol was developed by Memon and Wong (1998). One of its most relevant features is the use of a privacy homomorphism to avoid ambiguity in the offender identification process. However the proposed framework for the whole process is too simple.

The overall scheme of this Buyer-Seller protocol consists of four different protocols:

- The watermark generation protocol
- The watermark insertion protocol
- The copyright violation detection protocol
- The dispute resolution protocol

Its operation involves the participation of three entities: seller, buyer, and TTP, and it consists of the following actions which start when a buyer wishes to purchase a digital content (X) from an author or seller:

1. First, when a transaction begins, the watermark generation protocol runs. The TTP creates a valid watermark for the buyer from a random sequence (W1), ciphers the

watermark with the buyer's public key ($E_{KB}(W1)$), and generates a digital signature with its own private key ($Sign_{TTP}(E_{KB}(W1))$). Both data (encrypted watermark and its signature) are sent to the buyer.

2. The buyer sends to the seller the encrypted watermark, along with the signature of the TTP. Then the watermark insertion protocol is started in the seller's equipment, and a unique watermark (W2) for this transaction is generated and inserted into the content. A watermarked content (V_{w2}) is obtained. The seller also generates a random permutation of the encrypted watermark $E_{KB}(W1)$ received from the buyer, and inserts it into the content, as a second watermark. This operation is made in the encrypted domain, that is, the encrypted watermark is inserted into the previously encrypted content. Both parts have been encrypted with the buyer's public key. Then the seller sends to the buyer the encrypted and doubly watermarked content $E_{KB}(V_{w1 w2})$.
3. The seller stores the most significant data about the transaction.
4. The buyer deciphers the watermarked content with his private key.

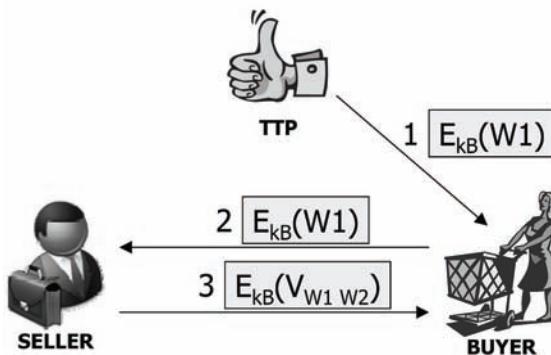
It is interesting to remark that the purpose of the watermark (W2) generated by the seller is to enable the identification of a buyer by the seller when a copy must be analyzed. But this watermark could not be used to prove to a third party (e.g. a judge) that a buyer has illicitly distributed copies of a digital content previously bought.

For the system to work as described, it should use a public-key cryptosystem which is a privacy homomorphism with respect to the operation used to insert the watermarks into the contents.

The following figure (Figure 2) shows the exchange of information taking place in transactions with the Buyer-Seller Protocol.

From this point, the fraud detection process is implemented as follows.

Figure 2. The Buyer-Seller protocol



1. The copyright violation detection protocol enters into operation when a suspicious copy is found, and it must be determined whether it is an authorized copy. In this case, the author (or seller) of the involved content should extract the watermark from the material. The mechanism used to extract the watermark and to find the match among the stored watermarks depends on the watermarking technique used by the seller.
2. If the buyer refuses his guilt, the dispute resolution protocol comes into play. The seller should reveal the permutation used, the encrypted watermark ($E_{KB}(W1)$), and the signature for that censored watermark ($\text{Sign}_{TTP}(E_{KB}(W1))$). A judge could ask the buyer for the first watermark ($W1$). The judge could then encrypt this piece of information with the buyer's public key and check if the result coincides with the data presented by the seller. The first watermark should then be extracted from the digital content and compared to $W1$, to verify the guilt of the buyer.

Now, after the description of the operation of the Buyer Seller Protocol, the main shortcomings of this approach are highlighted.

One of the main drawbacks of this protocol is its high computational cost. Although this computational cost is considerably smaller than in the

above-mentioned protocols by Pfitzmann *et al.*, it is still too high. This is because the insertion of the watermarks in the encrypted domain makes necessary to encrypt the watermarks and the contents. In the Buyer Seller protocol, Memon and Wong include the watermarking technique proposed by Cox *et al.* (1997) to insert watermarks into contents, and the homomorphic algorithm RSA to encrypt, so it is necessary to encrypt the 1000 samples that make up the watermark, to encrypt also the 1000 highest AC coefficients of the Discrete Cosine Transform (DCT) of the image to be watermarked (Cox *et al.* (1997) work with images as the material to watermark), and finally to decrypt the 1000 ciphered and watermarked coefficients as the last step (this last action must be carried out in the buyer's equipment). For encryption, as mentioned, the RSA algorithm is used, which involves a rather high computational cost; this implies a considerably high computational cost of the overall system.

Moreover, as already mentioned, the operation scenario proposed by this system is too simple, and keeps far from current schemes of distribution of digital contents, making more difficult its practical feasibility.

ECMS (Electronic Copyright Management System) Model

This fingerprinting model was presented by Piva *et al.* (2002) and is characterized by the participation of a trusted entity in the transactions to manage the integration of various watermarks in digital contents.

A key aspect of this ECMS system is that asymmetry is not provided, so it does not solve the problem of ambiguity in the identification of offenders between buyers and sellers (since both entities obtain the same deciphered version of the materials, as shown below), and it does not provide anonymity either.

Although this model is not considered feasible in practice due to its lack of asymmetry, it has

been included in this section since it provides some other interesting features. An example of these features is the watermark insertion and distributions strategy. This system enables all parties involved in a transaction to verify for themselves (without the intervention of a trusted third party) if watermarks have been properly inserted and therefore, if their rights have been observed. This technique uses a blind and robust watermarking technique and digital signatures.

One of the basic features of this protocol is that its operation consists of two phases:

- During the first phase the author of a digital content must register the content, and then he must allow different vendors to commercialize that content. This phase is carried out prior to the transactions.
- The second phase consists of the transactions, and takes place every time a buyer buys a content.

Another key feature of the ECMS protocol is that three watermarks are inserted into every distributed content throughout the whole process. The components and meanings of those watermarks are the following ones:

1. The first watermark contains an identifier which relates the author to the digital content. This identifier is called CUN (Creation Unique Number). To build this watermark, the author ciphers the CUN with its private key, Kpr_A . This watermark is inserted into the material by the author.
2. The second watermark consists of the mentioned CUN and the identifier of the distributor or vendor which is called PIN (Personal Identification Number), and relates the vendor to the content. The CUN and the distributor's PIN are encrypted by the author with his private key Kpr_A , building the second watermark.

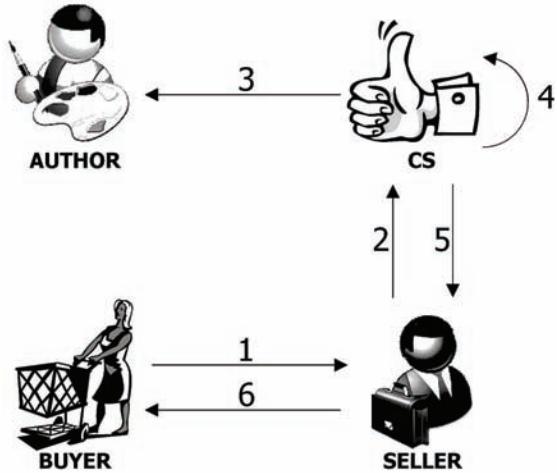
3. Finally, the third watermark consists of the CUN and the buyer's PIN. This watermark will be created by the third trusted party, which is called CS (Collection Society) in this ECMS model. This entity will cipher the CUN and the buyer's PIN with its private key, thus building the third watermark. This watermark will be inserted by the seller.

The use of three watermarks makes possible to have proofs of the participation of the different entities in a transaction with a specific content. That information could be used later to identify an offender or to prove the innocence of the participants.

On the other hand the operation of the protocol can be summarized as follows.

- The first step consists, as mentioned before, in the registration of the digital content. This action involves sending the material to the distributor. To do it in a secure way, the author of the content must create a watermark derived from data about himself (the CUN), insert it into the content, and register the watermarked content in the CS. This way, if someone else tries to register the same material, there is already a prior registration of it, and the authorship remains protected.
- Later, when a vendor wants to sell a registered content he should contact the author and send his own identifier or PIN to him. The author then creates a second watermark from the vendor's PIN and the CUN, which will be encrypted with the author's private key, and inserted into the previously watermarked content, with the aim of showing the author's authorization to the involved vendor.
- Finally, when a customer wants to purchase a digital content and asks for it to the seller, he has to identify himself by providing his PIN, which is used to generate the third

Figure 3.The transaction process in the ECMS distribution model



watermark. This watermark will be inserted by the seller into the material, encrypted with the private key of the CS. This is the transaction phase, and takes place every time a buyer purchases a content.

Figure 3 shows the different steps that make up a transaction.

The operations carried out in each step are:

1. The buyer sends his identifier or PIN to the distributor (seller), along with a request for the content he wants to buy.
2. The vendor sends the buyer's PIN, the CUN of the content, and the second ciphered watermark (which was encrypted with the author's private key) to the CS.
3. The CS lets the author know about the transaction (and about the involved profits).
4. The CS inserts into the content the second watermark, received from the vendor, and creates a third watermark from the CUN of the content and the buyer's PIN. This watermark is sent to the seller encrypted with the private key of the CS.

5. The CS calculates a digest of the watermarked content by means of a hash function, and sends the signed digest to the vendor together with the third encrypted watermark.
6. Finally the vendor inserts the third watermark into the content, and sends the triply watermarked content to the buyer, along with the third watermark and the signed digest he received from the CS in the previous step.

As pointed out before, although the ECMS model is a more sophisticated protocol than other previous developments, with many interesting features, it also presents two significant shortcomings. One is the lack of anonymity for buyers, and the other is the lack of asymmetry. This is because the seller and the customer obtain the same final deciphered version of the document (in this case, triply watermarked) in every transaction.

Another drawback is the high operational load assigned to the CS, in addition to the support of trust among the different parties. As shown, the CS in this model takes part in the purchase of every content, registering transactions and storing data, as well as inserting the corresponding watermarks into the materials.

Asymmetric Fingerprint Model with a TTP

Ferrer *et al.* analyzed and questioned the practical viability of their previous developments in asymmetric fingerprinting (1998, 1999, 2000) based on secure multipart computation schemes, on oblivious transfer tools and on zero knowledge proof. As a result of this analysis and questioning, they presented a different approach of a fingerprinting system based on the use of a TTP (2003).

This protocol makes use of the services of a TTP, which all participants in the transactions must trust in, and which implements some similar functions to those usually provided by a PKI (Public Key Infrastructure). This approach

involves a much lower computational cost than previous approaches.

The participating entities in this model are the following ones:

- Seller
- Buyer
- Fingerprinting authority (FA): the entity responsible for watermarking operations.
- Register authority (RA): the TTP, the entity that provides trust among the other entities in the system.

The basic operation of this system is shown in the following figure (Figure 4) and can be summarized as follows.

- A buyer who wants to acquire a digital content must first obtain a pseudonym for the transaction from the RA.
- After sending the purchase request to the seller, this entity sends to the FA the requested content and other data related to the transaction.
- Finally, the FA watermarks the material with the corresponding code and passes the material to the buyer.

In this model the seller has not access to the watermarked versions of the copies bought by the buyers, thus avoiding ambiguity in the identification of offenders between sellers and buyers when a suspicious copy is analyzed.

This approach also includes the use of digital signatures, as well as the sending of ciphered information among the entities with the aim of providing secure transactions.

On the other hand this approach uses the technique presented by Boneh and Shaw (1995) to generate the codes to be inserted into digital contents in order to make the system stronger against collusion attacks. As the watermarking algorithm should be as robust as possible, the

techniques presented by Ferrer and Sebe (2001, 2002) are suggested.

The entities participating in this system store several data about every transaction they take part in, as evidence of their participation or to identify possible offenders. The stored data should allow the identification of at least one of the participants in case of collusion attacks.

Distribution Models Derived from the Previous Ones

Some of the protocols presented so far have given rise to a significant number of subsequent proposals that are based on them and that try to improve some of their drawbacks. In this line, the buyer-seller protocol is one that has influenced a greater number of works.

This section includes a brief description of some of the main proposals that, as indicated, have been derived from the protocols presented above.

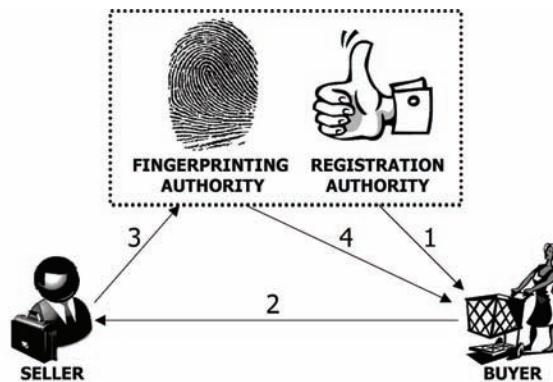
The Buyer-Reseller Watermarking Protocol

This buyer-reseller protocol developed by Curreem and Cheung (2001) tries to provide a strategy for the redistribution of digital contents in second hand markets over the Internet. It is based on the buyer-seller protocol described above, which does not provide mechanisms for performing resale operations of lawfully bought contents, since it does not address the possibility of a change of the ownership of contents. The buyer-reseller protocol covers this space, hence its name.

This approach also tries to avoid another shortcoming of the buyer seller protocol which consists in buyers' having to reveal the watermarks in the dispute resolution process when analysing suspicious copies of contents.

The buyer-reseller scheme is based on the use of certificates of the watermarks for each transaction. The watermark certificate of a buyer ($WCert_B$) consists of an encrypted watermark $E_{K_B}(W)$, the public key of the buyer K_B , and

Figure 4. Transactions in the asymmetric model with a TTP



the buyer's digital signature of the encrypted watermark $\text{Sign}(E_{KB}(W), K_B)$. This watermark certificate is generated to prevent anyone from using the buyer's encrypted watermark in other purchase operation.

It also implements a mechanism to transfer the property rights of buyers, so they could legally resell previously bought digital contents. This function is implemented by a new entity called Content Distributor (CD), which registers data about the contents' rightholders at every moment.

An Enhanced Secure Buyer-Seller Watermarking Protocol

This proposal from Chang and Chung (2003) is also based on the buyer seller protocol. This approach tries to improve the security of the buyer seller protocol addressing some issues, like the unbinding problem and the customer verification problem.

The unbinding problem is derived from the lack of a mechanism for binding a watermark generated for a transaction to the involved digital content, which can be used by the seller to use it again to embed it into other higher value content.

The verification problem refers to the fact that customers cannot usually check the originality of the obtained contents.

In this system presented by Chang and Chung the watermark is generated by the TTP from the public keys of buyers and sellers, and from a product-copy number ID. In addition a watermark identification number is used, which allows buyers and sellers to verify the originality of the purchase content.

An Efficient and Anonymous Buyer-Seller Protocol

This approach from Lei *et al.* (2004) also tries to improve some features of the buyer-seller protocol.

This system implies the insertion of two watermarks into digital contents. One of them is known by the sellers and used by them to identify offenders as a first quick step. And the second one, unknown to the sellers, would be used by an arbiter to determine if the involved buyers are innocent or not.

In addition this protocol solves the unbinding problem, already described. This feature is provided by means of a watermark certification authority, which creates the watermarks for specific contents and verifies the validity of these watermarks when necessary.

Anonymity is achieved in this model by means of anonymous certificates. These are digital certificates with a pseudonym as the content of their subject fields (instead of the real identity), being the certification authority the responsible for binding the certificate to the real identity of the applicant.

Another enhanced feature of this protocol is that buyers only have to contact sellers during the transactions.

Secure Buyer-Seller Watermarking Protocol

This approach from Zhang *et al.* (2006) presents another model based on the buyer-seller protocol, but in this case without the services of the TTP. The aim is to avoid the problems derived from the participation of this entity. This approach is based on shared secrets, through the insertion of

a watermark composed of two pieces of secret information, one generated by the seller and the other one by the buyer.

A Privacy Preserving Buyer-Seller Watermarking Protocol with Semi-Trust Third Party

This approach presented by Shao (2007) improves the buyer seller approach by means of the use of a notary entity (the semi-trusted third party) in addition to a trusted certification authority. The functions of the notary are to verify the integrity of the exchanged data, and to certificate the validity of watermarks created by the buyers.

In this protocol the unbinding problem is addressed by using digital signatures to link the buyer's watermark and the one-time public key created for the corresponding transaction.

This approach does not require that the buyer participates in the dispute resolution procedure, unlike the buyer seller protocol.

A Practical Digital Watermarking Protocol Based on PKI-CA

This system presented by Chen *et al.* (2007) aims to add features to the buyer-seller protocol for becoming it closer to traditional distribution patterns as well as improving its efficiency and security.

Its operation is based on the services of a so-called PKI-CA (Public Key Infrastructure-Certification Authority) entity which is the certification authority of the system, but also implements a watermarking generation and storage function.

This protocol, like the approach from Lei *et al.* (2004), makes use of two watermarks: one inserted by the seller and the other one by the PKI-CA. The first of these watermarks is used by the seller for a quick search for unauthorized copies, while the second one would have to be used by an arbitrator or judge to establish the guilt or innocence of a buyer. This last watermark is generated for each buyer and remains hidden for security reasons. It also makes easier the transactions carried out by a purchaser with a particular vendor since, after a first purchase has been made with a seller, the

following purchases with the same seller will not involve data exchange with the PKI-CA, increasing the speed of the purchase operations.

This protocol also avoids buyers having to show their watermarks associated with suspicious copies in the conflict or dispute resolution phase, as well as the unbinding problem mentioned above.

Other Buyer-Seller Watermarking Protocols

Another approach based on the buyer seller scheme was presented by Ju *et al.* (2002), with the aim of providing anonymity. It assumes a fully trusted watermark certificate authority.

Another interesting proposal not very different from the previous one, is the Choi *et al.* (2003) approach where the authors analyze and avoid some attacks by which two entities of the system (e.g. seller, and watermark server) could form an alliance to obtain the watermark assigned to a buyer, and use it later to distribute illicit copies so that the legal buyer is blamed. This scheme makes use of the El Gamal cryptosystem.

Just the opposite point of view is stated by Goi *et al.* (2004) which avoid the participation of the certification authority in transactions (although they include a certification authority to guarantee the validity of public keys of all participants). They consider that anonymity support in previous schemes is not very robust, since they are based on the fact that watermarking certificate authorities are trusted entities and do not reveal identities.

The proposal from Deng and Preneel (2008) incorporates secure group signature schemes to provide anonymity, traceability and some other security features.

A New Watermarking Protocol for Copyright Protection

This protocol by Ru *et al.* (2006) tries to improve some security features of the ECMS model. It involves the participation of a certificate authority which is also a copyright authority in the system. This protocol makes use of signatures and timestamps to register contents with the aim

of avoiding later ambiguity problems related to the intellectual property of the contents. This approach also enhances the security of the ECMS model against some well-known attacks previously identified by several authors like Craven *et al.* (1997) and Adelsbasch *et al.* (2003). However, despite these improvements this protocol, like the ECMS model, does not support asymmetry, so its operation is not considered feasible in practice.

SecDP Protocol

The so-called SecDP (Secure Distribution Protocol) protocol by Higuero (2005) tries to include some features derived from the traditional purchase operations in its business model. This approach also includes ideas derived from the buyer-seller protocol and from the ECMS model.

This protocol is based on a privacy homomorphism to support asymmetry, and on the services of a digital editorial to register the contents.

Through the transactions the buyers only have to contact the sellers, and the operations are faster than those involved in other protocols also based on similar privacy homomorphisms. It makes use of encryption and digital signatures to provide additional security.

Other Approaches

Other approaches are referred to several specific aspects of the distribution models, different from transactions. Some significant examples of this statement are the following ones.

Chang and Chang (2004) presented a specific scheme for watermark building based on the use of bar-codes and signatures. The system encodes a message into a bar-code including the buyer's identification, the seller's name, the object name, the object number, the price, and the timestamp. This code is built with error correcting capability, so it is robust against various attacks.

Cheung *et al.* (2004) developed a commutative encrypted protocol with the aim of improving some security shortcomings of previous approaches.

This system makes use of a protocol fulfilling the following commutative property: If a message m is doubly encrypted, first using a key K , and afterwards with another key K' , the result is equivalent to performing the encryption in reverse order. This can be expressed as: $E_{K_1}(E_{K_2}(m)) = E_{K_2}(E_{K_1}(m))$. In this system the involved seller and buyer encrypt consecutively the content; as a consequence the buyer cannot access the original unencrypted content, and the seller does not have access to the final watermarked content. In addition this approach does not require either that buyers reveal sensitive data in case of conflict.

Some other approaches are focused on the process of embedding watermarks, and they make proposals of new methods usually based on cryptosystems with homomorphic properties. Kurabayashi *et al.* (2001, 2004, 2008) present several proposals related to the method for embedding encrypted watermarks in encrypted contents. Their technique applies the additive homomorphic property avoiding some problems related to its implementation.

On the other hand Zhao *et al.* (2007) propose a new method based on a version of the El Gamal cryptosystem with additive property aiming to reduce the computational load involved in the watermark insertion process in the encrypted domain.

FUTURE RESEARCH DIRECTIONS

There are still some open issues in the development of systems for distribution of digital contents in Internet.

Firstly, a truly robust watermarking scheme should be developed. Many features related to security should be taken into account in the design of these approaches, but the usefulness of the whole system depends on the robustness of the watermarking system. For this reason, the more robust watermarking schemes are against false positives and negatives in the identification

of offenders, the greater the chances will be to succeed for systems that rely on those schemes to distribute contents.

Furthermore, a lot of efforts have been carried out so far in the research and development of watermarking techniques for images as the involved contents, and also for audio although to a lesser extent. Therefore the development of watermarking schemes adequate enough for other types of contents such as video is considered an important challenge. It would be interesting to have robust enough watermarking techniques for video, with an adequate performance.

Another pending issue is the development of systems that meet all the defined requirements and not just part of them:

- On the one hand it is very important that the systems offer some features to users, such as anonymity, simplicity, speed, etc., so users do not deter from using this type of system for downloading digital contents. Some work should be done into the improvement of robustness and operation of digital contents distribution systems, so that they become interesting for distributors of contents, and at the same time operate properly on platforms affordable to users, so that this form of shopping also becomes attractive for the buyers.
- And on the other hand the similarity of these approaches to the schemes traditionally used for content distribution is a key factor to get acceptance from the involved parties (in this sector) as well as to facilitate the migration from the traditional operation patterns. The various players in this economic sector are reluctant to change their business models. They are aware that the processes of production and distribution of contents have changed dramatically, but they find it hard to change their form of participation in the market to the same extent, as they feel the volume of

their profit threatened. For these reasons it is considered that the new business models in which the role of the different players is as close as possible to their current roles may have a greater chance of success.

And finally it should not be forgotten the importance of the development of a legal framework for the support of such content distribution schemes. It is noteworthy the work carried out by the administrations of many countries in recent years to protect the copyrights of authors, but further progress must still be done in this line. The proper functioning of such systems for digital contents distribution would be useless without a proper legal framework supporting them.

CONCLUSION

This chapter has described the main features of the most relevant proposals of systems for distribution of digital contents with copyright protection based on the use of watermarking techniques.

The described approaches are based on the combination of encryption and watermarking, and make use of various techniques to meet the set of requirements defined in each case. But almost all systems present drawbacks which affect their viability. Some of the most common shortcomings are the lack of asymmetry, the lack of anonymity, the high computational load involved, and the difference with the business models established today.

Anyway, one of the main problems of these systems often argued by authors is that a sufficiently robust watermarking technique has not yet been developed, which poses a handicap to the success of these systems.

Moreover, the need for standardization and development of the legal framework to support these technical solutions cannot be obviated, as they are key factors for the success of such systems.

REFERENCES

- Adelsbach, A., Katzenbeisser, S., & Sadeghi, A. (2002). Cryptography Meets Watermarking: Detecting Watermarks with Minimal or Zero Knowledge Disclosure. In *European Signal Processing Conference (EUSIPCO 2002)*, (Vol. I, pp. 446-449), TESA, France.
- Adelsbach, A., Katzenbeisser, S., & Veith, H. (2003). Watermarking schemes provably secure against copy and ambiguity attacks. In *3rd ACM Workshop on Digital Rights Management*, (pp. 111-119). New York: ACM.
- Atallah, M., Prabhakar, S., Frikken, K., & Sion, R. (2004). Digital rights protection. *A Quarterly Bulletin of the Computer Society of the IEEE Technical Committee on Data Engineering*, 27, 19–26.
- Biehl, I., & Meyer, B. (1997). Protocols for Collusion-Secure Asymmetric Fingerprinting. In *Proc. 14th Annual Symposium on Theoretical Aspect of Computer Science*, (LNCS Vol. 1200, pp. 399-412). Berlin: Springer-Verlag.
- Bloom, J. A., Cox, I. J., Kalker, T., Linnartz, J. M. G., Miller, M. L., Brendan, C., & Traw, S. (1999). Copy protection for DVD video. *Proceedings of the IEEE*, 87(7), 1267–1276. doi:10.1109/5.771077
- Boneh, D., & Shaw, J. (1995). Collusion-secure fingerprinting for digital data. *IEEE Transactions on Information Theory*, 44(5), 1897–1905. doi:10.1109/18.705568
- Brands, S. (1993). Untraceable off-line cash in wallet with observers. Advances in Cryptology - Crypto'93. (LNCS Vol. 773, pp. 302-318). Berlin: Springer-Verlag.
- Brassard, G., Chaum, D., & Crèau, C. (1988). Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37, 156–189. doi:10.1016/0022-0000(88)90005-0
- Chang, J., & Chang, L. (2004). A new image copyright protection algorithm using digital signature of trading message and bar code watermark. In *Image and Vision Computing New Zealand 2003*. Palmerston North, New Zealand: Massey University.
- Chaum, D., Damgaard, I., & Van de Graff, J. (1987). Multiparty computations ensuring privacy of each party's input and correctness of the result. In *Advances in Cryptology - Crypto'87*, (LNCS Vol. 293 pp. 87-119). Berlin: Springer-Verlag.
- Chaum, D., & Pedersen, T. P. (1992). Wallet databases with observers. *Advances in Cryptology - Crypto'92*. (LNCS Vol. 740, pp. 89-105). Berlin: Springer-Verlag.
- Chen, X., Zhu, D., & Liu, J. (2007). *A practical digital watermarking protocol based on PKI-CA*. *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, SNPD 2007* (Vol. 1, pp. 483–488). Washington, DC: IEEE Computer Soc.
- Cheung, S., Leung, H., & Wang, C. (2004). A Commutative Encrypted Protocol for the Privacy Protection of Watermarks in Digital Contents. In *37th Annual Hawaii International Conference on System Sciences (HICSS'04)*. Washington, DC: IEEE Computer Society.
- Cheung, S. C., & Curreem, H. (2002). Buyer-Reseller Watermarking Protocol for MP3 Music. In *26th Annual International Computer and Applications Conference (COMPSAC 2002)*, (pp. 105-110).
- Choi, J. G., Sakurai, K., & Park, J. H. (2003). Does it Need Trusted Third Party? Design of Buyer Seller Watermarking Protocol without Trusted Third Party. In *Applied Cryptography and Network Security ACNS'03*. (LNCS Vol. 2846, pp. 265-279). Berlin: Springer-Verlag.

- Cox, I., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673–1687. doi:10.1109/83.650120
- Craver, S., & Katzenbeisser, S. (2001). Copyright Protection Protocols Based on Asymmetric Watermarking. In *Fifth Conference on Communication and Multimedia Security (CMS'01)*, (pp. 159-170). Boston: Kluwer Academic Publishers.
- Craver, S., Memon, N., Yeo, B. L. & Yeung, M. M. (1998). Can invisible watermark resolve rightful ownerships? *IEEE Journal on Selected Areas in Communications. Special issue on copyright & privacy protection*, 16(4), 573-586.
- Deng, M., & Preneel, B. (2008). On Secure and Anonymous Buyer-Seller Watermarking Protocol. Internet and Web Applications and Services - ICIW '08, (pp. 524-529).
- Digital Rights Management. (n.d.). Retrieved May, 15, 2009, from Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Digital_rights_management.
- Ferrer, J. D. (1999). Anonymous fingerprinting based on committed oblivious transfer. Public Key Cryptography, (LNCS Vol. 1560, pp. 43-52). Berlin: Springer-Verlag.
- Ferrer, J. D., & Herrera-Joancomartí, J. (1998). *A privacy homomorphism allowing field operations on encrypted data. Jornades de Matemàtica Discreta i Algorísmica*. Spain: University Rovira i Virgili.
- Ferrer, J. D., & Herrera-Joancomartí, J. (2000). Efficient smart-card based anonymous fingerprinting. Smart Card Research and Applications. (LNCS Vol. 1820, pp. 231-238). Berlin: Springer-Verlag.
- Ferrer, J. D., & Sebe, F. (2002). Enhancing watermark robustness through mixture of watermarked digital objects. *International Conference on Information Technology: Coding and Computing. - ITCC'2002*. (pp. 85-89). Washington, DC: IEEE Computer Society.
- Goi, B., Chung-Wei, R., Yang, Y., Bao, F., Deng, R. H., & Siddiqi, M. U. (2004). Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity. *Applied Cryptography and Network Security - ACNS 2004*. (LNCS Vol. 3089, pp. 369-382). Berlin: Springer-Verlag.
- Higuero, M. V. (2005). *Modelo de distribución de contenidos digitales marcados en Internet, con protección de derechos de copyright. Evaluación y optimización de la seguridad del protocolo mediante metodologías de análisis de riesgos*. Unpublished doctoral dissertation, University of the Basque Country, Spain.
- Iannella, R. (2001). Digital rights management (DRM) architectures. *D-Lib Magazine*, 7(6). Retrieved May 15, 2009, from <http://www.dlib.org/dlib/june01/iannella/06iannella.html>
- IBM. (2001). *Watermark standarization for DVD copy protection*. Retrieved May, 15, 2009, from http://www.trl.ibm.com/projects/RightsManagement/datahiding/dhvgx_e.htm
- Ju, H. S., Kim, H. J., Lee, D. H., & Lim, J. I. (2002). An anonymous buyer-seller watermarking protocol with anonymity control. *Information Security and Cryptology - ICISC 2002*, (LNCS Vol. 2587, pp. 421-432). Berlin: Springer-Verlag.
- Kurabayashi, M., & Morii, M. (2008). On the implementation of asymmetric fingerprinting protocol. In *16th European Signal Processing Conference (EUSIPCO-2008)*. European Association for Signal Processing.

- Kuribayashi, M., & Tanaka, H. (2001). A new anonymous fingerprinting scheme with high enciphering rate. In *Progress in Cryptology - INDOCRYPT 2001*. (LNCS Vol. 2247, pp. 30-39). Berlin: Springer-Verlag.
- Kuribayashi, M., & Tanaka, H. (2004). *A watermarking scheme applicable for fingerprinting protocol*. *Digital Watermarking* (Vol. 2939, pp. 532–543). Berlin: Springer-Verlag.
- Lei, C. L., Yu, P. L., Tsai, P. L., & Chan, M. H. (2004). An efficient and anonymous buyer-seller watermarking protocol. *IEEE Transactions on Image Processing*, 13(12), 1618–1626. doi:10.1109/TIP.2004.837553
- Maillet, C., Martínez-Ballesté, A., Sebé, F., & Ferrer, J. D. (2003). *Prototipos del proyecto STREAMOBILE. (STREAMOBILE TIC-2001-0633-C03)*, University Rovira i Virgili, Spain. Retrieved May, 15, 2009, from <http://crises-deim.urv.cat/projects/spanish/streamobile/demo1/report.streamobile.pdf>
- Martínez-Ballesté, A., Sebé, F., & Ferrer, J. D. (2003). Aspectos prácticos de la protección de la propiedad intelectual en contenidos multimedia. *II Simposio Español de Comercio Electrónico (SCE'03)*, (Vol. II, pp. 219-228), Universitat Politécnica de Catalunya, Spain.
- Memon, N., & Wong, P. W. (2001). A buyer-seller watermarking protocol. *IEEE Transactions on Image Processing*, 10(4), 643–649. doi:10.1109/83.913598
- Mintzer, F., Braudaway, G. W., & Yeung, M. M. (1997). Effective and ineffective digital watermarks. *IEEE International Conference on Image Processing*, (Vol. 3, pp. 9-12). Santa Barbara, CA.
- Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1998). Attacks on copyright marking systems. *Information Hiding: Second International Workshop*, (LNCS Vol. 1525, pp. 218-238). Berlin: Springer-Verlag.
- Pfitzmann, B., & Sadeghi, A. R. (1999). Coin-based anonymous fingerprinting. *Advances In Cryptology- Eurocrypt'99*, (LNCS Vol. 1592, pp. 150-164). Berlin: Springer-Verlag.
- Pfitzmann, B., & Schunter, M. (1996). Asymmetric fingerprinting. *Advances in Cryptology -Eurocrypt'96*. (LNCS Vol. 1070, pp. 84-95). Berlin: Springer-Verlag.
- Pfitzmann, B., & Waidner, M. (1997). Anonymous fingerprinting. *Advances In Cryptology - Eurocrypt'97*. (LNCS Vol. 1233, pp. 88–102). Berlin: Springer-Verlag.
- Piva, A., Barni, M., & Bartolini, F. (2002). Managing copyright in open networks. *IEEE Internet Computing*, 6(3), 18–26. doi:10.1109/MIC.2002.1003126
- Qiao, L., & Nahrstedt, K. (1998). Watermarking schemes and protocols for protecting rightful ownership. *Journal of Visual Communication and Image Representation*, 9(3), 194–210. doi:10.1006/jvci.1998.0391
- Rivest, R., Adleman, L., & Dertouzos, M. (1978). *On data banks and privacy homomorphisms*. *Foundations of Secure Computation* (pp. 169–179). New York: Academic Press.
- Schneier, B. (2000). *Secrets and lies. digital security in a networked world*. Chichester, UK: John Wiley and Sons, Inc.
- Sebe, F., & Ferrer, J. D. (2002). Oblivious image watermarking robust against scaling and geometric distortions. In *4th International Conference on Information Security*. (LNCS Vol. 2200, pp. 420-432). Berlin: Springer-Verlag.
- Shao, M.-H. (2007). A privacy-preserving buyer-seller watermarking protocol with semi-trust third party. *Trust, Privacy and Security in Digital Business*, (LNCS Vol. 4657, pp. 44–53). Berlin: Springer-Verlag.

- Wagner, N. R. (1983). Fingerprinting. In *IEEE Symposium on Security and Privacy 1983*, (pp. 18-22).
- Zhang, J., Kou, W., & Fan, K. (2006). Secure buyer-seller watermarking protocol. *IEE Proceedings Information Security*, 153(1), 15–18. doi:10.1049/ip-ifs:20055069
- Zhang, R., Yu, X., Zhou, L., & Li, H. (2006). Anew watermarking protocol of copyright protection. In Intelligent Information Hiding and Multimedia Signal Processing - IIH-MSP '06. (pp. 83-88). Washington, DC: IEEE Computer Soc.
- Zhao, B., Dang, L., Kou, W., Zhang, J., & Cao, X. (2007). Design of secure watermarking scheme for watermarking protocol. Advances in multimedia information processing - PCM 2007, (LNCS Vol. 4810, pp. 357-366). Berlin: Springer-Verlag.
- Cox, I. J., & Miller, M. L. (2002). The first 50 years of electronic watermarking. EURASIP Journal on Applied Signal Processing: Vol. 2002. I. 1 (pp. 126–132). Hindawi Publishing Corp.
- Cox, I. J., Miller, M. L., & Bloom, J. A. (Eds.). (2002). *Digital Watermarking*. Morgan Kauffman Publishers.
- Eskicioglu, A. M. (2003). Protecting Intellectual Property in Digital Multimedia Networks. Computer.: Vol. 36. I. 7 (pp. 39–45). IEEE Computer Soc.
- Gjosteen, K. (2003). Homomorphic public-key systems based on subgroup membership problems. Progress in Cryptology - Mycrypt 2005. Vol. 3715 (pp. 314-327).
- Gopalakrishnan, K., Memon, N., & Vora, P. L. (2001). Protocols for watermark verification. IEEE Multimedia. Vol. 8, I. 4 (pp. 66-70).
- Hartung, F., Su, J. K., & Girod, B. (1999). Spread spectrum watermarking: malicious attacks and counterattacks. [SPIE-Int Soc Optical Engineering]. *Security and Watermarking of Multimedia Contents*, 3657, 147–158.

ADDITIONAL READING

- Adelsbach, A., Katzenbeisser, S., & Sadeghi, A. R. (2003). Watermark detection with zero-knowledge disclosure. *Multimedia Systems*: Vol. 9. LNCS, I. 3 (pp. 266–278). Berlin, Germany: Springer-Verlag.
- Adelsbach, A., Katzenbeisser, S., & Veith, H. (2003). *Watermarking Schemes Provably Secure Against Copy and Ambiguity Attacks*. 3rd ACM workshop on Digital rights management (pp. 111–119). USA: ACM.
- Carracedo, J. (Ed.). (2004). Seguridad en redes telemáticas. McGraw-Hill/Interamericana de España, S.A.U.
- Chor, B. A., Fiat, A., & Naor, M. (2000). Tracing Traitors. *IEEE Transactions on Information Theory*: Vol. 46. I. 3 (pp. 893–910). IEEE-Inst Electrical Electronics Engineers Inc.
- Higuero, M. V., Unzilla, J. J., Jacob, E., Saiz, P., & Luengo, D. (2004). Application of ‘Attack Trees’ technique to copyright protection protocols using watermarking and definition of a new transactions protocol SecDP (Secure Distribution Protocol). *Interactive Multimedia and Next Generation Networks*: Vol. 3311. LNCS(pp. 264–275). Berlin, Germany: Springer-Verlag.
- Jonhson, N. F., Duric, Z., & Jajodia, S. (Eds.). (2001). *Information Hiding. Steganography and Watermarking – Attacks and Countermeasures*. Kluwer Academic Publishers.
- Katzenbeisser, S. (2004). *On the Integration of Cryptography and Watermarks. Digital Watermarking*(Vol. 2939, pp. 50–60). Berlin, Germany: Springer-Verlag.

- Katzenbeisser, S., & Dittmann, J. (2004). Malicious attacks against media authentication schemes based on invertible watermarks. *SPIE Security and Watermarking of Multimedia Contents VI*, 5306, 838–847.
- Katzenbeisser, S., & Petitcolas, F. A. (Eds.). (1999). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House Books.
- Koch, E., Rindfrey, J., & Zhao, J. (1996). *Copyright Protection for Multimedia Data. Digital Media and Electronic Publishing* (pp. 203–213). Academic Press.
- Kundur, D., & Karthik, K. (2004). Digital fingerprinting and encryption principles for digital rights management. *IEEE [IEEE-Inst Electrical Electronics Engineers Inc]. Special Issue on Enabling Security Technologies for Digital Rights Management*, 92(6), 918–932.
- Lehman, B. A., & Brown, R. H. (1995). *Intellectual Property and the National Information Infrastructure*. USA: The Report of the Working Group on Intellectual Property Rights. Library of Congress Cataloging-in-Publication Data.
- Petitcolas, F. A. (2008). Information Hiding & Digital Watermarking: An Annotated Bibliography. Retrieved May, 15, 2009, from <http://www.petitcolas.net/fabien/steganography/bibliography/>.
- Petitcolas, F. A. P. (2003). MosaicAttack [Online]. Retrieved May, 15, 2009, from <http://www.petitcolas.net/fabien/watermarking/2mosaic/index.html>.
- Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—a survey. *Proceedings of the IEEE*. Vol. 87, I. 7 (pp. 1062-1078). IEEE-Inst Electrical Electronics Engineers Inc.
- Pfitzmann, B., & Waidner, M. (1997). Asymmetric Fingerprinting for Larger Collusion. *4th ACM Conference on Computer and Communications Security*. (pp. 151–160). ACM, USA.
- Sharman, R. K., & Decker, S. (2001). Practical Challenges for digital watermarking applications. *IEEE Fourth Workshop on Multimedia Signal Processing*. (pp. 237-242).
- Tirkel, A. Z., Rankin, G. A., Van Schyndel, R. M., Ho, W. J., Mee, N. R. A., & Osborne, C. F. (1993). Electronic Watermark. *Digital Image Computing, Technology and Applications (DICTA'93)*. (pp. 666–673).
- Wagner, D. (2003). Cryptanalysis of an Algebraic Privacy Homomorphism. *Information Security.: Vol. 2851. LNCS* (pp. 234–239). Berlin, Germany: Springer-Verlag.
- WIPO. World Intellectual Property Organization. (n.d.). Retrieved May, 15, 2009, from <http://www.wipo.int/>
- Zhao, J. (1997). Applying Digital Watermarking Techniques to Online Multimedia Commerce. *International Conference on Imaging Science, Systems, and Applications (CISSA '97)*.

KEY TERMS AND DEFINITIONS

Asymmetric Fingerprinting: Fingerprinting systems that only provide buyers with the final fingerprinted version of the digital contents. Thus when a fraudulent copy is found there is no ambiguity in the process of identifying offenders.

Business Model: Framework for marketing and distribution of products. This term can refer to a broad range of aspects involved in business.

Copy control Systems: Devices and technologies for protection against unauthorized making of copies.

Copyright: Rights derived from the realization of an original literary, artistic, or scientific work. These rights are granted by law and belong to the author or authors of the work.

Copyright Protection: Action to protect and safeguard intellectual property rights associated with creations for the benefit of the authors.

Digital Contents Distribution Protocol: Set of rules which establish the exchange of data and contents among the entities that participate in the distribution of digital contents.

Piracy: Unauthorized use or making of copies of literary, musical, audiovisual or software works, thus violating the copyright.

Privacy Homomorphism: Cryptographic function that allows performing the same operations on both the ciphered data and the deciphered data.

Symmetric Fingerprinting: Fingerprinting systems that provide two or more parties with the final fingerprinted version of the digital contents. Thus when a fraudulent copy is found there is ambiguity in the process of identifying offenders.

Section 4

Optimization and Hardware Implementation of Watermarking Algorithms

Chapter 15

Optimization in Digital Watermarking Techniques

Santi P. Maity

Bengal Engineering and Science University, India

Claude Delpha

Laboratoire des Signaux et Systèmes (L2S), France & Université Paris-SUD XI, France

ABSTRACT

Digital watermarking (DWM) becomes a multidisciplinary research area involving theory of communications, signal processing, multimedia coding, information theory, cryptography, computer science and game theory etc. This chapter looks digital watermarking as an optimization problem from different combination of these areas. The goal is to resolve the conflicting requirements of different parameters and properties of digital watermarking. The chapter also presents a review of recent advances in the state-of-the-art algorithms for optimized watermarking techniques. Optimized watermarking methods are then discussed from the rigorous mathematical analysis to theoretical derivations of algorithms with the aid of soft computing techniques. The design and implementation of optimized watermarking methods for the image, video and sound signals are discussed in the context of various diverse applications. Finally, the scope of future research in this area is highlighted.

INTRODUCTION

The widespread use of Internet and wireless networks, the blooming growth in consumer electronic devices and the advancement in digital techniques to achieve high compression rate, altogether make it possible nowadays to acquire multimedia streams easily. Hence, the owner as well as the users of multimedia data is under real threat due to the

growing concern of copyright infringement, illegal distribution, unauthorized tampering and security in communication (Cox, 2001; Wu, 2003). Digital watermarking and information hiding that deal with an acceptable embedding of an auxiliary data in the digital media become a potential solution to the class of problems over the last decade. Several diverse disciplines, namely communication, signal processing, information theory, computer science to very large scale integration (VLSI) technology for real time implementation make it an attractive

DOI: 10.4018/978-1-61520-903-3.ch015

research field. Digital watermarking (DWM) promises to meet plurality of applications varying from the conventional applications to the several new and promising applications like quality of service (QoS) assessment in future generation wireless communication, data indexing, medical transcription, lured application etc (Eggers, 2002). Nature, the best teacher of us, encourages learning the analogy of the biological systems to handle the challenges in the algorithm and application for information hiding too (Pan, 2009). In this chapter, the terms watermarking, data hiding and information hiding have been used interchangeably and indicate the same meaning while the term stego is used mostly to emphasize statistical non-detectability in data hiding.

Development of digital watermarking algorithm experiences a trade-off relationship to meet several essential properties. These properties, to cite some, include: the quality of the multimedia content containing the hidden data called imperceptibility, the security of the hidden data in term of statistically non-detection, the number of bits that can be embedded with the limits of acceptable quality called capacity, and the robustness indicating the capability to withstand the intentional or unintentional signal processing operations, called attacks. Interestingly, the properties have their own limitations, and they might have conflict to one another (Pan, 2004). For instance, hiding more information with a given decoding reliability degrades perceptual quality of the digital content to a great extent or maintains perceptual quality at the cost of robustness. The primary goal of watermarking is to develop efficient embedding strategy so that watermark fits the cover signal as maximally as possible. It is also required that the watermark symbol is expected to be detected/decoded reliably from various possible degraded versions of the watermarked signal.

Mathematical theory of digital communication in general and the information theory in particular was used in digital watermarking system design to evaluate the ultimate limits of the performance

achievable by any watermarking scheme subject to very general constraints, such as maximum allowed embedding and attacking distortions. Some interesting but surprising results are obtained by looking at digital watermarking from an information theoretic perspective. One such result is the independence of watermark detection/decoding reliability with/without the presence of host signal during decoding. Another benefit obtained by looking at digital watermarking from an information theoretic perspective is that such an analysis provides a number of hints on optimal attacking and decoding/detection strategies (Barni, 2004).

Soft-computing, a sub-branch of computer science is rich with many optimization tools. In digital watermarking, genetic algorithms (GAs) may be used to design several optimized algorithms for better trade-off in imperceptibility, robustness and security. Artificial neural networks (ANN) may be used to design robust watermarking for images to take advantages of relatively easy algorithmic specification, pattern matching and classification while designing optimized algorithms. The feasibility of support vector machine (SVM) may be explored to determine automatically where the significant blocks are and to what extent the intensities of the block pixels can be modified (Pan, 2004). Chaotic dynamic system may be used to generate sequences with spectrum properties such as lowpass or highpass characteristics in order to design optimized watermarking with respect to certain types of attacks (Feng, 2006). The soft computing techniques clubbed with wavelets such as probabilistic neural network and wavelets, spiking neural network and wavelets, GA and wavelets are also used extensively for better optimization in data hiding problems (Pan, 2009).

Although knowledge of different diverse disciplines have been applied in watermarking research, major emphasis is focused everywhere to resolve the conflicting requirements with an objective to develop optimized watermarking systems. The goal of this chapter is to view this optimization in digital watermarking from mathematical per-

spective to the application of bio-inspired soft computing methods.

BACKGROUND

Optimization in Watermarking: Analysis from the Mathematical Perspective

A great many digital watermarking algorithms have been proposed in this still emerging field. Early works mostly viewed digital watermarking as a digital communication problem. Two popular techniques, namely spread spectrum (SS) modulation (Cox, 1997) and quantization-index-modulation (QIM) (Chen, 2001) dominate mostly to resolve the conflicting requirement of digital watermarking. Several signal processing tools in the form of transforms have been used, namely discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), wavelet packets, M-band wavelets etc. to decompose host signals. Most of the SS watermarking algorithms make use of signal processing tools to meet the conflicting goal simultaneously. On the other hand, QIM appears from strong mathematical perspective with host signal interference (HSI) rejection. This has proven to be preferable and optimal in terms of the achievable performance trade-off among distortion, rate and robustness of the embedding. Several optimized QIM watermarking algorithms have been developed using distortion compensation, called as dither modulation (DM), spread transform dither modulation (STDM) and trellis coded quantization (TCQ) etc. (Chen, 2001). First, we will discuss on optimized watermarking schemes based on SS and various QIM, one after another from mathematical perspective. This analysis is also used to discuss other optimized watermarking schemes developed by using soft computing tools.

Spread Spectrum Watermarking

In SS watermarking, major attention of research community is focused on embedding single bit (zero-rate) information, although other works have also been developed to consider payload issue. However, we will develop SS watermarking here for multiple bit embedding. While mathematical analysis is used to optimize single bit SS watermark, several soft computing based methods are discussed for optimization in multiple bit SS watermarking.

Let B denotes the binary valued watermark bit string as a sequence of M bits.

$$B = \{ b_1, b_2, b_3, \dots, b_M \}, b_i \in \{1, 0\}$$

Let the symbol x denotes the original signal i.e. vector of length N in original domain or transform coefficients. A binary valued code pattern i.e. “chip sequence” u of length N with zero mean and whose elements are equal to $+\sigma_u$ or $-\sigma_u$, is used to spread each watermark bit. Thus a set P of M code patterns, each of length N , are generated to form the spread watermark sequence u_Q by performing the following operation

$$u_Q = \sum_{j=1}^M b_j u_j \quad (1)$$

The sequence u_j is added to or subtracted from the x according to the variable $b_j \in \{1, 0\}$, mapped to $+1$ or -1 . The watermarked signal s can be written as

$$s = x + \alpha u_Q = x \pm \alpha \sum_{j=1}^M b_j u_j \quad (2)$$

The above form is additive multiple bit SS watermarking. The parameter α is the gain factor or modulation index and its proper choice will optimize the maximum amount of allowed distor-

tion and minimum watermark energy needed for reliable detection (Maity, 2007). SS watermarking schemes can be called as signal adaptive or non-adaptive whether α is a function of original signal or not. The value of α may be positive or negative, integer or real and may vary continuously thus giving rise to the scope of setting embedding distortion to any desired value.

In SS watermarking, the detection reliability for the binary valued watermark data depends on the decision variable r_i obtained by evaluating the zero-lag spatial cross-covariance function between the watermarked signal s and each code pattern u_i (Depovere, 1998). The decision statistics r_i can be mathematically written as

$$r_i = \langle u_i - m_1(u_i), s - m_1(s) \rangle (0) \quad (3)$$

where $m_1(L)$ represents the average of the sequence L. If l_k represents the elements of L with $k=1,2,3,\dots,M$, $m_1(L)$ can then mathematically be expressed as follows:

$$m_1(L) = \frac{1}{M} \sum_{k=1}^M l_k \quad (4)$$

The symbol (0) in equation (3) indicates the zero-lag cross-correlation. The zero-lag cross-correlation, for two sequences L and R, is given by

$$\langle L, R \rangle (0) = \frac{1}{M} \sum_{k=1}^M l_k r_k \quad (5)$$

where l_k and r_k are the elements of sequences L and R, respectively and $k=1,2,3,\dots,M$. If the code patterns u_i are chosen so that $m_1(u_i)=0$ for all i , the computation of r_i becomes;

$$\begin{aligned} r_i &= \langle u_i, [s + \alpha \sum_{j=1}^M b_j u_j - m_1(s)] \rangle \\ &= \langle u_i, s \rangle + \alpha \sum_{j=1}^N b_j \langle u_i, u_j \rangle - \langle u_i, m_1(s) \rangle \\ &= \langle u_i, s \rangle \end{aligned} \quad (6)$$

The first and the second terms in equation (6) represent the host signal interference (HSI) and multiple bit interference (MBI), respectively.

The i-th embedded bit is detected as follows:

$$\hat{b}_i = \text{sgn}(r_i) = \text{sgn}(\langle u_i, [s + \alpha \sum_{j=1}^M b_j u_j] \rangle (0)) \quad (7)$$

where sgn represents signum function and acts as a hard detector. The bit $b_{i,0}$ is detected as **0** if $r_i > 0$ and as **1** otherwise.

The SS watermarking may be categorized into two group based on the embedding payload, namely zero-rate (one bit) SS watermarking and high payload (i.e. multiple bit) SS watermarking. We will address optimization separately, first zero-rate SS watermark optimization analytically and high payload system using soft computing tools.

ZERO-RATE OPTIMIZED SS WATERMARK SYSTEM: REDUCTION IN HSI

We rewrite the expression of equation (2) for zero-rate watermarked signal with embedding strength $\alpha = 1$, and including additive channel noise as follows:

$$y = s + n = x + bu + n \quad (8)$$

where y represents the noisy watermarked data. The estimation of embedded bit, using equations (7) and (8), becomes

$$\begin{aligned}\hat{b} &= \text{sgn}(r) = \text{sgn}\left(\frac{\langle y, u \rangle}{\langle u, u \rangle}\right) \\ &= \text{sgn}\left(\frac{\langle bu + x + n \rangle}{\langle u, u \rangle}\right) = \text{sgn}(b + x + n)\end{aligned}\quad (9)$$

A good example of optimized zero-rate SS watermark system design is reported in (Malvar, 2003) in the form of improved SS (ISS). An attempt has been made to reduce or even eliminate the presence of host signal as interference, achieving a much higher robustness to additive noise than conventional SS. The authors assume the original signal x and the noise n , as the samples from uncorrelated white Gaussian random processes as $x_i \sim \eta(0, \sigma_x^2)$, $n_i \sim \eta(0, \sigma_n^2)$. Following the additive SS watermarking and correlation detection, the analysis shows that an error probability p can be achieved provided the condition

$$N\sigma_u^2 > 2(\text{erfc}^{-1}(p))^2(\sigma_x^2 + \sigma_n^2) \quad (10)$$

is satisfied. The equation allows a trade-off between the length of the chip sequence N with the energy of the sequence σ_u^2 , given the other variables involved.

To compensate for the host signal interference, the authors develop improved SS (ISS), where the amplitude of the inserted chip sequence is varied by a function $\mu(x, b)$. For simple mathematical analysis, μ is first restricted as a linear function. The watermarked signal becomes

$$s = x + (\alpha b - \lambda x)u \quad (11)$$

The parameters α and λ control the distortion level and removal of the carrier distortion on the detection statistics. Following the same correlation detection and for the same expected distortion $E[D] = \sigma_u^2$ as in SS, it is found that

$$\alpha = \sqrt{\frac{N\sigma_u^2 - \lambda^2\sigma_x^2}{N\sigma_u^2}} \quad (12)$$

The error probability p can be computed as

$$p = \frac{1}{2} \text{erfc}\left(\sqrt{\frac{N\sigma_u^2 - \lambda^2\sigma_x^2}{2(\sigma_n^2 + (1-\lambda)^2\sigma_x^2)}}\right) \quad (13)$$

A careful look on equations (12) and (13) show that proper selection of the parameter λ allows the error probability (robustness) in the ISS several order of magnitude better than conventional SS, when the expected distortion (imperceptibility) and the noise variance (attack distortion) are same. It can be inferred from the expression of error probability that the optimum value of λ is usually close to unity. The optimum value for λ can be computed by setting $\frac{\partial p}{\partial \lambda} = 0$ and is given by

$$\lambda_{opt}(p) = \frac{1}{2} \left(\left(1 + \frac{\sigma_n^2}{\sigma_x^2} + \frac{N\sigma_u^2}{\sigma_x^2} \right) - \sqrt{\left(1 + \frac{\sigma_n^2}{\sigma_x^2} + \frac{N\sigma_u^2}{\sigma_x^2} \right)^2 - 4 \frac{N\sigma_u^2}{\sigma_x^2}} \right) \quad (14)$$

For N large enough, $\lambda_{opt}(p) \rightarrow 1$, as $\text{SNR}\left(\frac{\sigma_x^2}{\sigma_n^2}\right) \rightarrow \infty$.

The authors also compute the noise tolerance gain of ISS over traditional SS, i.e. how much larger can σ_n^2 (for ISS) be compared with σ_{n0}^2 (SS) for the same average distortion and same probability of error. The optimal design for ISS is obtained for the parameter λ such that σ_n^2 is maximized i.e. the improved system can tolerate the maximum amount of noise. It is easy to show λ_{opt} (noise) as

$$\lambda_{(opt)}(\text{noise}) = \frac{N\sigma_u^2}{N\sigma_u^2 + \sigma_x^2 + \sigma_{no}^2} \quad (15)$$

For the optimal design, the allowable noise level can be written as

$$\sigma_n^2 = \sigma_{no}^2 + \lambda_{opt} \sigma_x^2 \quad (16)$$

If $\lambda_{opt} \approx 1$, and SNR ($\frac{\sigma_x^2}{\sigma_n^2}$) is high, it is possible to have $\sigma_n^2 >> \sigma_{no}^2$.

Finally, the authors analyze the more generic case, where the function $\mu(x)$ is not restricted to be linear. The expression for the watermarked signal becomes:

$$s=x+\mu(x,b) \quad (17)$$

The distortion for a certain value of x is

$$d(x)=(\mu(x))^2 \sigma_u^2 \quad (18)$$

The objective is to find the function $\mu(x)$ that minimizes the expected detection error probability $p_e = E\{p_e(x)\}$ for a given expected distortion $D = E\{d(x)\}$. They compute $p_e(x)$ as

$$p_e(x) = \frac{1}{2} erfc\left(\frac{x + \mu(x)}{\sigma_n \sqrt{2}}\right) \quad (19)$$

To be optimum, $\mu(x)$ must satisfy $\frac{\partial}{\partial d} p_e(x) = k'$, for some constant k' . Therefore, an optimum solution of $\mu(x)$ has to satisfy

$$\frac{\partial}{\partial \mu} d(x) = 0 \text{ or } \frac{\frac{\partial}{\partial \mu} p_e(x)}{\frac{\partial}{\partial \mu} d(x)} = k' \quad (20)$$

From (20), the first condition is satisfied only for $\mu(x)=0$. The second condition can be written as

$$\frac{\frac{\partial}{\partial \mu} erfc\left(\frac{x + \mu(x)}{\sigma_n \sqrt{2}}\right)}{2\mu(x)} = k' \quad (21)$$

$$\Rightarrow \exp^{-((x + \mu(x)) / (\sigma_n \sqrt{2})^2)^2} = K\mu(x) \quad (22)$$

where K is another constant. However, there is no closed form solution for $\mu(x)$, and numerical technique can be used to solve.

ZERO-RATE OPTIMIZED SS WATERMARK SYSTEM: INCREASE IN WHC

An interesting study is recently reported in (Kumar, 2007) in the context of additive SS embedding and blind detection correlation of random phase watermarks in audio signal. Instead of trying to minimize HSI, in other words watermark-to-host correlation (WHC), the authors argued that one could also attempt in time domain additive watermarking scheme based on random phase watermark to harness this increased correlation. The authors analyze the problem in other way such that the detection success is based on the margin between the correlations of the watermark to a legitimately watermarked signal and an unwatermarked signal. In other words, an increased WHC is achieved when there is a legitimate watermark present in the audio signal as compared to that of an unwatermarked or alternately watermarked case.

We will not present the detail mathematical analysis; instead highlight the important results and the conditions for maximizing WHC advantages. However, interested readers can go through (Kumar, 2007) for more details. The authors define the host vector as $x \equiv x[n]$, $0 \leq n \leq N-1$, and define a real-valued random phase sequence $p \equiv p[n]$, $0 \leq n \leq N-1$, with its phase spectrum $\theta_p[k]$, that satisfies the following conditions:

$$\theta_p[k] \in \{0, \pi\}, k=0, N/2$$

$$\theta_p[k] \in (-\pi, +\pi), 1 \leq k \leq N/2-1$$

$$\theta_p[k] = -\theta_p[N-K], 0 \leq k \leq N-1 \quad (23)$$

They define time-domain sequence $p[n]$ is given by $p[n] = F_N^{-1}(e^{j\theta_p[k]}), n, k \in \{0, 1, \dots, N-1\}$, where F_N^{-1} denotes the N-point IDFT (inverse discrete Fourier transform) operation.

The actual watermark sequence w is computed from the host through the shaping process. This is defined, in general form, as

$$w = \phi(p, x) \quad (24)$$

The watermarked vector can be expressed as in equation (24). Let us assume that the available signal is z , with or without a watermark embedded. The goal of the watermark detector is to verify the presence of a particular watermark sequence w , which is characterized by the specific random phase sequence p . For blind detection, x is not available at the decoder, and generation of w is not possible from equation (24). The problem is overcome by deriving $w' \equiv w'[n], 0 \leq n \leq N-1$ from the available signal z with an assumption that z is a close approximation to s (this is quite true for imperceptibility requirement of watermarking). Similar to the equation (9), the correlation coefficient is

$$\rho_{zw'} = \frac{z^T w'}{\|z\| \|w'\|} \quad (25)$$

Hypotheses H_1 : Legitimate watermark present

$$z = x + \alpha w \quad (26)$$

The test statistics under this hypothesis is denoted as $(\rho_{zw'}, H_1)$.

Hypotheses H_0 : Legitimate watermark absent

$$z = x + \alpha v \quad (27)$$

where v is any N-length watermark vector (including the zero vector). It is to be noted that $v \neq w$, i.e. $v=0$ or $v = \phi(q, x)$ when $q \neq p$, a different random phase sequence. The test statistics under this hypothesis is denoted as $(\rho_{zw'}, H_0)$.

Let us now assumed that the available signal z contains u , arbitrary watermark signal (legitimate, alternate or zero). We can write z as: $z = w + \alpha u$. Let the legitimate watermark of interest is w . The correlation coefficient $\rho_{zw'}$ can be written as

$$\rho_{zw'} = \frac{z^T w'}{\|z\| \|w'\|} = \frac{x^T w'}{\|z\| \|w'\|} + \alpha \frac{u^T w'}{\|z\| \|w'\|} \equiv \xi_{zw'} + \alpha \eta_{zw'} \quad (28)$$

The first term is the WHC, the correlation between the host and the examined watermark while the second term is the correlation of the later and the embedded watermark. The second term is zero, when no watermark is present. It is desirable that $E\{\xi_{zw'}\} \approx 0$ and $E\{\eta_{zw'}, H_1\} \approx 1$. This essentially gives the mean separation $\Delta\rho_{zw'} (= E\{\rho_{zw'}, H_1\} - E\{\rho_{zw'}, H_0\})$ of α between the two hypothesis. The authors argued that it is advantageous to have $E\{\xi_{zw'}, H_0\} \approx 0$ but, $E\{\xi_{zw'}, H_1\} > 0$. They have shown the intended result for the suggested watermarking scheme, under certain conditions.

Finally, it has been shown that $E(\Delta\xi_{zw'}) = \frac{\alpha}{2}$ which is the increased WHC in the legitimate case. The increased WHC of $\frac{\alpha}{2}$ is obtained if the phase difference ($\beta_{sp}[k] = \frac{2}{\pi} \theta_s[k] - \theta_p[K]$) between the host signal and the watermark is uniformly distributed in $(-\pi, +\pi)$. The work also verifies that a uniformly distributed watermark

phase is a sufficient condition for achieving the maximum advantage of increased WHC.

OPTIMIZATION IN QUANTIZATION INDEX MODULATION WATERMARKING

Chen and Wornell (Chen, 2001) propose an optimal information embedding system called quantization index modulation (QIM) that rejects host-signal interference effect. The embedding function $s(x; m)$ is viewed as an ensemble of function of x , indexed by m , where m indicates the message to be hidden. According to the property of watermarking, to satisfy the condition of small embedding-induced distortion, each function in the ensemble must be close to an identity function in some sense so that $s(x; m) \approx x, \forall m$. To meet robustness against perturbations, the points within the domain of one function in the ensemble should be as much as away from the domain of any other function, at the least possible case, domain should be non-intersecting. This non-intersecting property essentially leads to host-signal interference rejection. The above two properties suggest that the desired functions be discontinuous. Quantizers corresponds to a class of discontinuous, approximate identity functions, hence, the name quantization index modulation. Properties of the quantizer ensemble can be related directly to the performance parameters of rate, distortion and robustness. Intuitively, the minimum distance among the ensemble of embedding functions measures the size of perturbation vectors that can be tolerated by the system. For the bounded channel perturbations, $\|y - s\|^2 = \|n\|^2 \leq N \sigma_n^2$, the minimum distance decoder is guaranteed not to make an error as long as

$$\frac{d_{\min}^2}{4N\sigma_n^2} > 1 \quad (29)$$

where y is the noisy watermarked signal, s is the watermarked signal, d_{\min} is the minimum distance.

To improve rate-distortion-robustness trade-off in QIM, a post-quantization processing called distortion compensation (DC) may be applied. The corresponding embedding scheme is called distortion compensated quantization index modulation (DC-QIM). Scaling of all quantizers by $\alpha \leq 1$, for a fixed rate and a given quantizer ensembles, increases d_{\min}^2 by a sale factor of $1/\alpha^2$. This increases the robustness of the embedding. On the other hand, the embedding-induced distortion also increases by a factor of $1/\alpha^2$. This may be compensated by adding back a fraction $(1-\alpha)$ of the quantization error. The resulting embedding function is

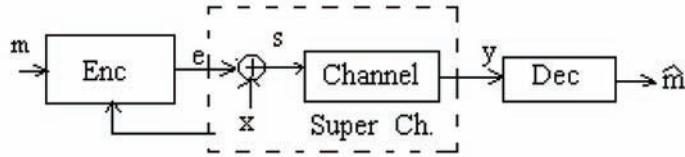
$$s(x, m) = q(x; m, \Delta / \alpha) + (1 - \alpha)[x - q(x; m, \Delta / \alpha)] \quad (30)$$

The first term represents normal QIM embedding while the second term as the distortion-compensation term. The term $q(x; m, \Delta / \alpha)$ corresponds to the m -th quantizer and its reconstruction points have been scaled by α . The recombination points previously separated by a distance Δ before scaling, are now being separated by a distance Δ / α after scaling.

Mathematical form of equation (30) closely reveals the fact that the quantization error added back is a source of interference to the decoder. Robustness can be increased by decreasing α that leads to greater minimum distance. But for a fixed embedding-induced distortion, the distortion compensation interference at the decoder increases which in turn affects robustness performance. One optimality criterion for choosing α is to maximize signal-to-noise ratio (SNR) at the decision device and is written as

$$SNR(\alpha) = \frac{d_1^2 / \alpha^2}{(1 - \alpha)^2 D_s / \alpha^2 + \sigma_n^2} = \frac{d_1^2}{(1 - \alpha)^2 D_s + \alpha^2 \sigma_n^2} \quad (31)$$

Figure 1. Super channel model for information embedding



SNR represents the ratio between the squared minimization distance between quantizers and the total interference energy containing both distortion-compensation interference and channel interference. The term d_1 is the minimum distance corresponding to $\alpha=1$ and is a characteristic of the particular quantizer ensemble. It can be easily verified that the optimal scaling parameter α that maximizes SNR is

$$\alpha_{opt} = \frac{DNR}{DNR + 1} \quad (32)$$

where DNR is the (embedding induced) distortion-to-noise ratio D_s / σ_n^2 .

A canonical “hidden QIM” structure is suggested that consists of 1) preprocessing of the host signal, 2) QIM embedding, and 3) post-processing of the quantized host signal to form the composite signal. In hidden QIM, equivalent super-channel model for information embedding is made use. An auxiliary random variable u is generated from x , and, in turn, e from u and x . Figure 1 shows equivalent super channel model to understand the concept. While the mapping from x to u , in general, probabilistic, e is a deterministic function of (u,x) . In this case, the capacity is

$$C = \max_{p_{u,e|x}} I(u; y) - I(u; x) \quad (33)$$

where $I(\cdot, \cdot)$ denotes mutual information.

DC-QIM scheme, when viewed as a form of hidden QIM, is found that u is a quantized version

of αx . The authors have argued that suitably coded versions of DC-QIM can achieve capacity. This needs maximizing distribution $p_{u, e|x}$ in equation (33) in a form such that the post-processing is linear i.e. e is generated according to

$$e = u - \alpha x \quad (34)$$

The authors have shown that one can construct an ensemble of random DC-QIM codebooks that satisfy equation (34) to achieve capacity. It is easy to understand that quantizing x is equivalent to quantizing αx with a scaled version of the quantizer and scaling back the result i.e.

$$q(x; m, \Delta / \alpha) = 1/\alpha q(\alpha x; m, \Delta) \quad (35)$$

where $q(\cdot, \cdot, \cdot)$ is as defined in equation (30). Rearrangement of terms in the DC-QIM embedding function in equation (30) and substituting equation (35) into the result, it is found that

$$\begin{aligned} s(x; m, \Delta / \alpha) &= q(x; m, \Delta / \alpha) + (1-\alpha) \\ [x - q(x; m, \Delta / \alpha)] &= \alpha q(x; m, \Delta / \alpha) + (1-\alpha)x \\ &= q(\alpha x; m, \Delta) + (1-\alpha)x \end{aligned} \quad (36)$$

Random DC-QIM codebooks are constructed by choosing the codewords of $q(\cdot; m, \Delta)$ from the i.i.d distribution p_u . This is one by maximizing pdf in equation (33) together with the host pdf p_x . It is seen from equation (36) that

$$s(x, m) = x + [q(\alpha x; m, \Delta) - \alpha x] = x + (u_0 - \alpha x) \quad (37)$$

Since $s(x, m) = x + e$, it is seen that $e = u_0 - \alpha x$.

Finally, the ultimate performance limits of information-embedding methods are studied when both the host signal is white and Gaussian. The channel is AWGN and the host and channel noise are independent of one another. It is shown that DC-QIM is optimal for this class of channels. In addition, the optimum distortion-compensation parameter α is also given by equation (32), which maximize SNR in uncoded DC-QIM systems. For squared-error distortion-constrained, Gaussian information embedding is equivalent to power-constrained communication over Gaussian channel with Gaussian side information known at the encoder. This typical case, for which Costa (Costa, 1983) has determined the capacity to be, expressed in terms of the (embedding induced) DWR (document –to- watermark ratio)

$$C_{\text{Gauss}} = \frac{1}{2} \log_2 (1 + DNR), \quad DNR = D_s / \sigma_n^2 \quad (38)$$

It is interesting to note that capacity is independent of the signal variance σ_x^2 . This is also found to be same when the host signal x is known at the decoder. This in other words mean that an infinite energy host signal causes no decrease in capacity in this Gaussian case, i.e. good information-embedding systems can completely reject host-signal interference in the Gaussian case.

To establish the optimality of DC-QIM for Gaussian channel, it is sufficient to verify that equation (34) is satisfied. The pdf that maximizes equation (33) is indeed one implied by equation (34). For some parameter α , where u is chosen as a function of x so that $e \sim \eta(0, D_s)$ and the pair e and x are independent. It is to be noted that for a fixed value of α , an achievable rate $I(u; y) - I(u; x)$ is

$$R(\alpha) = \frac{1}{2} \log_2 \left(\frac{D_s (D_s + \sigma_x^2 + \sigma_n^2)}{D_s \sigma_x^2 (1 - \alpha)^2 + \sigma_n^2 (D_s + \alpha^2 \sigma_x^2)} \right) \quad (39)$$

which can also be written in terms of the DWR and the host SNR ($\text{SNR}_x = \sigma_x^2 / \sigma_n^2$)

$$R(\alpha) = \frac{1}{2} \log_2 \left(\frac{DNR(1 + DNR + \text{SNR}_x)}{DNR(1 - \alpha)^2 \text{SNR}_x + (DNR + \alpha^2 \text{SNR}_x)} \right) \quad (40)$$

This rate is maximized by setting

$$\alpha_{\text{cap}} = \frac{DNR}{DNR + 1} \quad (41)$$

It is interesting to see that in QIM, host signal is considered as the side information of a Costa's popular scheme "writing on dirty paper" (Costa, 1983). By leading on the result of (Costa, 1983), the capacity of informed watermarking scheme is optimal since the side information is not considered as a nuisance signal. A practical and efficient implementation of the Costa's ideas is the scalar Costa scheme (SCS) proposed by Eggers (Eggers, 2003) which is quite similar to the distortion compensated QIM (DC-QIM) watermarking.

Similar to imperceptibility-robustness trade-off in watermarking, a trade-off between security i.e. statistical invisibility and robustness exists in steganography in active warden context. A widely used security measure is the closeness of probability density function (pdf) of the host and the marked signal defined by Cachin (Cachin, 1998). This decision criterion is the Kullback-Leibler distance (KLD) or also called relative entropy. The scalar Costa scheme (SCS) is robust to AWGN attack for optimal value of Costa's factor α , but is drastically insecure since its probability density function for Gaussian host signal is severely discontinuous. To avoid this problem, a modification of SCS is introduced in (Guilon, 2002). The scheme uses a compressor before embedding the watermark to equalize the histogram of the host signal with a non-linear function. After encoding, an inverse compression step is applied to the watermarked

signal with uniform pdf in order to reconstruct the signal with the original pdf. However, the gain in security is achieved at the cost of lower robustness since one has to choose $\alpha=0.5$. It is impossible to choose the optimal value of α which allows a good robustness facing an AWGN attack.

An interesting investigation of asymptotically scalar quantizers is reported in (Boyer, 2006) to address QIM watermark detection with i.i.d host data and additive noise. The work keeps the upper bound of the embedding distortion and the miss probability fixed. It minimizes the false-alarm probability of detection. Interestingly, the authors have used KLD between the watermarked and the non-watermarked data in order to avoid the intractability of false-alarm probability. The object is to find the quantizer which maximizes the false-alarm error under distortion constraints. The optimization problem is solved using a quantizer updating Lloyd-Max-like procedure through Lagrange multiplier minimization. To study analytic performance, the authors have modeled host and noise signals as Gaussian like. The simulation results have shown notably enhanced performance by using proposed application-optimized quantizers in comparison with uniform or Lloyd-Max quantizers. It has also been shown that gain is effective even for small number N of sample at the detector input. The gain becomes more substantial as N grows. The authors have also remarked that good quantizers in terms of distortion are not suitable for detection task.

SPREAD TRANSFORM WATERMARKING

In (Chen, 2001), the authors describe the spread transform (ST) in the context of robust watermarking. They model the system as a way to improve the robustness of watermarking. In ST watermarking, the watermark is not directly embedded into the original signal x , but into the projection x^{ST} of x onto a random sequence t . It

is to be noted here that the term “transform” as introduced by Chen and Wornell, is somewhat misleading since ST watermarking is mainly a pseudo-random selection of a signal component x^{ST} to be watermarked. Let us assume that τ denotes the spreading factor, meaning that data element x_n to be embedded in x_l^{ST} will be spread on τ data elements by the inverse ST. The spread transform (ST) can be computed by

$$x_l^{ST} = \sum_i x_n t_n$$

Any algorithm can be applied to embed a watermark into x^{ST} to obtain s^{ST} . The watermarked data is computed by the inverse spread transform

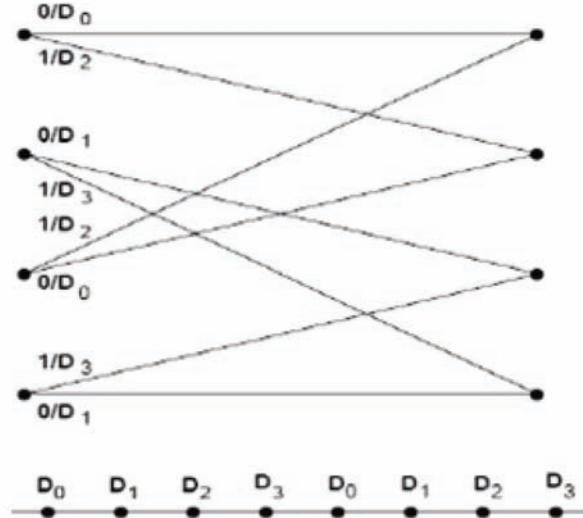
$$s_n = x_n + w_l^{ST} t_n$$

The basic idea behind the robustness improvement in ST watermarking is that an attacker, not knowing the exact spreading direction t , has to introduce much larger distortions to impair a ST watermark as strong as a watermark embedded directly into x .

In (Braci, 2008a), the authors have shown by simulations and theoretical formulation that the Spread Transform(ST) also makes some quantization based stegosystems statistically undetectable. The message is better preserved, by using the ST, if the warden becomes active and introduces distortions. In (Braci, 2009a), the authors give theoretical justifications explaining how the ST increases the stego-message security level, in a realistic case (images). They have argued that steganographic performance improvement is achieved due to the two fold reasons as stated below.

1. The spread transforms hide the stego-message in a pondered average of host samples
2. The message spreading smoothes the stego-signal probability density function and makes it close to the cover signal density function.

Figure 2. Four state trellis with four sub-code books



Trellis Coded Quantization and Watermarking

Trellis Coded Quantization (TCQ) is a quantization method using a structured codebook which has been applied in watermarking specially for quantized based schemes. Inspired from Trellis Coded Modulation (TCM) (Marcellin, 1990) this method was generally used for reducing system complexity and distortion. This quantization technique is based on the partitioning idea proposed by Underboëck (Ungerboëck, 1987). This approach consists in partitioning an initial codebook (structured codebook) in complementary sub-codebooks (with same length), associated to the transitions between the states of a convolution code. Thus, for coding a sample sequence with TCQ, Viterbi algorithm (Viterbi, 1967) is used for obtaining the transitions in the trellis associated with the convolution code which best minimises the distortion. Each transition of the trellis is coded on \mathbf{b} bits. Thus, the $\mathbf{n} \cdot \mathbf{b}$ resulting bits are used for indexing the codeword in the chosen sub-codebook associated to the transition.

The following figure represents a four state trellis with 4 sub-codebooks D_0, D_1, D_2, D_3 .

In watermarking applications, quantization with TCQ is proposed to avoid the regular partitioning generally obtained with scalar quantization. Moreover, such type of quantizer is preferred to enhance the partitioning codebook and then improve the distortion introduced on the watermarked signal PDF (statistical undetectability).

To apply TCQ in watermarking, the trellis' paths are set by the bits values of the message. The host signal samples are quantized by using the sub-codebook corresponding to the taken transition. Thus the embedding rate is fixed to one bit by sample. This approach is called TCQ path selection (TCQ-PS) (Esen, 2003) and can be fully described as follow.

Let us consider a trellis defined by the transition function:

$$E \times \{0,1\} \rightarrow e$$

$$t : (e_i, m[i]) \rightarrow e_{i+1}$$

$E = \{0, 1, \dots, 2^{r-1}\}$, corresponds to the set of possible states of the trellis.

The distortion relative to the watermark embedding depends on the previous state of the trellis and the input symbol:

$$\begin{aligned} E \times \{0,1\} &\rightarrow \left[-\frac{\Delta}{2}, \frac{\Delta}{2}\right] \\ o : (e_i, m[i]) &\rightarrow d[i] \end{aligned}$$

Then, the sub-codebook can be written with the following equation:

$$U_m[i] = \{k\Delta + o(s_i, m[i]), k \in Z\}$$

The auxiliary variable $u^* \in U_m$ which is closest to the signal sample s is computed with the Viterbi Algorithm (Viterbi, 1967; Forney, 1973):

$$u^* = \arg \min_{u \in U_m} \sum_{i=1}^N (s[i] - u[i])^2$$

During the decoding step, the received signal is quantized again and Viterbi algorithm is used to find the best paths and transitions for which we are able to extract the embedded message.

Another approach for using TCQ in watermarking is noted as TCQ initial state (TCQ-IS). In this approach, the message is embedded in the initial state of the trellis' path instead of the transitions. In this case, the message length is dependant of the number of states of the trellis. So, if the length of the message is high, the trellis will have a large number of states; the complexity of the watermarking scheme will then increase. With TCQ-IS, the robustness will be better than for TCQ-PS, but highly depends on the communication channel. These last elements concerning this approach explain why TCQ-IS is less used than TCQ-PS.

In fact Trellis codes was first introduced in watermarking schemes as an alternative to lattice

codes (Miller, 2002; Miller, 2004) to address the issue of volumetric scaling, e.g. changes in image brightness. The codes of a trellis lie on the surface of a high dimensional sphere. For a given message, the trellis structure permits an efficient identification of the most appropriate code to embed in a given cover work. As a quantization method for quantized based watermarking schemes, TCQ was introduced by Esen (Esen, 2003; Esen, 2004). With TCQ-PS proposed approach, several investigations were done for video or image watermarking applications. The main results were given by the works of G. Leguelvouit (Leguelvouit, 2005) and S. Braci et al (Braci, 2008a; Braci, 2008b) and also (Braci, 2009b) recently published.

In (Leguelvouit, 2005), the author has highlighted the robustness of the scheme. He experimentally shown that the steganographic performance of the scheme is better than the reference scalar Costa scheme (SCS) or optimized QIM: the statistical undetectability is better due to the low embedding distortions. He has also shown that the robustness with TCQ is better when the watermark to noise ratio (WNR) is high.

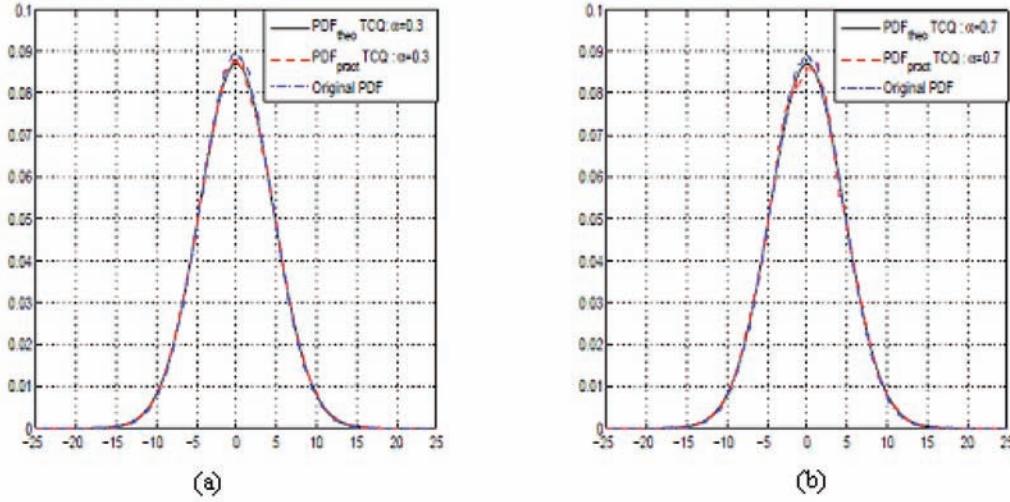
$$WNR_{dB} = 10 \log_{10} \left(\frac{\sigma_w^2}{\sigma_v^2} \right)$$

where the σ_w^2 is the watermark variance and σ_v^2 is the noise power. Nevertheless, if the watermark variance increases, the watermark transparency will be lowered.

Thus to obtain high WNR values with the TCQ and then an improved robustness when the watermark power is increased, the system transparency is reduced.

S. Braci et al in (Braci, 2008a) have widely studied the trade-off performances of this scheme TCQ. The authors present the limits in term of capacity, robustness and undetectability for using such a scheme in an active warden steganographic context. They also propose to combine the TCQ

Figure 3. Probability density functions of the cover and watermarked signal for two different values of the Costa's robustness optimization parameter (a: $\alpha = 0, 3$; b: $\alpha = 0, 7$)



approach with spread transform watermarking and show its efficiency. It is well known that the spread transform (ST) scheme allows increasing the WNR, leading to the increase in robustness against AWGN attack. On the other hand, the TCQ scheme has a good robustness for high WNRs and better security compared to SCS. Thus combination of ST and TCQ (called STTCQ) has shown the best robustness-security trade-off compared to (Guillon, 2002) and SCS (Eggers, 2003), and this trade-off is better for large spreading factor but limited by the constraint of payload.

In (Braci, 2008b), the authors have theoretically confirmed the good steganographic performances with TCQ: the Kullback-Liebler distance between the host signal probability density function and the watermarked signal probability function is low (see Figure 3). They also show that compared to other performed systems that TCQ offer a great security level than spread transform based schemes. They have modeled the activities of active warden by an AWGN and hence, capacity analysis is done according to Shannon definition (Shannon, 1948). Through mathematical analysis as well as experiment results, it is shown that for

strength warden attack (low WNR), the capacity of ST-SCS is better than the one of TCQ. On the contrary, for high WNR values, the capacity of the TCQ is better, thus leads to difficulty to have a system which permits a good invisibility and at the same time a good capacity; a compromise between these characteristics becomes important. The authors have shown through simulation results the compromise of ST-SCS in the active warden context. Finally, the authors have suggested that in the case of public key steganography, TCQ stego-system may be used in the initialization phase to transmit the secret key, and the ST-SCS in the permanent phase, which allows to the best compromise between statistical un-detectability and capacity.

In (Braci, 2009b), the authors try to evaluate which amount of information an attacker will need to evaluate the watermarking embedded information. In fact, they use theoretical developments and practical simulations to measure the contribution of each observation available to an attacker on the total gathered information about the watermarking secrecy. The confirm again the good and secure

behaviour of TCQ based schemes especially when they are combined with spread spectrum.

SOFT COMPUTING BASED OPTIMIZED WATERMARKING

Soft-computing, a sub-branch of computer science, is rich with many optimization tools such as fuzzy logic (FL), rough Sets (RS), artificial neural networks(ANN),geneticalgorithms(GAs), support vector machine (SVM), chaos theory etc. (Bezdek, 1992; Pal, 1996; Pal, 1999). In the following sub-sections, we discuss the usages of various soft-computing tools in the context of design of optimized watermarking intended for various applications.

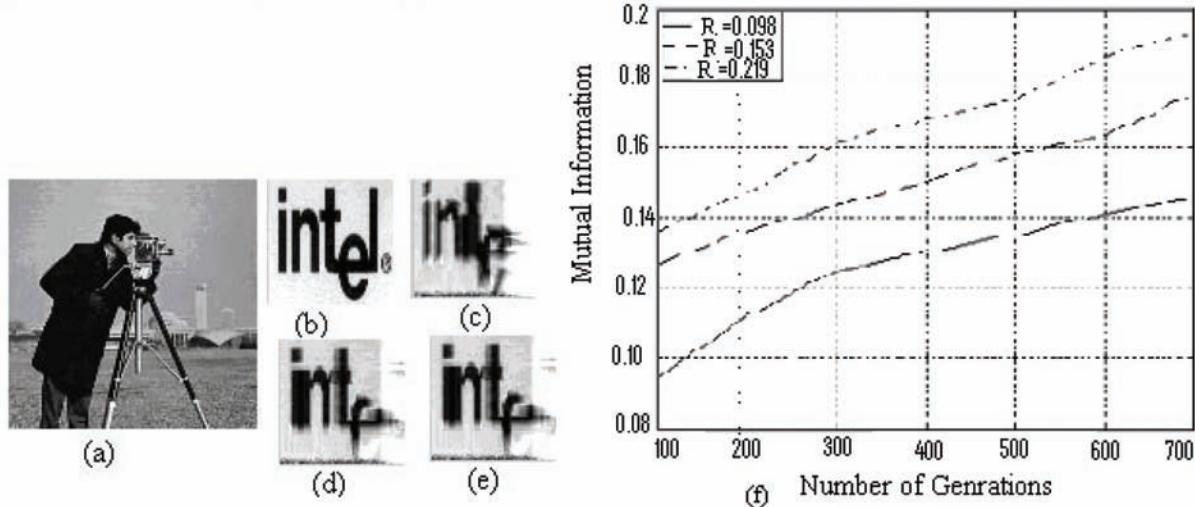
Soft Computing Based Spatial/Original Domain Optimized Watermarking

Early optimization in digital image watermarking was developed mostly in spatial domain and focus was primarily put to imperceptibility aspect. Wang et al. (Wang, 2000) proposed an algorithm to embed secret messages in the moderately significant bit of the cover images. A genetic algorithm is developed to find an optimal substitution matrix for the embedding of the secret messages. A local pixel adjustment process (LPAP) is used to improve the image quality of the stego-image. The weakness of the local pixel adjustment process is pointed out in (Chan, 2001). Wang et al. (Wang, 2001) also proposed a data hiding scheme by optimal LSB substitution and genetic algorithm. Using the proposed algorithm, the worst mean-square-error (WMSE) between the cover image and the stego image is shown to be 1/2 of that obtained by the simple LSB substitution. These LSB based data hiding methods mostly satisfy imperceptibility requirement but their robustness performance against non-malicious signal processing operations are not satisfactory.

Maity et al (Maity, 2009) propose two additive data hiding methods in digital images intended for optimal detection and optimality in imperceptibility and robustness. In the first data hiding method, GA is used to achieve a set of parameter values (used as Key) to represent optimally the difference signal (D). The difference signal is obtained by subtracting the pixel values of the auxiliary images (messages) from that of the pixel values of the cover image. The approximate difference signal with its proper embedding strength is added to the respective cover data. The above problem can be stated mathematically as follows: Given an M -point difference signal (D), how an approximate signal (D') be generated using N - signal points where $N \gg M$ and (D') is close resemblance of (D). One way to regenerate better approximation signal using higher order interpolation. But in that case, the computation cost increases exponentially with order of interpolation. Linear interpolation is a good compromise between the computation cost and better approximation for the regenerated signal. In such case, it is the important point to find which N -points would generate better approximation and how N -values affect this approximation function. This is an optimization problem and GA finds application to yield optimal solutions. We define a parameter called *payload efficiency* (R) which is the ratio of N and M (N/M). The low value of R indicates better data imperceptibility as a given payload is met by embedding less number of signal points. The embedding strategy ensures visual and statistical invisibility of the hidden data. The usage of GA, with the increase of iterations, improves detection of the hidden data and the facts are depicted in Figure 4.

In the second data hiding method, Maity et al (Maity, 2009) use GA to find two parameter values, namely reference amplitude (A) and modulation index (μ). The parameters represent linear and non linear transformation functions that are used to optimally modulate the auxiliary message. The power-law function $x' = A(x + \varepsilon)^\mu$ which is widely used for image enhancement

Figure 4. (a) Watermarked image; (b) watermark image; (c)-(e) retrieved messages after 100, 200 and 400 iterations, respectively; (f) Detection improvement with the number of iterations/generations for different payload efficiency 'R'



operation is considered as modulation function. Here X denotes the pixel value in auxiliary message. Transformation function modulates x to x' , the pixel value of the cover image selected for embedding. Two other transformation functions, one is linear transformation function of the form $x' = A(1 + \mu x)$ and other one is parabolic function of the form $x' = A(1 + \mu\sqrt{x})$, are also used. The functions are studied for their suitability on imperceptibility, security and robustness issues of data embedding. The proposed GA based data hiding methods can be used for secured data transmission. GA is used here to achieve optimal imperceptibility of the hidden data.

Calculation of A

Differentiating x' in power law function with respect to x , we get $dx'/dx = A\mu(x+\varepsilon)^{\mu-1}$. Here, dx'/dx is positive provided $A > 0$, $\mu > 0$ and $(x + \varepsilon) > 0$. This implies that x' increases monotonically with x . The upper (U) and the lower (L) bound of the modulated pixel values are $U=x'_{max}=A(x_{max}+\varepsilon)^\mu$ and $L=x'_{min}=A(x_{min}+\varepsilon)^\mu$, respectively. The range (Ψ) of the modulated pixel values is given

as $\Psi=U-L=A[(x_{max}+\varepsilon)^\mu-(x_{min}+\varepsilon)^\mu]$. The relation shows that for large 'A' value, the span of the modulated pixel values (Ψ) will be large. This leads to smaller probability of matching between the modulated message and the embedding regions. This in turn suggests to select lower value of 'A' for better imperceptibility. The small span (Ψ) is also possible for large 'A' value provided very small value is selected for μ . But it is shown in the detection process that small value of μ will make the auxiliary message vulnerable to elimination in noisy transmission media. Similar argument also holds good for the value of 'A'. The value of 'A' depends on the selection of the auxiliary message as well as regions selected for embedding. As rule of thumb 'A' is selected as $A=x'_{mode}/(x_{mode}+\varepsilon)^\mu$. The symbols x'_{mode} and x_{mode} denote the mode of the gray values for the embedding regions and the auxiliary messages, respectively.

Calculation of μ

Power-law transformation suggests that if ' μ ' value is taken small ($\mu < 1.0$) keeping 'A' constant, auxiliary message is mapped into a narrow

range of gray values. Confinement of gray values inside a narrow range increases the probability of matching between the modulated message and the data embedding region. But very small value of μ degrades the quality of the detected message to a non-recognizable form even after a very small image distortion. The upper and the lower value of μ are calculated as follows: It is found that x' is a monotonically increasing function of x . The value of ε , acts as offset value in image display, is set to (~0.01). We write $x'_{max} = A(255 + 0.01)^{\mu} = A(255.01)^{\mu}$. The maximum x' value is taken 255 for monochrome gray level image. The corresponding μ value is designated as μ_{max} and is related with x'_{max} and A as follows:

$$\mu_{max} \approx \frac{\log X'_{max} - \log A}{\log 255}$$

Similarly, μ_{min} value can be written as follows: The value of μ will be positive if A lies between x'_{max} and x'_{min} . The latter two values represent the maximum and the minimum gray values of the embedding regions, respectively.

$$\mu_{min} \approx \frac{\log X'_{min}}{\log 0.01} = \frac{\log A - \log X'_{min}}{\log 2.0}$$

The value of μ will be positive if A lies between x'_{max} and x'_{min} . The later values represent the maximum and the minimum gray values of the embedding regions, respectively. Data recovery process uses inverse transformation function that maps x' into x and thus message is recovered. If power-law, linear and parabolic functions are used for message modulation, the extracted message can be represented respectively as follows:

$$x = (x'/A)^{1/\mu} - \varepsilon \quad (42)$$

$$x = (1/\mu A)(x' - A) \quad (43)$$

$$x = 1/(\mu A)^2 (x' - A)^2 \quad (44)$$

Differentiating equations (42), (43) and (44) with respect to x' , the following equations are obtained respectively,

$$dx/dx' = (1/\mu)(1/A)^{1/\mu} (x')^{1/\mu} \quad (45)$$

$$dx/dx' = 1/\mu A \quad (46)$$

$$dx/dx' = 2(x' - A)/(\mu A)^2 \quad (47)$$

The parameter dx/dx' denotes the change of x with respect to the change of x' i.e. a measure of noise immunity in the decoding process. The large values of A and μ are preferable for reliable decoding whereas small values of the same are desirable for better imperceptibility. Lower value of dx/dx' indicates better reliability in decoding process. Experiment results strongly conform mathematical analysis for selection of proper modulation function. This simultaneously better visual and statistical invisibility of the hidden data as well as robustness against common signal processing operations are achieved.

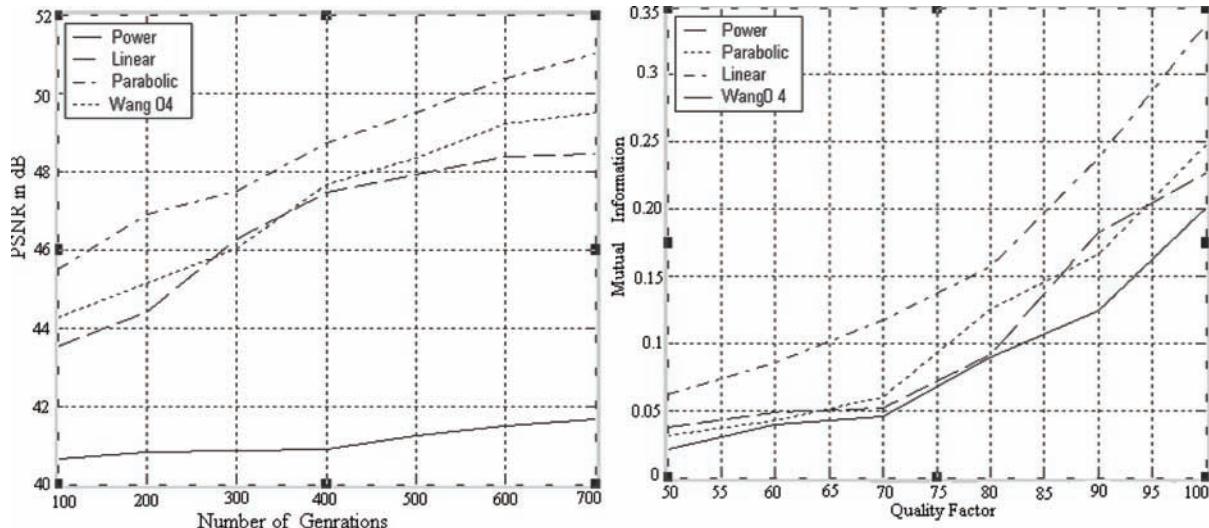
Table 1 shows numerical values of different properties using different modulation functions with the effect of number of generations. Figure 5(a) shows graphically visual quality measures (imperceptibility) in peak-signal-to-noise ratio (PSNR) as an effect of number of generations for the watermarked images with different modulation functions. The method of Wang et al. (Pan, 2004) is also compared with the proposed one. Figure 5(b) shows robustness performance against JPEG at different quality factors of compression. Figure 6(a)-(p) show watermarked images and the extracted messages after various image processing operations.

Yu et al (Yu, 2001) embed a binary watermark in the spatial domain of color image. The image owner collects a set of training patterns to train a neural network. The authors have argued that due to the learning and adaptive capabilities, the trained neural networks recover the watermarks with good fidelity from the various noisy/attacked versions

Table 1. Performance results of different modulation functions

Gener- ation no	PSNR (dB)1	ε value (1)	$I(x; y)$ value(1)	PSNR (dB)2	ε value (2)	$I(x; y)$ value(2)	PSNR (dB)3	ε value (3)	$I(x; y)$ value(3)
50	40.56	0.046	0.15	43.49	0.030	0.39	45.42	0.037	0.32
150	40.79	0.045	0.19	44.36	0.034	0.40	46.74	0.037	0.34
400	40.90	0.041	0.20	47.90	0.036	0.42	48.73	0.036	0.35
600	41.50	0.039	0.21	48.36	0.037	0.44	50.37	0.025	0.38
800	41.77	0.038	0.28	47.45	0.040	0.48	51.53	0.023	0.39

Figure 5. (a) Imperceptibility for different modulation functions with the number of iteration; (b) Robustness against lossy JPEG compression operation

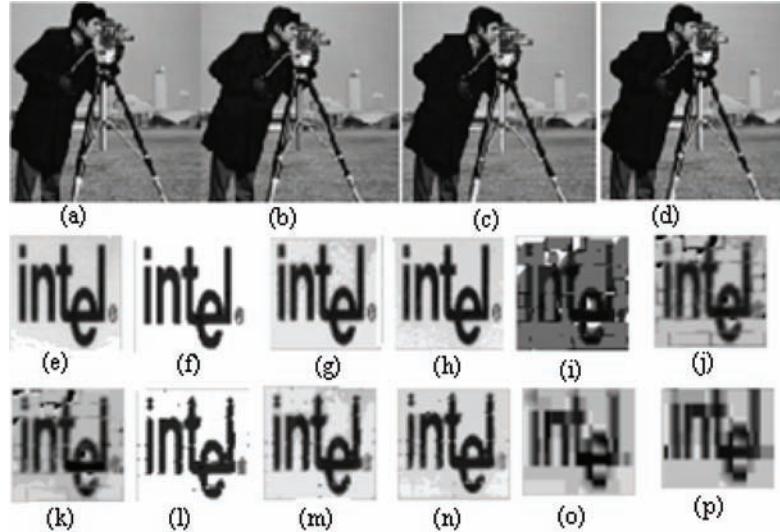


of the watermarked image. Their work was based on the algorithm proposed by Kutter et al (Kutter, 1998); watermark sequence w is formed from the concatenation operation of H and L ; $H = h_0 \ h_1$, and $L = l_0 \ l_1 \ l_2 \dots \ l_{m-1}$ are a 2-bit and an m -bit binary sequences, respectively. Watermark embedding is done by pseudo randomly selecting the pixels and by modifying the blue component B_{pt} . The symbol p_t corresponds to a random position with ' t ' is the length of watermark sequence l .

The extraction of watermark algorithm selects the embedded pixels using the same secret key. It generate the blue component B_{pt}' of the respective chosen pixel using as the centre of a sliding window with symmetric cross-shape. A param-

eter β_t is computed as $\beta_t = B_{pt} - B_{pt}'$ and adaptive threshold is determined by $\theta = \frac{1}{2}(\delta_0 + \delta_1)$. The subscripts 0 and 1 correspond to 0 and 1 of h_0 and h_1 , respectively. Each watermark bit w_t , $t=2, \dots, m+1$, is determined by $w_t = 1$, if $\beta_t > \theta$, else $w_t = 0$. The watermark recovery process requires the knowledge of $w_0 = 0$ and $w_1 = 1$ to be known. This determines an adaptive threshold so that threshold (constant of decision function) can be defined to extract the watermark bits. However, it has been demonstrated through the experimental results that the constant decision function does not accurately extract watermark when the watermarked image

Figure 6. (a) Cover image; (b), (c), (d) watermarked images using power-law ($PSNR=41.77\text{ dB}$), parabolic function ($PSNR=51.58\text{ dB}$), linear function ($PSNR=47.45\text{ dB}$) respectively; (e) Auxiliary message; (f), (g), (h) Extracted messages from (b), (c), (d) respectively; (i), (j), (k) Extracted messages from mean filtered watermarked images when power law, parabolic, linear functions are used respectively after 200 generations; (l), (m), (n) Extracted messages from median filtered watermarked images when power law, parabolic, linear functions are used respectively after 200 iterations; (o), (p) Extracted messages from compressed (JPEG) watermarked images ($PSNR=31.06\text{ dB}$) and ($PSNR=31.88\text{ dB}$) at quality factor 70 using linear and parabolic function respectively after 400 iterations.



undergoes geometrical transformation or image processing operations.

Yu et al use (Yu, 2001) neural network to determine more adaptive threshold so that the false recovery can be reduced greatly. The watermark used is denoted as $w = H_{p,q} + L = \alpha_{11} \alpha_{12} \dots \alpha_{1q} \alpha_{21} \dots \alpha_{2q} \dots \alpha_{p1} \dots \alpha_{pq} \dots l_0 \dots l_{m-1} = W_0 w_1 \dots w_{pq+m-1}$, where $H_{p,q} = \alpha_{11} \alpha_{12} \dots \alpha_{1q} \alpha_{21} \dots \alpha_{2q} \dots \alpha_{p1} \dots \alpha_{pq}$ is a $(p \times q)$ -bit binary sequence, and $\alpha_{ij} \in \{0,1\}$, $1 \leq i \leq p$, $1 \leq j \leq q$. Here, $H_{p,q}$ can be made of arbitrary length for obtaining a more accurate signature in contrast to preceding H (2 bit length sequence). The main purpose of creating $H_{p,q}$ is to construct the training patterns for a neural network. The pattern memorizes effectively the characteristics of the relation between watermark and the watermarked image. The intention is to emphasize the adaptive capability of the neural network for the extraction of the digital signatures that can never be trained in

advance. They have performed simulations using 9-5-1 multilayer perceptron (MLP) including an input layer with 9 nodes, a hidden layer with 5 hidden nodes, and an output layer with a signal node. Multiple embedding strategies i.e. each watermark bit is embedded in several different positions. This exploits the ability of the neural to generate further improvement in θ by increasing the number of the size of extra information i.e. increasing the number of training patterns. They have shown through large number of experiment results that their method shows much improved detection performance against varieties of attacks like blurring, median filtering, sharpening, JPEG compression, scaling and rotation operation compared to that of Kutter's method.

Neural network theories of attractors and attraction bins are used for information hiding capacity bound analysis (Zhang, 2008). With

this method, the processes for determining upper and lower limits of information hiding are unified within single theoretical framework. In digital watermarking, the embedded data distorts the host data. The modification for amplitude of some pixels will appear as change in the image. The more watermark information is hidden, the larger the Hamming distance between the stego-image and the original image. When the Hamming distance is out of the bounds of the attraction basin, the neural network cannot retrieve the more number of points that can be modified in an image. Therefore, the modification restricts its information hiding capacity.

Pan et al. (Pan, 2001) propose spatial domain image watermarking scheme combined with genetic algorithm (GA). The objective function for training of GA is developed from the combined contribution of imperceptibility and robustness measure. The binary watermark is embedded by pixel value difference of mean gray values of a neighborhood. The GA trained result is seen as a secret key and is used in the embedding and extraction process of watermark information. Chang and Lin in (Pan, 2004) discuss the feasibility of support vector machine to carefully select intensities according to the characteristics of the blocks so that the marked image is visually indistinguishable from the original. They set up an empirical model by training an SVM to classify blocks of pixels from an image. Then they determine the ranks of the blocks in accordance with the perceptual significance blocks. The training set, $\{d_i, p_i\}$, contains m data points. The symbol d_i indicates i-th input pattern which is the 4 leftmost significant bits (MSB) for each pixel in a texture block. The input pattern d_i is a 9-dimensional data as the block size is 3×3 . The output value p_i has to be selected carefully by means of the human visual system (HVS) and decides the range of each pixel in the block to be modified. Linear SVM or non-linear SVM for multiclass data can be used for training of SVM. After training, a SVM is constructed to extract

the feature of the test block. The SVM and classification regulations must be kept secret by the image owner. For experimentation, they prepare 50 patterns in the training set, where each pattern contains 9 input values and 1 target value. Finally, they have shown the robustness performance against blurring, sharpening, JPEG compression and image rescaling operations.

SOFT COMPUTING BASED ADVANCED SPATIAL/ ORIGINAL DOMAIN OPTIMIZED WATERMARKING

Several advanced spatial domain optimized watermarking techniques are developed recently based on mathematical modeling. Maity et al (Maity, 2009a) recently propose an optimized SS watermark detection using fuzzy logic through the cancellation of multiple bit interference effect. A new model of SS watermarking is proposed. Each watermark bit is spread over N-mutually orthogonal signal points using a distinct code pattern. The watermarked image s for embedding the k-th watermark bit s_k is considered as a N-dimensional vector $\{s_{1k}, s_{2k}, \dots, s_{Nk}\}$. This is

written as $s_{nk} = \sum_{n=1}^N x_n + \gamma P_{nk}$, where $n, k \in \mathbb{Z}$

and γ is the embedding strength. The symbol p_{nk} corresponds to the n-th binary element of k-th code pattern. The authors assume that an attacker modifies the n-th watermarked signal point by an amount which takes values randomly from Rayleigh distribution. Furthermore, it is assumed that the watermarked signal is also corrupted by additive white Gaussian noise (AWGN) when transmitted through the communication channel. The distorted and the noise corrupted watermarked signal at the input of the watermark decoder can be written as

$$s_n'' = \sum_{k=1}^K \sum_{n=1}^N \alpha_n (x_n + \gamma p_{nk}) + \eta_n \quad (48)$$

where α_n is the modification at n -th signal point due to Rayleigh attack model and η_n is the contribution in the same signal point due to AWGN. The decision variable for each watermark bit decoding is obtained from the weighted average of N -decision statistics. This leads to better stability against attack distortions. The received watermarked signal is first projected onto N -orthogonal signal points. The decomposed signal is then correlated using j -th spreading code that results to $r^j = (r_1^j, r_2^j, \dots, r_N^j)$. The decision variable for the j -th bit at n -th signal point is denoted by r_n^j and can be written as follows:

$$r_n^j = \langle s_n'', p_{nj} \rangle = \alpha_n \gamma + \sum_{k=1, k \neq j}^K \alpha_n \gamma \rho_{kj} + \eta_j \quad (49)$$

The decision variable D^j for the j -th bit is obtained by the minimum mean square error combining (MM-SEC) strategy. The expression is $D^j = \sum_{n=1}^N r_n^j w_{nj}$ where, $w_{nj} = \alpha_n / (\text{var}(b_k) A_{nj} + N_0 / 2)$, $A_{nj} = \sum_{k=1, k \neq j}^K \alpha_n (\rho_{kj})_n$ and $\text{var}(b_k) = 1$. The decision variable D^j is fed to the decision device, the output of which determines the binary bit pattern. Thus the correlator's outputs generate a decision vector $D = [D^1, D^2, \dots, D^K]$ which is used to obtain initial estimates of the embedded bits. These initial estimates are then used to evaluate the multiple bit interference experienced by individual bit during interference cancelation.

The authors use fuzzy membership function to map each decision magnitude D^j for j -th embedded watermark bit to the interval $[0, 1]$ using the function $f_j = 1/(1+|D^j|)$. The range of membership values and their corresponding embedded bits are classified into different groups. Multiple group

combined interference cancelation (MGCIC) is used to perform interference cancelation.

1. The greater the magnitude of decision variable $|D^j|$, the stronger the interference effect of the respective embedded bit. Thus, the bits for which the membership values f_j corresponding to the magnitude of decision variables satisfy the condition $0 \leq f_j < 0.25$ are classified as very strong groups. The bits for which the membership value f_j satisfy the conditions $0.25 \leq f_j < 0.5$, $0.5 \leq f_j < 0.75$ and $0.75 \leq f_j < 1.0$ are classified as strong, weak, and very weak groups, respectively.
2. GCIC is performed within the group of very strong bits. This is done by simultaneously canceling the interference of all other bits except the desired one. The very strong data bits are thus estimated.
3. Using the updated data of very strong bits, the interferences due to these bits are removed. GCIC is employed within the block of strong bits. The strong data bits are estimated.
4. Using the updated data of strong bits and very strong bits, the interferences due to these bits are removed. Then GCIC is employed within the group of weak bits. The same processes are continued for all other remaining groups. The updated decision statistics of all the bits are used to compute the membership values. The MGCIC process, i.e. steps 1, 2, 3, 4 are repeated iteratively. This is done until a desired probability of error is achieved or preset number of iterations is complete.

The authors also develop (Maity, 2009a) fuzzy logic based weighted combined interference cancelation (CIC) within the strong and the weak groups. This is done to make a trade-off between performance improvement and computation cost. Weights are determined for interference cancellation using the fuzzy membership function $f_j = 1 - e^{-(a|D^j| + b)}$, where f_j is the decision variable of j -th bit. It has been observed through simulation

results that the performance of four, three and two GCIC detection based on fuzzy logic is better than that of the conventional interference cancellation (IC). In conventional IC, during decoding of a particular bit, estimated interference due to all other remaining bits for the previous stage are canceled simultaneously. Thus fuzzy logic becomes potential to beat uncertainties associated with multiple bit interference effect.

Further improvement in detection performance is done through optimal partitioning of groups in diversity assisted system (Maity,2009b). Diversity in watermarking implies formation of the resultant watermarked image from the weighted average of multiple copies. Weights may be determined based on the visual quality of the individual watermarked images. Since it is a multiple bit watermark detection system, the authors use watermark signal-to-interference ratio (WSIR) as weight factor to achieve low BER rather than watermark signal-to-noise ratio (WSNR) based approaches of conventional watermarking methods. WSNR is the ratio of watermark signal amplitude square (Power) to the noise power offered by the attack channel. The noise power is calculated from the noise variance. Higher weight factor is assigned for the copy of the watermarked signal which offers higher value of WSIR. Genetic algorithm is used here to find out the optimum boundaries to partition different embedded bits into different groups. The goal of this optimal partitioning is to club the bits with similar decision magnitudes in a particular group. At the same time, the bits with different magnitudes are considered into different groups. Each partition point is denoted here as a parameter. Thus the fitness value for each block is obtained for such partitioning from the decision magnitude of individual block divided by the total decision magnitudes. The objective function is developed from the weighted average of bit error rate (BER) for the individual block containing the particular bits belonging to that group. Simulation results show that GCIC technique using GA provides significant detection improvement over

conventional interference cancelation at the cost of slight increase in computation complexity. Diversity assisted detection system based on WSIR improves this BER performance almost two times.

Maity et al (Maity 2009c) further extend this SS watermarking for variable embedding rate so that each signal point allows different payload under fading attack. Fading attack can be estimated using GA and similar detection improvement can be achieved without/with interference cancellation at single stage. The objective function for GA based attack estimation is formed from the weighted average of data hiding capacity and detection performance on individual host component. Data hiding capacity at each host signal point is determined by SIR (signal-to-interference) corresponding to each watermark bit. The SIR is formed from the ratio of the sum of signal term and estimated error in signal term to that of sum of interference power, estimation error in interference power and noise power. Simulation results show that gap in BER performance with the actual value of fading attacks and for its estimated value are very small. Performance improvement is achieved with much lower computation cost.

Maity et al (Maity, 2009d) also use genetic algorithm for optimization of watermark embedder. The objective is to meet an acceptable BER (bit error rate) and peak-to-average distortion (PAD) on a single point of the cover signal under the constraint of a given embedding distortion and cover size. The authors want to show that optimizing the number of cover signal points (N), payload capacity (K) and watermark signal-to-interference ratio (WSIR). It is possible to achieve better acceptable values of both BER and PAD simultaneously. Diversity scheme is employed and WSIR is used as weight factor to generate resultant watermarked image from the multiple copies. The authors define PAD (in dB) as $PAD_{dB} = 10 \log (P_d / P_{avg})$ where P_d is the total embedding distortion on a signal point and P_{avg} is the average embedding distortion for the watermarked signal. The WSIR

for the k-th bit in the first modified watermarked image can be written as

$$WSIR_{k1} = \sum_{n=1}^N (\alpha_n \gamma \rho_{kj})^2 / \sigma_{MBI}^2 + \sigma_N^2 \quad (50)$$

So the total WSIR for the first watermarked image can be written as $WSIR_1 = \sum_{k=1}^K WSIR_{k1}$. Similarly, the total WSIR for the second watermarked image can also be calculated accordingly. Total weighted WSIR for the two watermarked image signals is calculated using the following equation.

$$WSIR_{Th} = 10 \frac{(WSIR_1)^2 + (WSIR_2)^2}{WSIR_1 + WSIR_2} \quad (51)$$

They have performed the experiment over large number of images and a scaling factor of 10 has been included to enhance the optimization performance (based on simulation result). The objective function is defined as follows:

$Nmax$: maximum number of cover signal points
(N)

$Nmin$: minimum number of cover signal points
(N)

$Kmax$: maximum number of watermark bits (K)

$Kmin$: minimum number of watermark bits (K)

$PADmin$: minimum value of PAD (in dB)

$WSIRmax$: maximum value of $WSIR_{TW}$

The function ' F ' is calculated in two steps as follows:

- First, minimum PAD is calculated corresponding to maximum K and minimum N value within the permissible range. Note that PAD on a watermarked signal point depends on the number of bits embedded as well as average distortion. It is not related to WSNR

value on a cover signal point. This is why WSNR is not considered during calculation of minimum PAD. Similarly, maximum value of $WSIR$ is calculated corresponding to minimum K, maximum N, and the maximum WSNR i.e., $(WSNR)_{max}$ values within the permissible range.

- For each individual set of {N,K,WSNR}, PAD, and $WSIR_{Th}$ values, calculate P_{diff} and SIR_{diff} as follows.
 - $P_{diff} = PAD - PAD_{min}$
 - $SIR_{diff} = WSIR_{max} - WSIR_{Th}$

The fitness function F essentially contains difference in PAD and $WSIR_{Th}$.

$$F = 20 \frac{P_{diff} SIR_{diff}}{P_{diff} + SIR_{diff}} \quad (52)$$

Thus minimization of ' F ' will keep PAD to a low value in order to avoid large signal distortion on a single cover point. It will also keep $WSIR_{Th}$ value to low value in order to reduce the MBI effect. Therefore, the value of ' F ' indicates how good (or bad) a particular set of {N,K,WSNR}. The set will be used in each stage of iteration of GA in order to achieve optimal values of {N,K,WSNR}. Table 2 shows performance results as an effect of number of generations.

Genetic algorithms are also used to give an intelligent shaping of a digital watermark based on an anticipated attack (Khan, 2007). This will help to achieve a superior trade-off between the watermark robustness and imperceptibility. Robustness versus imperceptibility trade-off and increase in bit correct ratio after attack has been employed as the optimization criterion in genetic algorithm approach.

SVM based watermarking is also explored for the authentication of color image (Tsai, 2007). The method constructs a set of training patterns with the use of binary labels by employing three image features. The features are the difference

Table 2. Performance results of GA based watermark embedder optimization

Generation number	K	N	WSNR in dB	PAD in dB	WSIR In dB	BER
50	52	400	28.68	3.234	1.7922	0.017
150	60	289	33.48	4.685	1.9441	0.015
400	48	269	28.21	3.156	2.0429	0.014
600	62	324	29.63	4.432	2.1274	0.011
800	55	289	28.50	3.546	1.7655	0.009

between a local image statistic and the luminance value of the centre pixel in a sliding window with three distinct shapes. This set of training patterns is gathered from a pair of images, an original image and its corresponding watermarked image in the spatial domain. The set of training pattern is used to train the SVM. Trained SVM is applied to classify a set of testing patterns. A quasi-optimal hyperplane (a binary classifier) is realized and hidden signature is retrieved without the use of original image.

SOFT COMPUTING BASED OPTIMIZED WATERMARKING USING UNITRARY TRANSFORM

Soft-computing tools are also being used extensively to design transform domain optimized watermarking techniques for image and video signals. Shih et al. (Shih, 2004) propose progressive watermarking where GA is used to find the optimal frequency bands for watermark embedding into DCT based watermarking system. This can simultaneously improve security, robustness and visual quality of the watermarked image. GA is used to choose the DCT coefficients under certain attacks in every iteration. Cost function is developed from the combined contribution of imperceptibility and robustness measure. The authors have shown through simulation results with different watermark embedding strength. Both imperceptibility and robustness are increased simultaneously with

the increase of number of iterations. They have also extend their transform–domain genetic based watermarking scheme with some modifications for the progressive transmission scheme in JPEG (Shih, 2009). They apply spectral selection mode in JPEG like DC coefficient of every block, first AC coefficients, second AC coefficients, until stage 63 for every 8x8 block. This way transmits the watermarked image progressively.

Hwang et al. (Hwang, 2000) propose optimized copyright protection system by modifying the discrete cosine transform (DCT). This focuses on finding the optimized correlation among the watermarking requirements, including watermarked image quality, the capability for resisting attacks, and the number of bits embedded. Back propagation neural network (BPN) model is used where the first nine AC DCT coefficients are the input vectors and the twelfth AC coefficient is the output vector. The weight values can be modified by the training set according to approximate errors. Binary watermark is embedded by exploiting pixel value difference to yield optimum imperceptibility.

Shih et al (Shih, 2009) make use of differential evaluation (DE) technique for breaking the visual steganalytic system. The authors argued that DE is a simple and efficient adaptive scheme. This can find the global optimum of a multidimensional, multimodal function with good probability unlike the drawback of GA which converges slowly to the optimal solution. Thus evolutionary strategy (ES) gets stuck on a local optimum. The stego-image generation depends on two criteria, namely (i) the

extracted message is obtained from the specific coefficients of a stego-image. This ensures closeness of the extracted message to the embedded messages, (ii) the statistical features of the stego-image is compared with that of the cover image such that the differences should be as small as possible. The method of DE mainly consists of four steps: initialization, mutation, recombination, and selection. The algorithm developed by Shih et al is briefly described here.

Step 1: Random initialization of the parent population, each with element of NP vectors in 'n' dimension, is done.

$$y_i^m = y_{\min}^m + r \text{ and } (0,1)x(y_{\max}^m - y_{\min}^m) \quad (53)$$

where $i=1, 2, \dots, NP$ and $m=1, 2, \dots, n$.

Step 2: To start with the object function $f(y)$, where $y=(y^1, y^2, \dots, y^n)$ is a vector of n decision variables, is defined and need to be optimized.

Step 3: Three random numbers (a , b , and c) is selected within the range from 1 to NP . A noisy vector n_i is generated through the perturbation of y_c by the weighted difference ($y_a - y_b$) as follows:

$$n_i = y + F(y_a - y_b) \quad (54)$$

where $i=1, 2, \dots, NP$.

Step 4: A trial vector t_i is generated through the recombination of target vector y_i with the noisy random vector n_i as follows:

$$t_i^m = n_i^m \text{ if } r \text{ and } (0,1) < CR \text{ or } m=r \text{ and } (1,n) \quad (55a)$$

$$t_i^m = y_i^m \text{ otherwise,} \quad (55b)$$

where $i=1, 2, \dots, NP$ and $m=1, 2, \dots, n$.

Step 5: The decision variable of the trial vector is checked whether to lie within the bounds. If it lies outside, the following operation is made to keep it within the bound,

$$t_i^m = y_{\min}^m + 2(p/q)(y_{\max}^m - y_{\min}^m) \quad (56)$$

$$\text{where } p=t_i^m - y_{\max}^m \text{ and } q=t_i^m - y_{\min}^m \text{ if } t_i^m > y_{\max}^m \quad (57)$$

$$\text{otherwise, } p=y_{\min}^m - t_i^m \text{ and } q=y_{\max}^m - t_i^m \quad (58)$$

Step 6: The objective functions of the two vectors t_i and y_i are calculated. The parameter with low value survives and proceeds to the next generation.

Steps are repeated until the convergence criterion meets or preset number of iterations is complete.

Experimental results demonstrate that the DE based steganography is superior to the genetic algorithm based steganography. Both the imperceptibility and robustness can be enhanced.

An interesting application of the usage of GA in least-significant-bit substitution (LSB) based watermark embedding on DCT coefficients of the image is seen in (Shih, 2008). The motivation of this use is to determine the rules for translating real number into integers. The author has shown through some demonstration that the extracted watermark looks noisy when a rounding operation is usually recommended to convert real numbers into integer numbers. So, an important question arises, is it possible to correct the error by changing the certain pixel values? The answer is yes. But the mapping from spatial to transform and the reverse operation, being many to many, is difficult to control and predict the changes. To solve the rounding error problem using GA, binary strings of 64 (for block of size 8x8) bits length are considered as chromosomes. The binary data in each position converts corresponding real number r , to an integer r_{int} according to the following rule:

If the binary data at a position is 1, $r_{int} = \text{Trunc}(r) + 1$
 (59a)

If the binary data at a position is 0, $r_{int} = \text{Trunc}(r)$
 (59b)

The fitness function of each chromosome is determined by the difference between the embedded and the extracted watermark. It can be mathematically written as

$$F(\beta) = \sum_{\forall i} w(i) - w'(i) \quad (60)$$

where $w(i)$ and $w'(i)$ denote the i -th bit of the embedded and the extracted watermarks, respectively. Then, the normal rule of GA is applied to get the best solution following the procedure of repetitions of GA steps for predefined numbers or until the predefined condition is satisfied.

Particle swarm optimization (PSO) algorithm is also being applied in recent time for data hiding. An optimal substitution matrix for transforming the secret messages is first derived by means of the PSO algorithm. More secret messages are embedded by modifying the standard JPEG quantization table (Wang, 2009). The transformed messages are then hidden in the DC-to-middle frequency components of the quantized DCT coefficients of the cover image. JPEG entropy coding is finally applied to obtain JPEG file with secret messages. PSO is also used to design dual watermarking algorithm for video signal based on the audio video coding standard (AVS). One watermark is embedded in luminance components, whose embedding positions are optimized using PSO technique, resisting common signal processing operations such as median filtering, adding noise, cropping and so on. To combat geometric and reencoding attacks, the other watermark is embedded in chrominance components. This is done by adjusting the energy relationship between c_b and

c_r components based on just noticeable distortion (JND) concept of human visual system (HVS).

WAVELETS AND SOFT COMPUTING TECHNIQUES IN OPTIMIZED WATERMARKING

Wavelets, due to its multiresolution capability, better scale space tiling, better human visual system (HVS) characterization becomes a natural choice from the early part of digital watermarking research. Wavelet analysis when clubbed with various soft computing tools advances significantly optimized digital watermarking research (Maity, 2008). The combination of dual tree wavelet transform and probabilistic neural network is used to select the efficient wavelet coefficients to cast the watermark information (Wen, 2009). The learning and adaptive capabilities of neural networks helps to achieve the trained neural networks that can recover the watermark form the watermarked images. Thus the combination offers better imperceptibility and robustness in watermarking. Chang et al (Pan, 2004) use neural network to select coordinate set from DWT (discrete wavelet transform) decomposition. A training set is constructed to train the network to be used to embed watermark. Biologically inspired spiking neural network (SNN) is successfully integrated with wavelet theory and provides a more effective hybrid approach to resolve security problems (Hassanien, 2009).

Genetic algorithm is also used in the design of optimized digital watermarking by Kumsawat et al (Kumsawat, 2005). GA finds parameters that consist of threshold values and the embedding strength to improve the visual quality of the watermarked images and the robustness of the watermark. GA is used in discrete multiwavelet (DMT) coefficients for zero-rate spread spectrum watermarking. They embed watermark information in all subbands except the approximation subbands (contains the high-energy components and may create visual

degradation) and in the subbands of the finest scale (due to low-energy components and may suffer from robustness problem). All DMT coefficients greater than the embedding threshold T_1 are chosen for watermark embedding according to the rule as $s_i' = x_i + \alpha |x_i| \cdot w_i$, where i runs over the watermark coefficients. The symbols x_i and s_i' denote the coefficients of the original and the watermarked image, respectively. The variable w_i indicates here the watermark signal generated from a Gaussian distribution with zero mean and unit variance and α denotes the embedding strength to make a balance between robustness and visual distortion.

The suspected and the possibly distorted watermarked image is first decomposed into three levels using DMT. They select all the DMT coefficients which are greater than the detection threshold T_2 . The coefficients belong to all subbands except the approximation and the subbands of the finest scale, are chosen for possible detection of watermark. The value of T_2 is slightly greater than T_1 . The reason is that some coefficients, which were originally below T_1 , may be greater than T_1 due to image manipulations. They calculate the correlation ρ between the selected coefficients of the watermarked image s_i' and the original watermark using the following equation $\rho = \frac{1}{M} \sum s_i' w_i$ (61)

where i runs over the wavelet coefficients s_i' , and M is the number of the coefficients s_i' . The authors argue that both s_i' and w_i are independent random variables. So the product $s_i' w_i$ should also be treated as an independent random variable tends towards standard normal distribution. The existence of the embedded watermark is identified by computing correlation z with the threshold T , where

$$T = \frac{\alpha}{2M} \sum_i |s_i'| \quad (62)$$

They apply GA to find optimal set of parameter values, namely embedding strength (α), embedding threshold (T_1), and detection threshold (T_2). The objective function for searching the parameter values is formed from the weighted sum of robustness and invisibility measure. The objective value F is defined as

$F = \beta_1 (1 - UQI) + \beta_2 DIF$, where β_1 and β_2 are weighting factors of universal quality index (UQI) and DIF. DIF indicates difference (DIF) between correlation ρ and the threshold T as a watermark detection index, respectively. The value of each weighting factor indicates the relative importance of individual. If both are equally important should have value 0.5 each, and the relationship $\beta_1 + \beta_2 = 1.0$ must hold.

Similar type of optimized zero-rate SS watermarking system is also developed by Bhattacharya (Bhattacharya, 2009) where GA is used in multi-band wavelet. The authors consider optimization in robustness, imperceptibility (taking into consideration of both global and local distortion), and length of Gaussian watermark. The host image is decomposed into 16 subbands by applying multiband (where $M=4$) wavelet transform (MWT). The parameters T and $\alpha_1, \alpha_2, \alpha_3$ and α_4 are defined from the population. The parameter ‘ T ’ is defined as the lower bound threshold limit of the coefficients selection, while x corresponds to the maximum coefficient value. T lies between ($g\%$ of x) and ($j\%$ of x) and the parameters $\alpha_1, \alpha_2, \alpha_3$ and α_4 are the embedding strengths within a specific limit i.e. 0 to 0.25 to 0.50 to 0.75 to 1. The optimization problem develops fitness function from the weighted average of imperceptibility, robustness and capacity. Since, Gaussian watermark is used for watermarking, the capacity is represented by the length of the Gaussian watermark. Thus, the normalized fitness function F is then defined as:

$$F = \beta_1 \times MSSIM + \beta_2 \times C + \beta_3 \times CC \quad (63)$$

where, $0 < MSSIM, C, CC < 1$, MSSIM is a measure of imperceptibility, CC (cross correlation) is a measure of robustness. The authors apply various attacks like mean filtering, median filtering, JPEG, salt and pepper noise, dynamic range change, histogram equalization on the watermarked image and calculate the CC values for each attack. Then an average CC value is calculated to find the quantitative measure of robustness.

They define normalized capacity C in case of zero-rate embedding using Gaussian watermark as,

$$C = \frac{\text{Capacity at any particular iteration}}{\text{Maximum Capacity}} \quad (64)$$

where the maximum capacity indicates the maximum length of Gaussian watermark. This amount of watermark information may be embedded without much distortion on visual quality of the host signal. Each of the weight factor $\beta_1, \beta_2, \beta_3$ is represented in terms of the other two factors like β_2 by ($MSSIM, CC$), β_3 by ($MSSIM, C$) and β_1 by (C, CC) so that $\beta_1 + \beta_2 + \beta_3 = 1$. Figure 7 shows the block diagram representation of the zero-rate optimized Gaussian SS watermark. Watermark embedding strategy considers both global and local distortion. The authors define local distortion as follows: local distortion = (new value of the coefficients after watermark embedding) - (old value of the coefficients before watermark embedding). Let us consider $T1$ be $x\%$ of the selected coefficients from a band, say, 80% of the total selected coefficients which are involved in watermark embedding. Also let us consider only those combinations of T and α 's so that after watermark embedding modified coefficients that have a difference with the old value greater than a predefined delta value, does not exceed 80% of the total coefficients in the band. If $N2 < T1$, perform inverse multiband wavelet transform to get the watermarked image. The value of mean structural similarity index measure (MSSIM) is calculated as measure of imperceptibility. Cross

correlation (CC) values are obtained under different attacks as measure of robustness. The CC value is calculated according to method followed by (Kumsawat, 2005).

Table 3 shows the simulation results for the respective values of MSSIM, CC, PSNR and normalized capacity obtained after 50 generations for different test images. It is to be noted that we have also used PSNR as measure of visual quality as it is widely used one. Probability of crossover is 0.95 and probability of mutation-0.2. Simulation results show that how proposed optimized watermarking scheme takes care for conflicting parameter values simultaneously. Similarly, Table 4 shows the gradual improvement of MSSIM, CC, PSNR and normalized capacity with the number of generations /iterations for the test image Lena.

Shih (Shih, 2005) has also shown an interesting application of GA for medical image watermarking. In medical images, in order to make a good trade-off between the compression rate and correct diagnosis, a hybrid compression method has been developed. The region of interest (ROI) is processed with lossless compression and the rest with lossy compression. The watermark is embedded surrounding the ROI for copyright protection. The host image is divided into ROI and non-ROI. Robust technique is used for embedding the watermark of signature information or textual data around the ROI of a medical image based on genetic algorithms. A fragile watermark is adopted to detect any unauthorized modification.

Wavelets and GAs are also used together to find optimized values of 'M' in M-band wavelet decomposition and 'N' value in N-ary modulation in the work of optimized spread spectrum watermarking (Maity, 2006; Panda, 2009). It is reported in (Maity, 2006) that M-band wavelets and N-ary modulation scheme improves both imperceptibility and robustness in high payload SS watermarking system. The large value of 'M' in M-band wavelets offers better imperceptibility through better scale-space tiling. On the other hand, large N-values in N-ary modulation

Figure 7. Block diagram for optimization of zero-rate SS watermarking using genetic algorithms

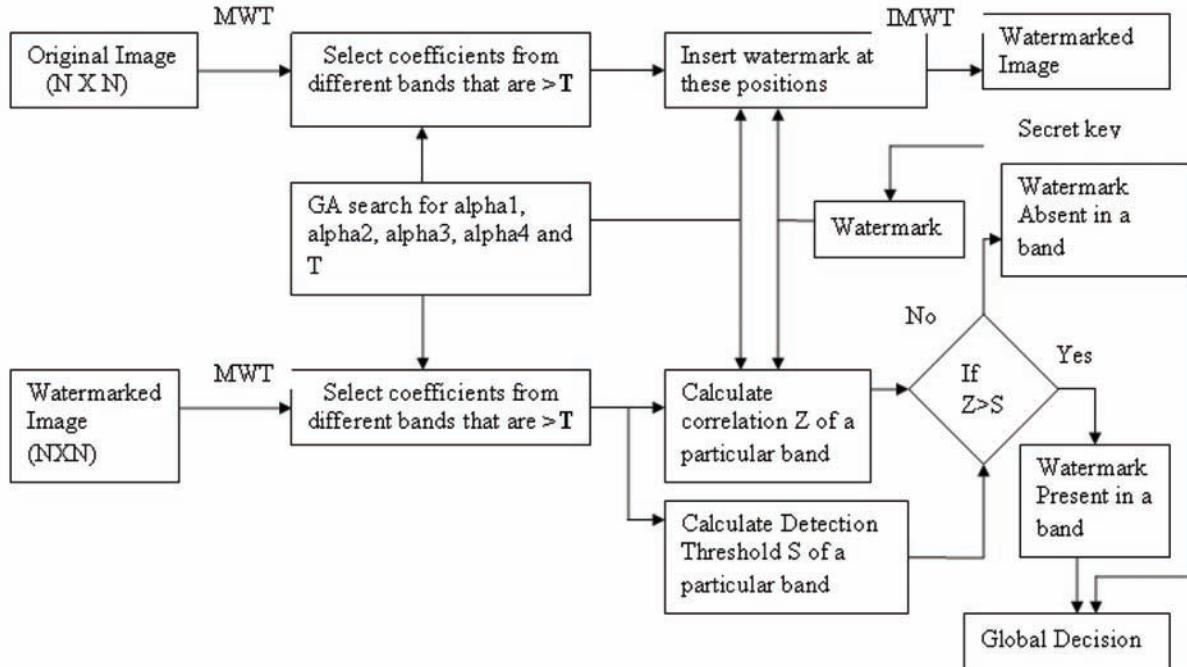


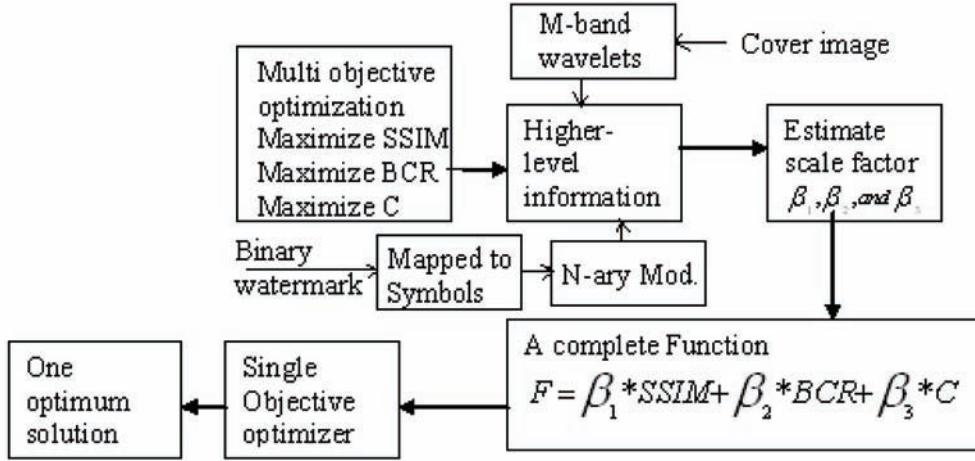
Table 3. Normalized capacity, PSNR, MSSIM and CC for different images

Image	MSSIM	CC	PSNR	Normalized Capacity
Lena	0.9813	0.4444	34.2551	0.2738
Baboon	0.9775	0.3111	31.1748	0.7795
Pepper	0.9846	0.3222	34.9662	0.2345

Table 4. Normalized capacity, PSNR, MSSIM and CC for different generations incase of Lena image

Generations	MSSIM	CC	Capacity (normalized)	PSNR (dB)
5	0.9869	0.2556	0.2514	35.5927
8	0.9863	0.3111	0.2738	35.6418
10	0.9824	0.3778	0.2738	34.5298
12	0.9820	0.3889	0.2738	34.4029
30	0.9813	0.4444	0.2738	34.2551
50	0.9813	0.4444	0.2738	34.2551

Figure 8. Block diagram for optimization of M-band wavelet and N-ary modulation in SS watermarking



improve significant detection reliability at the cost of exponential computation cost. It is also shown that similar performance at lower N-value is possible with the use of higher M-values. Then, an optimized set of values for M and N become essential to meet acceptable imperceptibility and robustness with high payload and at low computation cost. This motivates the development of optimized M-band wavelets and N-ary modulation based SS watermarking. The fitness function used in watermarking consists of weighted average of imperceptibility, robustness and normalized capacity. The maximization of fitness function under the constraint of sum of weight factor to be 1 is searched for. Watermark embedding subbands are selected depending on their variance values. Each bit or symbol of watermark information is embedded in the two sets of subbands that have the variance value in the lower and upper range. A block schematic representation for the algorithm is shown in Figure 8.

GA is also used to find the optimal watermark from a watermark database that will be the best suited for a particular host image from the image database (Phadikar, 2009). The scheme integrates GA with DWT to avail the benefits of multi resolution analysis (MRA). The use of lifting reduces

computation time of the proposed scheme. GA is used to reduce searching time for watermarking in image database. Experimental results duly support those claims.

FUTURE RESEARCH DIRECTIONS

Over the last one and half decade, digital watermarking techniques are being explored for varieties of applications. The applications vary from conventional copyright protection, ownership identification, copy protection, authentication, integrity verification to the several new and promising applications like QoS (quality of services) assessment in future generation wireless communication, data indexing, medical transcription, lured application etc. All these diverse applications demand fulfillment of varieties of conflicting requirements and thus makes digital watermarking research as an interesting optimization problem. Mathematical analysis to find optimal solution, most often, theoretically sounds well but results obtained through simulations are not always appealing. The main reason is due to the fact that mathematical analysis considers particular statistical model for the host signal

and attacks. On the other hand, the real life host and the majority of the attacks cannot be modeled exactly in the similar statistical form. Hence design of implementation based optimized digital watermarking methods become highly demanding. This in turn demands the scope of usage of several bio-inspired soft computing tools such as fuzzy logic, genetic algorithms, neural networks, support vector machine, chaos theory, and particle swarm optimization. Some of the possibly less/unexplored but interesting promising applications may be considered as future work for designing optimized watermarking techniques. From that perspective, the chapter will give an insight how analytical methods as well as soft-computing tools can be made use for optimization in watermarking. It can be remarked here that soft-computing tools often give better results compared to analytical result and integration or synergy of these tools such as fuggy-GA, neuro-fuzzy, GA-neuro etc. can also be explored to enhance performance results further.

(1) To determine information hiding capacity for a given host signal, information-theoretic model is mostly used. The research in this direction focuses on the maximum amount of information that can be hidden i.e. the upper limit of hidden information. But determining the lower limit of information hiding or the amount of information that can reliably be decoded with minimum error probability (even after attacks), is also an interesting problem. It is difficult to analyze this lower bound incorporating the characteristics of the host and using information theory. The application of soft-computing tools may be more appropriate in such cases. Neural network based information-hiding capacity may be studied and can be explored further for different information hiding scenarios, such as covert channels, steganography, anonymity and copyright marking, and fingerprinting.

(2) Genetic algorithm based optimal spread spectrum watermark embedder and improved detection discussed in this chapter can be integrated

with the concept of GA based watermark shaping to achieve optimal imperceptibility in data hiding. Similarly, GA based watermark shaping can also be integrated with fuzzy logic based improved detection. Integration of SVM based color image authentication may also be explored for spread spectrum watermarking and GA based watermark shaping. The integration expects to achieve better detection. This is due to improved classification performance over traditional learning methods.

(3) Although spread spectrum and QIM watermarking are governed by well defined mathematical analysis of individual type, integration of various soft-computing tools can be well explored for further betterment. For example, in zero rate SS watermarking for reduction of HSI, the nonlinear function $\mu(x,b)$ can be derived to minimize the expected detection error probability with the aid of soft-computing, instead of using numerical technique; similarly, to maximize WHC in zero rate SS watermarking, GA based watermark shaping can be applied for better implementation than the analytic approach. Integration of QIM theory with the use of soft-computing tools which has been discussed less in the chapter may be explored as future research. For example, the authors in (Braci, 2008a) did not show any well defined mathematical relation between security and robustness. They have used alternative simulation results to show the trade-off relation. In such case, one may develop a GA based optimization function from the weighted average of the two parameters. Similar may be the case for (Boyer, 2006) where the authors have used KLD to avoid intractability of false-alarm probability but GA may directly be used.

(4) Recently a comparative study of five evolutionary based algorithms (genetic, memetic, ant-colony optimization, shuffled frog leaping, and PSO algorithm) is reported. It is found that the PSO method outperforms the other four algorithms in success rate, solution quality, and processing time. Some of the GA based optimized watermarking schemes may be re-explored using PSO. Another

important tool, called chaotic dynamic system may be explored to generate special sequences applied in spread spectrum watermark. With controlling parameter, chaotic sequences show various spectrum properties such as lowpass or highpass properties. Accordingly, watermark energy may be concentrated in order to meet the characteristics. For example, if the spread spectrum watermark is expected to survive the strong compression, the sequences with lowpass property should be chosen (Feng, 2006).

(5) Some optimization is also done on attacker's perspective. As matter of fact, GA based breaking algorithms on spatial domain steganalytic systems and frequency domain steganalytic systems are developed. The emphasis is shifted from traditionally avoiding the changes of statistic features to artificially counterfeiting the statistic features. The idea is based on the concept as follows: in order to manipulate the statistic features for breaking the inspection of steganalytic systems, the GA-based approach is adopted to counterfeit several stego-images (candidate images) until one of them can break the inspection of steganalytic systems. The game theory is also extensively used: for a given capacity, the attacker and the owner try, respectively, to minimize and maximize the attack distortion. The goal of the embedder is to maximize payload capacity with minimum achievable distortion. On the other hand, the opponent optimizes by selecting the filter and noise to minimize attacked-signal distortion under a capacity constraint. A significant research on optimal attack models on watermarking has been carried out by Su, Eggers and Girod (Su, 2000; Su 20001) as well as Moulin et al (Moulin, 2003). The works vary from capacity analysis subject to optimal collusion attack, desynchronizing attacks, amplitude scaling and additive white noise attack. This is also extended to a strong attack that still provides an attacked document with good subjective quality. All these related works can be re-explored with the aid of several soft-computing tools discussed here.

(6) One direction of future research work for watermarking may be application specific. Hence, more implementation algorithms rather than mathematical modeling are also demanded. For example, in host signal database application, with a given set of watermarks (company trademark) and cover signals (company product), how optimally watermark can be selected for the respective cover. This may demand optimum deformation of the cover signal in the form of rotation, scaling, warping, morphing or erosion. The objective is to minimize the dissimilarity difference between the watermarks and the cover signals. In lured watermark application, this can be used for secret information transmission so that steganalysis cannot detect the presence of the hidden message.

(7) Recently, watermarking of image database gets its popularity for the protection of cultural unit which is no longer a single image but a large scale structured or unstructured (such as the web) image database. In other words, a single image is useless; it only gets importance in relation to a large database. Optimization in watermarking may be explored for copyright protection of image database.

(8) Nowadays, it is rare to encounter any kind of multimedia signal in a raw, uncompressed format, be it in the digital cameras, world wide web alike, or audio/video-on-demand on broadcast network channel. So future research work may be explored for optimized watermarking on compressed host data. However, watermarking and compression operations are antagonistic in characteristics, while the former exploits redundancy present in the host, the latter operation removes the same. Optimized algorithm needs to be designed so that for a given compression rate of the host data, how watermark power and payload can be distributed to meet acceptable levels of imperceptibility and robustness as well as the file size of the compressed data remains unchanged.

Research on optimized watermarking should also be directed for development of application specific low cost algorithm in order to imple-

ment in real time through hardware. Some of the optimized watermarking methods discussed here may be explored to design VLSI chip using ASIC or FPGA.

CONCLUSION

The chapter discusses digital watermarking from the angle of an optimization problem. First, optimization in watermarking is analyzed from mathematical perspective in the context of spread spectrum modulation and quantization index modulation. This mathematical analysis highlights the theoretical bound one can achieve in optimized watermarking system and how different conflicting requirements may be trade-off. A detailed discussion for soft-computing based optimized watermarking then follows. Discussion gradually moves from simple spatial domain methods, unitary transform domain optimized watermarking scheme to several wavelet domain methods. This host signals considered here vary from image, video to audio, gray scale images to color images, uncompressed data to compressed data. Scope of several soft-computing tools, namely fuzzy logic, genetic algorithms, neural network, support vector machine, chaotic theory, particle swarm optimization tools are analyzed with the merits and limitations of individual. The discussion is done in the context of design of overall optimized watermarking systems, optimization on individual aspect, namely embedder optimization, attack optimization, estimation of attack parameters, optimized improved detection, optimized watermarking in image database, etc. A good number of future research problems related to optimized watermarking are discussed at the end. The problems explore the scope of several soft-computing tools as well as with respect to newer emerging applications. The chapter presents an overall discussion on optimized watermarking system, of course, not fully exhaustive. Beginner in watermarking research will learn mathematical

analysis and the usage of soft-computing tools to design optimized system. At the same time, experts in the field will find several interesting problems and integration of several tools and techniques to solve the problem optimally.

REFERENCES

- Barni, M., & Bartolini, F. (2004). *Watermark System Engineering*. New York: Marcel Dekker.
- Bezdek, J. C., & Pal, S. K. (Eds.) (1992). Fuzzy models for pattern recognition: methods that search for structures in data. New York: IEEE CS Press.
- Bhattacharya, A. (2009). *On Optimization of M-band wavelets zero-rate spread spectrum watermarking using Genetic Algorithms*. Unpublished master's thesis, Bengal Engineering and Science University, Shibpur, India.
- Boyer, J.-P., Duhamel, P., & Blanc-Talon, J. (2006). Asymptotically optimal scalar quantizers for QIM watermark Detection. In *Proceedings of IEEE International Conference on Multimedia and Expo*.
- Braci, S., Boyer, R., & Delpha, C. (2008a). On the trade-off between security and robustness of the trellis coded quantization scheme. In *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*.
- Braci, S., Boyer, R., & Delpha, C. (2009b). Security evaluation of informed watermarking schemes. *IEEE International Conference on Image Processing (ICIP)* (Accepted).
- Braci, S., Delpha, C., & Boyer, R. (2009a). How quantization based schemes can be used in steganographic context. In *IEEE Int. Workshop on Multimedia Signal Processing (MMSP)*, Rio de Janeiro, Brazil.

- Braci, S., Delpha, C., Boyer, R., & Guelvouit, G. L. (2008b). Informed stego-systems in active warden context: statistical undetectability and capacity. In *Proceedings of IEEE International Workshop on MultiMedia Signal Processing (MMSP)*, Cairns, Queensland, Australia.
- Cachin, C. (1998). An information theoretic model for steganography. In D. Aucsmith (Eds.), *Proceedings of 2nd Workshop on Information Hiding* (LNCS vol.1525, pp. 306–318). Berlin: Springer.
- Chan, C. K., & Cheng, L. M. (2001). Improved hiding data in images by optimal moderately significant-bit replacement. *IEE Electronics Letter*, 37(16), 1017–1018. doi:10.1049/el:20010714
- Chen, B., & Wornell, G. W. (2001). Quantization Index Modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, 47(4), 1423–1443. doi:10.1109/18.923725
- Costa, M. H. M. (1983). Writing on dirty paper. *IEEE Transactions on Information Theory*, 29(3), 439–441. doi:10.1109/TIT.1983.1056659
- Cox, I. J., Kilian, J. F., Leighton, T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673–1687. doi:10.1109/83.650120
- Cox, I. J., Miller, M. L., & Bloom, J. A. (2001). *Digital Watermarking*. San Francisco: Morgan Kaufmann.
- Depovere, G., Kalker, T., & Linnartz, J. P. (1998). Improved watermark detection reliability using filtering before correlation. In *Proc. of IEEE International Conference on Image Processing (ICIP)*: (Vol. 1, pp. 430–434).
- Eggers, J., & Girod, B. (2002). *Informed Watermarking*. Amsterdam: Kluwer Academic Publishers.
- Eggers, J. J., Bauml, R., Tzhoppe, R., & Girod, B. (2003). Scalar Costa scheme for information embedding. *IEEE Transactions on Signal Processing*, 51(4), 1003–1019. doi:10.1109/TSP.2003.809366
- Esen, E., & Alatan, A. A. (2004). *Data Hiding using Trellis Coded Quantization*. ICIP.
- Esen, E., Alatan, A. A., & Askar, M. (2003). *Trellis coded quantization for data hiding*. Ljubljana, Slovenia: EUROCON.
- Feng, G. R., Jiang, L. G., He, C., & Xue, Y. (2006). Chaotic spread spectrum watermark of optimal space-filling curves. *Chaos, Solitons, and Fractals*, 2, 580–587. doi:10.1016/j.chaos.2005.04.051
- Forney, G. D. Jr. (1973). The Viterbi algorithm. *Proceedings of the IEEE*, 61, 268–278. doi:10.1109/PROC.1973.9030
- Ghosh, A., & Pal, S. K. (Eds.). (2002). *Soft computing approaches to pattern recognition and Image processing*. Singapore: World Scientific Press.
- Guillon, P., Furon, T., & Duhamel, P. (2002). Applied public-key steganography. In *Proceedings of SPIE*, San Jose, CA.
- Hassanien, A. E., Abraham, A. & Grosan, C. (2009). Spiking neural network and wavelets for hiding iris data in digital images. *Bio-inspired information hiding: A fusion of foundations, methodologies and applications*, 13(4), 401-416.
- Hwang, M. S., Chang, C. C., & Hwang, K. F. (2000). Digital watermarking of images using neural networks. *Journal of Electronic Imaging*, 9, 548–555. doi:10.1117/1.1289357
- Khan, A., & Mirza, A. (2007). Genetic perceptual shaping: utilizing cover image and conceivable attack information using genetic programming. *Information Fusion*, 8(4), 354–365. doi:10.1016/j.inffus.2005.09.007

- Kumar, K. S., & Sreenivas, T. (2007). Increased watermark-to-host correlation of uniform random phase watermarks in audio signals. *Signal Processing*, 87, 61–67. doi:10.1016/j.sigpro.2006.04.005
- Kumsawat, P., & Attakitmongkol, K. (2005). Anew approach for optimization in image watermarking by using genetic algorithms. *IEEE Transactions on Signal Processing*, 53(12), 4707–4719. doi:10.1109/TSP.2005.859323
- Kutter, M., Jordon, F., & Bossen, F. (1998). Digital watermarking of color images using amplitude modulation. *Journal of Electronic Imaging*, 7(2), 326–332. doi:10.1117/1.482648
- Le Leguelvouit, G. (2005). *Trellis coded quantization for Public key steganography*. Philadelphia, USA: ICASSP.
- Maity, S., Maity, S. P., & Sil, J. (2009d). Spread spectrum watermark embedder optimization using Genetic Algorithms. In 7th International Conferences on Advances in Pattern Recognition, (pp.29-32). Washington, DC: IEEE CS Press.
- Maity, S. P. (2008). *Studies on data hiding in digital media for secured communication, authentication and content integrity*. Unpublished doctoral dissertation, Bengal Engineering and Science University, Shibpur, India.
- Maity, S. P. & Kundu, M. K. (2009). Genetic algorithms for optimality of data hiding in digital images. *Bio-inspired information hiding: A fusion of foundations, methodologies and applications*, 13(4), 361-373.
- Maity, S. P., Kundu, M. K., & Das, T. S. (2007). Robust SS watermarking with improved capacity. *Pattern Recognition Letters*, 28, 350–357. doi:10.1016/j.patrec.2006.04.004
- Maity, S. P., Kundu, M. K., & Mandal, M. K. (2006). Performance improvement in spread spectrum watermarking via M-band Wavelets and N-ary modulation. In *Proceedings of 3rd IET International Conference on Visual Information Engineering*, (pp. 35-40).
- Maity, S. P., & Maity, S. (2009a). Multistage spread spectrum watermark detection technique using fuzzy logic. *IEEE Signal Processing Letters*, 16(4), 245–248. doi:10.1109/LSP.2009.2014097
- Maity, S. P., Maity, S., & Sil, J. (2009b). Diversity Assisted GCIC for Spread Spectrum Watermark Detection using Genetic Algorithms. *IEEE Conference on Image Processing*, (pp.3649-3652). Washington, DC: IEEE CS Press.
- Maity, S. P., Maity, S., & Sil, J. (2009c). Estimation of fading attack on high payload spread spectrum watermarking with variable embedding rate using genetic algorithms. *Third International Conference on Imaging for Crime Detection and Prevention (ICDP-09)*, (Accepted).
- Malver, H., & Florencio, A. F. (2003). Improved spread spectrum: A new modulation technique for robust watermarking. *IEEE Transactions on Signal Processing*, 51(4), 898–905. doi:10.1109/TSP.2003.809385
- Marcellin, M. W., & Fisher, T. R. (1990). Trellis coded quantization of memoryless and Gauss-Markov sources. *IEEE Transactions on Communications*, 38, 83–93. doi:10.1109/26.46532
- Miller, M. L., Doerr, G. J., & Cox, I. J. (2002). Dirty-paper trellis codes for watermarking. In *Proc. of IEEE Int. Conf. on Image Processing*, Rochester, New York, (vol. 2, pp. 129–132).
- Miller, M. L., Doerr, G. J., & Cox, I. J. (2004). Applying informed coding and embedding to design a robust high capacity watermark. *IEEE Transactions on Image Processing*, 13, 792–807. doi:10.1109/TIP.2003.821551

- Moulin, P., & Ivanovic, A. (2003). The zero-rate spread spectrum watermarking game. *IEEE Signal Processing*, 51(4), 1098–1117. doi:10.1109/TSP.2003.809370
- Pal, S. K., Ghosh, A., & Kundu, M. K. (Eds.). (2000). *Soft Computing for Image Processing*. Heidelberg, Germany: Physica Verlag.
- Pal, S. K., & Mitra, S. (1999). *Neuro-fuzzy pattern recognition methods in soft computing*. New York: John Wiley.
- Pal, S. K., & Wang, P. P. (1996). *Genetic algorithms for pattern recognition*. Boca Raton, FL: CRC Press.
- Pan, J. S., & Abraham, A. (Eds.). (2009). Bio-inspired information hiding: A fusion of foundations, methodologies and applications. Springer, 13(4).
- Pan, J. S., Huang, H. C., & Jain, L. C. (Eds.). (2004). *Intelligent Watermarking Techniques*. Singapore: World Scientific.
- Pan, J. S., Huang, H. C., & Wang, F. H. (2001). Genetic watermarking techniques. In *Proceedings of the fifth International Conference on Information Engineering Systems & Allied Technologies*, (pp. 1032-1036).
- Panda, M. (2009). *On Optimization of M-band wavelets and N- ary modulation for high payload spread spectrum watermarking using Genetic Algorithms*. Unpublished master's thesis, Bengal Engineering and Science University, Shibpur, India.
- Phadikar, A., Maity, S. P., & Kundu, M. K. (2009). An Optimized Image Database Watermarking Scheme using Genetic Algorithms and Lifting. In *Proceedings of IEEE International Advanced Computing*, (pp. 2151-2155).
- Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, 27, 379–423.
- Shieh, C. S., Huang, H.-C., Wang, F. H., & Pan, J. S. (2004). Genetic watermarking based on transform domain techniques. *Pattern Recognition*, 37(3), 555–565. doi:10.1016/j.patcog.2003.07.003
- Shih, F. Y. (2004). *Digital watermarking and steganography- fundamental and techniques*. Boca Raton, FL: CRC Press.
- Shih, F. Y., & Edupuganti, V. G. (2009). A differential evolution based algorithm for breaking the visual steganographic system, *Bio-inspired information hiding: A fusion of foundations, methodologies and applications*, 13(4), 345-353.
- Shih, F. Y., & Wu, Y. T. (2005). Robust watermarking and compression for medical images based on genetic algorithms. *Information Sciences*, 176, 200–216. doi:10.1016/j.ins.2005.01.013
- Su, J. K., Eggers, J. J., & Girod, B. (2000) Optimum attack on digital watermarks and its defense. In *Proceedings of 34th Asilomar Conference on Signals, Systems and Computers*, Asilomar, CA, USA.
- Su, J. K., Eggers, J. J., & Girod, B. (2001). Analysis of digital watermarks subjected to optimum linear filtering and additive noise. *Signal Processing*, 81, 1141–1175. doi:10.1016/S0165-1684(01)00038-X
- Tsai, H., & Sun, D. (2007). Color image watermark extraction based on support vector machines. *Information Sciences*, 177(2), 550–569. doi:10.1016/j.ins.2006.05.002
- Ungerboëck, G. (1987). Trellis-coded modulation with redundant signal sets, parts i and ii. *IEEE Communications Magazine*, 25, 5–21. doi:10.1109/MCOM.1987.1093542
- Viterbi, A. (1967). Error bounds for convolution codes and an asymptotically optimum decoding algorithm. *IEEE Transactions on Information Theory*, 13, 260–269. doi:10.1109/TIT.1967.1054010

- Wang, R. Z., Lin, C. F., & Lin, J. C. (2000). Hiding data in images by optimal moderately significant-bit replacement. *IEE Electronics Letters*, 36(25), 2069–2070. doi:10.1049/el:20001429
- Wang, R. Z., Lin, C. F., & Lin, J. C. (2001). Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition Letters*, 34(3), 671–683.
- Wang, Y. G., Lu, Z. M., Fan, L., & Zheng, Y. (2009). Robust dual watermarking algorithm for AVS video. *Signal Processing Image Communication*, 24, 333–344. doi:10.1016/j.image.2009.03.004
- Wen, X. B., Zhang, H., Xu, X. Q. & Quan, J.J. (2009). A new watermarking approach based on probabilistic neural network in wavelet domain. *Bio-inspired information hiding: A fusion of foundations, methodologies and applications*, 13(4), 355–360.
- Wu, M., & Liu, B. (2003). *Multimedia Data Hiding*. New York: Springer-Verlag.
- Yu, P. T., Tsai, H. H., & Lin, J. S. (2001). Digital watermarking based on neural networks for color images. *Signal Processing*, 81, 663–671. doi:10.1016/S0165-1684(00)00239-5
- Zhang, F., Pan, Z., Cao, K., Zheng, F., & Wu, F. (2008). The upper and lower bounds of the information-hiding capacity of digital images. *Information Sciences*, 178, 2950–2959. doi:10.1016/j.ins.2008.03.011
- Katzenbeisser, S., & Petitcolas, F. A. (Eds.). (2000). *Information hiding techniques for steganography and digital watermarking*. Norwood, MA: Artech House.
- Moulin, P., & Koetter, R. (2005). Data-Hiding codes. *Proceedings of the IEEE*, 93(12), 2083–2126. doi:10.1109/JPROC.2005.859599
- Voloshynovskiy, S., Pereira, S., & Pun, T. (2001). Attacks on digital watermarks: classification, estimation-based attacks, and benchmarks. *IEEE Communications Magazine*, 39(8), 2–10. doi:10.1109/35.940053

KEY TERMS AND DEFINITIONS

Digital Watermarking: Digital watermarking deals with hiding or embedding of an auxiliary message in digital content in a secure, robust and imperceptible fashion.

Optimized Watermarking: Optimized watermarking corresponds to a state that attempts to maximize imperceptibility (minimizes embedding distortion), robustness, payload/capacity and statistical invisibility of the hidden data.

Spread Spectrum Watermarking: A robust watermarking scheme that works on the principle of spread spectrum modulation of digital communication. Each bit of watermark information is spread over wide spectrum of the cover signal through the use of pseudo-noise spreading code.

QIM Watermarking: This is a watermarking scheme that applies quantization operation on host signal, where the embedding function is viewed as an ensemble of the cover indexed by the message to be hidden.

Soft Computing: Soft computing is a consortium of methodologies that aims to exploit the tolerance for imprecision, uncertainty, approximate reasoning and partial truth in order to achieve tractability, robustness, low cost solution, and close resemblance to human like decision making.

ADDITIONAL READING

- Johnson, N. F., Duric, Z., & Jojodia, S. (2001). *Information hiding, steganography and watermarking-attacks and countermeasures*. Moston, MA: Kluwer.

Fuzzy Logic: It is a soft computing tool that deals with imprecise or vague information and contains objects that satisfy imprecisely defined properties to varying degrees.

Artificial Neural Network: A soft computing tool that attempts to mimic human learning and adaptation property. It enjoys the characteristics of adaptivity, speed, robustness, ruggedness and optimality in decision making process through computation.

Genetic Algorithms: A soft computing tool widely used in optimization and complex search problems. It works on a set of coded solutions, called population, with three basis operations: selection/reproduction, cross-over and mutation.

TCQ Watermarking: Trellis Coded Quantization (TCQ) is a quantization method using a structured codebook which has been applied in watermarking specially for quantized based schemes.

Chapter 16

Application of Error Control Coding for Multimedia Watermarking Technologies

Mehul S. Raval
DA-IICT, India

ABSTRACT

Intellectual property right, copyright, trademark, digital rights management (DRM) are buzz words heard more often in era of Internet. Along with the uncountable advantages Internet has also brought certain evils. These evils have social, technological, economical and legal impact on our society in general. One of the issues concerning the “content creators” is mass violations of copyrights for their work through illegal distribution via “darknet”. Watermarking is seen as one of the component for DRM systems that can act as a deterrent to content flowing into the darknet. The performance of watermarking schemes can be improved if channel codes are used for encoding the hidden message. The chapter targets applications of Error Control Coding (ECC) to watermarking namely: copyright protection, authentication, forensics and stego watermarking techniques including active steganography. This chapter aims at studying various properties of watermarking systems (depending on application), looking into their specific requirements and then try to search for suitable error control code. This will boost the over all performance of watermarking techniques. This chapter also intends to discuss the state of art research in this direction and then presents a watermarking method based on facts covered in chapter.

INTRODUCTION

The watermarking has seen a sudden spurt in activities and interest after 1995. This is an era when internet started penetrating globe connectivity. This brought several worrying points including the rising

concerns for copyright violations. Watermarking is seen as one of the potential means for preventing content flowing into the darknet. The watermarking has been included as technology into future DRM standards. The goal of the **watermarking** is to protect the copyright and prove ownership of digital content. There are several applications of watermarking apart from copyright protection. The

DOI: 10.4018/978-1-61520-903-3.ch016

Table 1. Associating watermarking with applications and their desirable properties

Type	Application	Desirable property
Robust watermark	Copyright protection/Ownership identification	Robustness (Ability to survive)/Security
Fragile watermark	Authentication/Integrity of the content	Sensitivity to changes / Fragility
Forensic	Finger printing/ Traitor tracing	Detection of tampering/ Localization of changes/ Possible revival of content.
Active steganography	Covert and secure communication	Security / Undetectability / Capacity

Table 1 associates the type of watermark with their application and its desirable properties (Ingemar, 2008; Wenjun, 2006). It is presumed that readers are very clear about the basics of each one of these applications and hence they have been described very briefly in Table 1.

Summarizing issues that can be handled well by the ECC for watermarking are:

- Providing reliable transmission of watermark through communication channel (Ingemar Cox, 2008)
- Improving the payload of watermark by using codes operating near Shannon's limit (A. Bastug, 2004).
- Providing authentication and traitor tracing (Kaushal, 2004).
- Providing the covert and secure communication (Kaushal, 2007).
- Providing the unauthorized access protection (M. C. Davey, 2001).

However we have to always consider the fact when ECC is applied to watermarking is that, every type of code will perform error correction to its capacity only above minimum SNR level in communication channel. Below this level some of the codes instead of providing a "gain" will introduce a "loss" in terms of increased BER. This increased BER can also attributed be type of decoder and characteristics of errors. If we can keep check on channel input BER than we can use any type of ECC provided output BER drops.

BACKGROUND

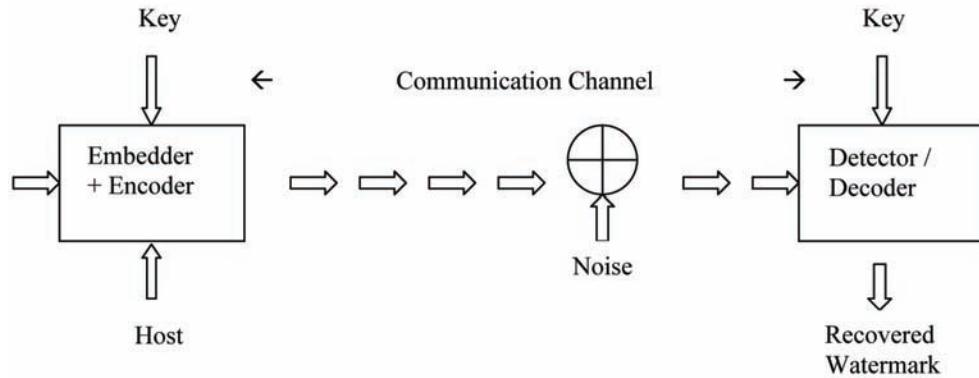
Watermarking as a Communication Problem Perspective

Channel coding has been classically seen as a mean for increasing reliability during transfer of content. Importance of coding theory has been realized and it has been applied to different communication scenario. Errors occur due to intentional or unintentional manipulations that are applied to the "watermarked" data as it travels through communication channel. Thus watermarking can also be seen as a communication problem (M. Barni, 1998; J.R.Herandez, 2000).

The block diagram in Figure 1 represents this model. The watermark is "message" which is to be sent from transmitter to receiver. There is a notion of communication channel and insertion of noise into the transmitted message. This noise is due to intentional or unintentional manipulations that may occur during its journey. The noise is presumed to be independent of the message being transmitted. There are multiple ways in which this can be handled and in one of the scenario the cover object or container itself is treated as a noise (Is it like an ordinary noise superimposed in channel?).

This model allows one to use conventional wisdom of information and communication theory and apply it to domain of digital watermarking. One of them is application of "channel coding" to improve the performance in terms of Bit Error Rate (BER) reduction. Statistical formulation and

Figure 1. Watermarking from communication problem perspective



analysis of the spread spectrum watermarking techniques was carried out for better understanding of watermarking as communication problem by J.R.Hernandez(1999). There are several advantages for this formulation like:

1. Watermarking techniques performance parameters can be defined, quantified, analyzed.
2. Effects of these parameters on images drawn from different distribution for specific watermarking application can be quantified and studied.
3. The watermarking detectors and decoders can be made efficient and their performance be enhanced.

In most of the cases for an ECC scheme, not every sequence of the given alphabet is used for watermark message representation but only few valid code words are chosen from the alphabet. By suitable mapping between the given watermark message and the valid sequences, decoders will be able to identify the sequence closest to the recovered one. Thus ECC would improve the performance depending on the redundancy generated. The performance of watermarking scheme is dependent on detectors/decoders which are discussed in next section.

Watermarking Detectors / Decoders

Watermarking **detectors/ decoders** are the most crucial design element of this chain. In-fact the watermark encoder design would be governed by the characteristics of decoder. For the copyright applications watermark detector/decoder performs two important functions. First it detects the presence of the watermark in the given digital content. On affirmation, watermark decoder extracts and decodes the watermark. The use of the secret key in this whole scenario is optional. The watermarking decoder has two important design criteria: The probability of false positive or probability of insertion and probability of false negative or deletion.

Computational complexity is also one of the prime requirements for real time implementation of watermarking. The design of decoders plays an important role in this aspect. For e.g. in case of the correlation based decoder the number of correlative computations can be reduced if given watermark message is represented by the code words from given alphabet. In case if every possible sequence of the given alphabet is used for the representation of the watermark than some sequences may have poor distance separation and it deteriorates the error performance. ECC can be used to handle this issue. This problem will become

severe as the length of the sequence for message representation increases (Ingemar, 2008) and the closest pairs becomes similar with the minimum distance among them reducing.

Often watermark decoders use Maximum-Likelihood (ML) detection to haul out the bits. The ML detector is dependent on the pdf of the original host. Normally Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) or Discrete Wavelet Transform (DWT) are used with the watermarking techniques. Statistical characterization of transforms yields very good design for the detectors and decoders in terms of performance. Since for blind detection original image is not available, detection of parameters are estimated from watermarked image. This will hold true under the assumption that watermark insertion have not changed the coefficients significantly. The DFT amplitudes are modeled by the “Weibull” distribution (A. Bastug, 2004). The scale and the shape parameters have to be estimated form the using a moment matching technique. **DCT** coefficients have some interesting statistical properties which can be exploited for improving the performance of detectors and decoders (J.R.Hernandez, 1999). Some of them are:

1. DCT is an energy compact transform.
2. If image statistics can be modeled as first order Markov processes with correlation factor close to 1, than it will have uncorrelated DCT coefficients.
3. AC coefficients can be better modeled than DC coefficients.
4. Low frequency DCT coefficients are modeled by Generalized Gaussian distribution (R. J. Clarke 1985).

Earlier AC coefficients were modeled as Gaussian but accurate representation is by the generalized Gaussian. Laplacian and Gaussian distribution are the special case of this distribution. Given that only small manipulations are done by watermark insertion and the fact that watermark

can be modeled statistically, a very good estimate of distribution parameters can be obtained.

In some watermarking technique bits are extracted by **hard decisions** which is typically characterize by the Binary Symmetric Channel (BSC) model. On the other hand if extraction is carried out with **soft decision** it becomes a case for additive Gaussian channel model. In BSC channel numbers of errors will follow the Gaussian distribution. Hard decision is simplest of approach for decoding for channel code. It has two steps:

1. Binary decision about each output bit from AWGN channel. It is compared with a threshold and resulting bits are called hard decisions.
2. Feeding these bits to a binary decoder.

However it may not be optimum always as there is a loss of information (J.-F. Delaigle, 2000). Better strategy would be obtain a real valued output from the AWGN and provide the output sequence. The outputs from AWGN channel are called soft decisions. In case of a soft decoding, information about reliability of decoded bits is kept. This will provide a set of binary words to work with instead of one binary word in hard decoding. So instead of using a *majority* logic one can use log- likelihood. This will improve the reliability of detection and errors in detection are minimized.

The types of codes which are commonly used in the watermarking domain are Reed Solomon (RS), Bose Chaudhuri and Hocquenghem (BCH), Low density parity check codes (LDPC), turbo codes, **convolution** or trellis codes. Different codes handle different types of error like burst errors are handled well by the RS and BCH codes, random errors are taken care by the Hamming code. Trellis or convolution code has provided the good performance in terms of BER and coding gain. Initial work in watermarking domain includes usage of trellis codes (Jim, 1999; J.R.Hernandez, 2000). Types of errors in watermarking are discussed in next section.

Types of Errors

Following are the types of error encountered normally in domain of watermarking:

1. Substitution
2. Insertion
3. Deletion
4. Erasure
5. Synchronization

Errors which are due to process of communication are known as “substitution” error. It is caused when transmitted bits are replaced by other bits at receiver. Block codes can be useful in correcting the substitution errors. In case of watermarking scenarios “insertion” and “deletion” errors are common. “Insertion” errors are caused when detector decides presence of watermarking bit even though none exist. This is the case of the false positives. For several watermarking applications like finger printing or traitor tracing false positives should be kept to the minimum (ideally zero). The false positive may lead to wrong diagnosis by a doctor or false implication in case of traitor tracing. “Deletion” errors are caused when watermarking bits are “missed” by the detector even though one is present. This is also termed as false negatives. For an application like traitor tracing this may not have much significance as compared to false positives. These false positive and negative rates are dependent on the application scenario. False positive and negative rates will be computed differently and have distinct implications in case of copyright protection Vis a Vis traitor tracing.

Synchronization error occurs when receiver cannot decide block boundary of a code word. Errors may also creep in due to deliberate losses incurred at the transmitter. In one such possible case shown by Kaushal (2004), usage of informed embedding in selection of coefficients at encoder is responsible for such erasures. Authors used informed embedding in which knowledge about the “cover” is exploited to embed the data. As

described earlier in certain scenario of watermarking, cover is also treated as a noise, but the peculiarity is that its statistics are known. This knowledge is exploited while embedding the data. In case the embedding criteria are not met, the symbol is erased at transmitter resulting in “erasures”. There are several types of channel codes like Reed Solomon (RS) code which can handle the erasures.

There is a specific property for each of the code which can be exploited depending on the application scenario. Some desirable properties of channel codes with reference to watermarking application includes:

1. It should be able to detect loss of synchronization and regain it quickly.
2. It should also be able to recover the corrupted bits.
3. Code should have a high code gain and operate nearly to Shannon’s limit.
4. Codes should be able to counter every possible type of error class.
5. Applications should not be very costly from computational and resource perspective. (This is really a tough requirement)

Types of Codes Useful for Watermarking

In this section let us explore the different codes which are useful for watermarking highlighting the basics for each one of these applications and codes.

Block Codes and Repetition Codes

The **block code** takes “ k ” message symbols and append it with the “ r ” redundant symbols to generate n message symbol code word. The improvement brought in by the (n, k) error correcting code is a function of redundancy n/k introduced and the minimum distance. It is however presumed that (n, k, d_{min}) like BCH code will correct all code

words containing up to t errors and will fail for all others. Instead of using the block codes, repetition coding can also be used (Severine Baudry, 2001). For a low value of SNR repetition code remained the best strategy. The block codes like BCH faltered in case of very low value of channel SNR. Repetition code is decoded by the majority logic.

The block codes are systematic and non systematic types. In systematic type the redundant symbols are added after the block of k message symbols. In case of non systematic block codes the redundant symbols are inserted in between the k message symbols block. These codes have significant practical applications and many analyses in the coding theory are available based on the block codes. The types of block codes are Hamming code, BCH, RS etc. The basic coding model, concept of the minimum distance, redundancy, code rate and perfect code are some of the basic concept required in understanding the block based codes. The next few sections are dedicated to illustrate these concepts.

Basic Coding Model

Each watermarking messages have to be encoded. Let each watermarking message be designated as \mathbf{M}_i . Each \mathbf{M}_i is represented by the finite sequence of symbol S_i drawn from the alphabet \mathbf{A} . The sequence S_i is also known as **code word**. The encoding function \mathbf{E} maps : $\mathbf{M}_i \rightarrow S_i$. This mapping represents encoding process. Not all the code words from the given alphabet \mathbf{A} will be used in mapping. If all code words have identical length (n) it is known as block code of length n .

The receiver attempts to retrieve the original message \mathbf{M}_i based on the received sequence S'_i . The corresponding decoding function \mathbf{D} : remaps $S'_i \rightarrow \mathbf{M}'_i$. The channel may introduce a noise due to which S'_i differs from S_i . In case the decoded message $\mathbf{M}'_i \neq \mathbf{M}_i$ it results in decoding error.

Minimum Distance Decoding (MD)

MD is one of the important decoding strategies. For a received code word \mathbf{C}' , MD decoder outputs

the code word \mathbf{C}'' which is closest in **hamming distance** terms to original code word \mathbf{C} . Hamming distance is defined as the number of positions in which the these codeword differ. This also represents the distance between the transmitted and received code word, which is equivalent to number of errors introduced in transmitted code word. Thus the **minimum distanced**(C) of a code word C is defined as

$$d(C) = \min_{C' \neq C} d(C, C')$$

Thus $d(C)$ is the minimum of pair-wise hamming distance between the different code words. It has been shown fundamentally in coding theory that code C can correct t errors iff $d(C) \geq 2t + 1$. Also it has been shown that code word is capable of correcting t errors and detecting s errors iff $d(C) \geq t + s + 1$. Thus greater the hamming distance better is error correcting capability.

Redundancy, Code Rate and Perfect Codes

Error correcting and detecting capability of the block codes is also dependent on the redundancy. An M message transfers over completely noise less channel requires q -ary k tuples for representation, such that $k = \lceil \log_q M \rceil$. $r = n-k$ is called the **redundancy** of the code. The code rate (R) = $\log_q M/n = k/n$ is an important parameter designating the reduction in information transfer. Shannon's channel coding theorem states that for $R < C$ Channel capacity, there is an existence of the error correcting code. Probability of decoding error reduces exponentially as the length of the code word is increased. It of course hints towards the existence of the coding mechanism and does not explicitly specify one. Codes which satisfy the Hamming bound are called as *perfect codes* and they have a *packing density* of 1. Hamming bound is an upper bound on the code rate for the MD code.

BCH can be decoded by the Berlekamp Massey algorithm. The problem is that this method is not

optimal as it is an *incomplete* algorithm. It means, it can find the closest code word in case only if distance is less than t . It could be Hamming distance for a BSC channel or Euclidean distance for an AWGN channel. For the BCH code complete algorithm with reasonable complexity is difficult to obtain. However with incomplete decoding algorithm, detection and decoding can be performed jointly. In case of failure for decoding the data can be considered as non-watermarked. Joint detection is more optimal in a sense that quantization of data does not occur thus it is loss less.

Reed Solomon Code (RS)

The **RS code** is one of the most applicable classes of codes with heaps of research utilizing the ease of this code. For any (n,k) code singleton bound which holds true is $d \leq r + 1$. It holds for any linear codes i.e. $M_q(n,d) \leq q^{n-d-1}$ where M is the cardinal number of length q , d is the minimum distance, n is length of code. The code reaching this bound is called is an optimal code and is called the maximum Distance Separable (MDS) code.

Reed Solomon code can correct up-to $(n-k)$ erasures and $(n-k)/2$ errors. Also it is desirable that the block length n of the RS code be smaller than watermarking alphabet. RS code also uses large non binary alphabets and such symbols can be interpreted as a block of bits. This can be well matched with the block based scheme of watermark insertion as the entire blocks are placed or removed.

Interleaving is also an important phenomenon in which the code symbols are interleaved so as to reduce the effects of burst error. In burst errors several blocks of data is lost simultaneously. So if the data is interleaved it will lead to partial loss per block after de-interleaving which is repaired by error correction mechanism. If interleaving is not performed than the entire code word would be lost and recovery is not possible. The objective of interleaving is thus to spread the erasure at the

encoder so that out of every n bits transmitted at least k bits are received at the receiver. Codes words can be arranged in such a manner that code symbols with least probability are placed at the center of an image where it is certain to contain the details. Unfortunately RS code is not matched well with the AWGN channel. They may be used in conjunction with the inner code which can essentially be matched to a communication channel like a low density parity check codes (LDPC) which is covered next.

Low Density Parity Check Codes (LDPC)

LDPC codes are linear codes with sparse parity check matrix. It means that only small number of rows and column elements are one, rest are all zero. This will also reduce the complexity of the “belief propagation” based decoder (M. C. Davey 2001). The code is defined as (n,c,r) code with length n , parity check matrix has column of weight c and the rows has weight r . Incidentally they also define the quality of LDPC code along with the minimum hamming distance d . LDPC code with equal number of 1's in rows and columns are called as regular while with unequal number of rows and column are called as irregular code. Good irregular code requires probability models. They have to be appropriately chosen to improve the gain factor of the code. The LDPC code ensembles are defined by n,c,r . The LDPC codes have following different parameters based on which the construction are possible

- The minimum hamming distance d
- Code length n and rate R .
- Girth g_0
- BER in AWGN channel

Some of the properties of regular LDPC codes are:

- Each row of parity check matrix contains exactly r ones.
- Each column of parity check matrix contains exactly c ones.
- The number of non zero position common to any two columns are no more than 1

Decoding algorithm for LDPC codes are both soft and hard decision cases. The soft decision iterative scheme can operate with both probability / log likelihood ratio and it gives good results in AWGN channel. “Belief propagation” algorithm is the standard procedure for decoding the LDPC code. The maximal numbers of decoding iterations are based on the code length n , required BER and decoding complexity requirement. LDPC codes have different convergence speed depending on the implementation. It may act as one of the parameter for selection of code in communication systems. The most known fast LDPC decoders are based on “min-sum” algorithm. LDPC code performs significantly better than BCH or repetition codes in terms error probability for a given SNR (A. Bastug, 2004). Under absence of any attack, watermarking capacity with LDPC code will almost be double than BCH or repetition.

Convolution Codes

Convolution codes are extensively used in digital communication because of their simplicity and better performance. Convolution codes are much better than BCH block codes for similar code rates. They will attain mode strength when used soft decision viterbi decoding which is a type of ML decoding structure for AWGN channel.

The convolution code encoder can be described as a Finite State Machine (FSM). The state of the encoder is defined by the content of the shift registers. The output symbols o is defined by the present p input symbols and by the encoder current state. This kind of device is known as FSM. It is also convenient to describe the operation of state machine through the state diagram which is

a directed graph. The nodes represent the possible states and branch is allowed transition between the nodes. Another form of convolutional code representation is tree diagram. It represents the encoding process as a tree with branches corresponding to the transition of encoder. If all parts of the tree diagrams are merged where the encoder takes the same state at the same time and so number of nodes at any time is no more than number of states is called the trellis diagram.

With the help of trellis diagram one can define the important measure of performance “Free distance”. The free distance can be defined as

$$d_{\text{free}} = d(C) = \min_{C \neq C'} d(C, C')$$

where C and C' corresponds to information sequence I and I' . The error correcting codes can be given by the equation

$$t = \left\lfloor (d_{\text{free}} - 1) / 2 \right\rfloor,$$

where t is the maximum number of errors that a code is capable of correcting.

The **viterbi algorithm** is one of the best decoding algorithms for the convolutional code. Viterbi decoder is the maximum likelihood sequence detection algorithm. The complexity of viterbi algorithm does not depend on the exponentially on the number of symbols in the code sequence. It also assumes channel to be memoryless and thus noise affects each transmitted symbol independently. Viterbi algorithms can be implemented with the hard and soft decision. The viterbi algorithm is also based on the principle of optimality i.e. if any two paths in the trellis merge to same state than one of them can be discarded. The soft decision viterbi algorithm exploits the additional information which is provided by the soft decision demodulator which allows improvement in the performance. The hamming distance is not used as a metric and is defined by the channel.

A more commonly used ECC in watermarking now a day is the **turbo codes** (P. Loo, 2003; F. Balado, 2001). They are systematic recursive convolutional codes using two or more coders connected in parallel. Turbo codes can achieve gain close to the Shannon limit and thus finds an application in the area with very low SNR. Output BER of the turbo codes has a very stiff slope when channel SNR is low and longer is the length of the code better is the gradient of this slope.

CURRENT ART OF CHANNEL CODING WITH PERSPECTIVE TO WATERMARKING

Let us now look at the existing literature of the watermarking domain and try to figure out usage of the codes to handle multiple watermarking problems like copyright protection, image tampering and authentication, active steganography.

Robustness and Copyright Protection

When the SNR is extremely poor, performance in terms of **robustness** will be poor for the blind and uninformed detectors. This is due to the fact the original content is treated as a source of noise by the detector with unknown statistics. The power of this “noise” is much higher than the power of watermark. Introduction of redundancy is the key factor responsible for improving the robustness of watermarking technique. Robustness also improves with length of the codes and size of image. However there is an upper limit on this improvement and it is restricted by the size of a digital content. A channel encoder essentially transforms these symbols in such a manner that distance between the two increases. Placing the symbol far apart will increase noise immunity as probability of false interpretation by decoder will reduce.

Kaushal (2004) has shown a remarkable improvement in capacity with high robustness using ECC. Application of error control codes has also been shown to detect the tampering and localization in same publication. This allows the algorithm to be used for forensic and medical applications. Kaushal (2003) used a local adaptation criteria in embedding and used a concept of “erasure” for the solving the problem of bit embedding which fails local criteria. They used very long code words to achieve good correction capability. They used a Repeat Accumulate (RA) code with turbo code like properties. It involves the folding, interleaving and repetition. The code stream is hidden in the coefficient such that the code symbol is erased at the encoder if it fails embedding criteria. The threshold criteria are shared with the decoder which is used to find the erasure. There is also loss due to synchronization in the data due to false positives and false negative which are inserted due to intentional or unintentional manipulations. The coding frame work can also be used to tackle this issue. The coding is proposed over the entire marking space. In one proposed scheme RS code which is an MDS code used to handle the issue of erasure and in another turbo like code is used which operates close to the Shannon limit.

M.C.Davey (2001) has introduced a new block code that can take care of the false positives, false negatives and substitution error. The external LDPC codes are used with the non linear inner codes over a non binary field. The inner code is used to provide the soft probabilistic decoded output to the outer code.

Jaejin (2000) used an error control coding to generate the watermark. This can help in the error recovery as well as detect and correct the possible changes in the watermark. They used RS code for generation of code word parities which was used as a watermark. The extracted parities are used to check whether the watermark has undergone certain changes or not. This can be used for the authentication purpose. If the changes are beyond

certain distortion threshold than the content can simply be rejected. This is done as the integrity of the content is at stake and it is believed to be lost.

T.S.Das (2007) has used the concept of joint source and channel coding for Spread Spectrum (SS) watermarking problem. The demodulated signal will have a very high BER and thus a substantial number of errors. The error coding mechanism will compensate for the poor estimation of the decoded signal. The entire ECC mechanism can be simulated at the encoder thus helping in selection of proper resources. The authors have used a convolutional code with viterbi decoding. The minimum hamming distance and redundancy of the codes are the important design parameters.

Image Tampering and Content Authentication

The proposed coding frame work (Kaushal 2004; Kaushal 2007) can also be used to solve the problem of tamper localization. **Tampering** is the local replacement of data. Tampering can be both local and global phenomenon. The code rate has to be lowered enough to tackle the problem of loss of data due to the tampering. One anticipates this kind of loss and designs the code rate and shares this criterion between encoder and decoder. The area of error correction indicates the region where most of the removal or tampering of data would have taken place. At the decoder once the decoded bit stream is available, use the same parameter to generate the encoded bit stream. The location of the corruption can be found by comparison with the original encoded bit stream. Most of the errors would be located in the positions where image has been tampered with. It is potentially a medical imaging and forensic science application.

Active Steganography

In **active steganography** it is perceived that the warden is active and will maliciously tries to manipulate the secretly embedded data. Kaushal

(2007) has proposed a coding framework which will cover the loss due to the JPEG compression and helps in revival of the secret message. Also this frame work allows the author to avoid the perceptual distortion and the adaptive embedding. The encoder will not embed in the coefficients which will quantize to zero. Authors have used an RA code frame work which allows them to have:

1. Secretly embedded data is recovered without any error.
2. The encoder algorithm is adaptive in choosing the embedding coefficients thus improving the overall quality of secret image by reducing the perceptual distortion.
3. The coding frame work provides protection against many types of manipulation which is not possible in the naïve or passive steganography. It is believed in the passive steganography that the warden is passive and just observes the secret communication among the concern party.

To summarize the Table 2 relates codes, their properties and their usefulness for application to watermarking problems.

Design Criteria for Codes in Watermarking Applications

Looking at the above properties some of the important design criteria for watermarking using ECC could be:

- For forensic applications lower code rates can be selected beforehand.
- Code words are to be arranged in an image in such a manner that certain code symbols of a code word lies in the centre of image.
- Depending on the robustness level the code rate can be adjusted.
- Code rate can be made adaptive and depending on the channel conditions they can be changed which may allow one to

Table 2. Relating codes, their properties and intended application

Type of code	Useful properties	Intended Application
Turbo like codes Repeat Accumulate /Low Density Parity Codes	<ul style="list-style-type: none"> Simplicity / Operation close to Shannon's limit/Near capacity performance. Can overcome the synchronization error. Soft decoding using viterbi or sum product algorithm is possible. These codes require some overhead to process the erasures error. Turbo like codes can be mapped to channel very well like AWGN channel. 	<ul style="list-style-type: none"> Copyright protection. Fragile watermarking. Active steganography. Robustness against many attacks. Is useful for tamper detection as well.
Maximum distance separable codes like RS codes	<ul style="list-style-type: none"> “Erasures” at the source can be tackled without any penalty. It resolves $(n-k)$ erasures and $(n-k)/2$ errors. It is not well matched to AWGN channel. 	<ul style="list-style-type: none"> Copyright protection. Fragile watermarking. Erasure errors can be eliminated. Insertions and deletion can be tackled. Useful for tamper detection and burst error detection.
Prefix codes	<ul style="list-style-type: none"> No valid code word can prefix the other valid code word. A synchronization marker sequence is inserted at periodic interval. It is searched for and symbols are inserted or deleted to regain synchronization. 	<ul style="list-style-type: none"> Fragile watermarking. Can recover from synchronization error. Insertion deletion recovery is not possible. Some prefix code can correct the substitution error.

use more bandwidth in terms of sending more number of bits (Payload).

design of complementary error correcting codes in concatenation.

The salient features of the method are as follows:

- QIM helps in developing a high capacity data hiding technique. Such data hiding application needs optimization for carrying a large amount of data along with good robustness.
- Robustness of the technique is achieved by implementing a double layered error control coding. The usage of single code for error control will not be effective against large set of “attacks”. Hence, a classical coding theory approach is taken in which RS code acts as outer code, following an inner code like convolution codes. This improves the bit error rate resulting into better robustness. In the applications mentioned above, it is very important to maintain perceptual quality of the host due to data embedding.

PRACTICAL IMPLEMENTATION OF WATERMARKING SCHEME

Having looked at various channel codes let us look at the practical implementation of watermarking scheme using channel coding. It has been proposed to implement quantization index modulation (QIM) based data hiding technique using image dependent quantizers for adaptation and double layered error control coding for robustness improvement. Some applications require embedding relatively large volume of data. Annotation of images in the fields of medicine, biology, geography, and geology is another application where one must hide large number of bits with robustness against a variety of compression attacks. It is also desirable to have robustness against attacks such as compression, additive noise and cropping. The observation that error correcting codes individually will not justify their usage fully led to the

Figure 2. Channel code encoding process

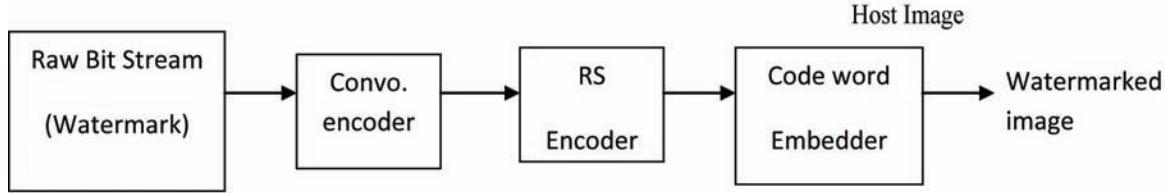
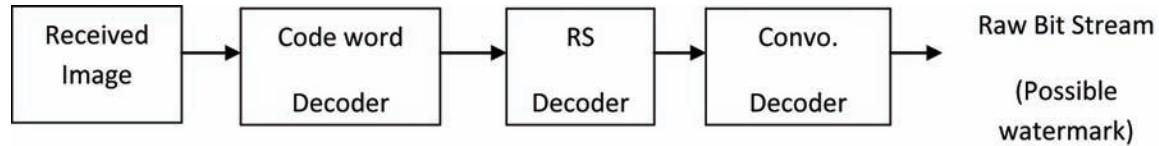


Figure 3. Channel code decoding process



Block diagrams of approach towards coding and method, watermarking embedding and decoding algorithm, results and observations are discussed in the next few sections. It would be followed by the conclusion and open issues related to the application of channel coding in the area of watermarking.

Coding for Error Control

The method for encoding is shown in Figure 2. Figure 3 shows decoding process.

The raw bit stream (watermark bits) consisting of ones and zeros is to be guarded against the attacks. Bit stream to be hidden is coded using a low rate code. The raw bit stream is passed to convolution encoder and then its output is fed to RS encoder. Code word generated is then embedded into image using QIM. Convolution code is used as an inner code because of their simplicity and near capacity performance.

RS code is the maximum distance separable code. It does not incur any penalty for erasures at the encoder. A (n,k) RS code (where n is code word length and k is a number of message bits) can correct a pattern of e erasures and r errors as long as $e+2r < n-k$, which means errors are twice

as costly as erasures.

Watermark Embedding Algorithm

The 8×8 image dependent quantization matrix is derived by modeling the distribution followed by the middle frequency band coefficients of an image. The parameters like mean and variance of this distribution is estimated. An 8×8 image dependent quantization matrix is derived. The matrix derived will be unique for the image under consideration and thus helps to improve the security. The algorithm for Error control in 512×512 image and watermark embedding is as follows:

- Partition image in 4096 ($512/8 \times 512/8$) 8×8 non overlapping blocks.
- Use 14 coefficients per block to give the maximum hiding capacity of $14 \times 4096 = 57,344$ bits in an image.
- Choose a convolution code with code rate of $1/7$ to provide large redundancy.
- Code the raw bit stream of 5000 randomly generated bits using a $1/7$ Turbo code. This will generate 35000 bits long code word.

- Pass the convolution encoded code word to (35, 21) RS encoder resulting in 57344 bits.
- Hide encoded bit stream using QIM implementation.
- Derive the image dependent quantization matrix.
- Compute forward DCT and extract 8x8 blocks.
- Compute energy for each block (excluding zero frequency components). Only the blocks whose energy exceeds a predefined threshold are used for embedding.
- Divide these blocks by the derived quantization matrix.
- Out of 14 middle frequency coefficients select only those which do not quantize to zero.
- Use scalar QIM to embed an encoded bit-stream into the sequence of selected coefficients. The quantizer step size for each coefficient is determined from the derived quantization matrix.
- Transform the modified coefficients back to the image domain using the inverse 2-D block DCT.
- Use soft Viterbi algorithm for convolution decoder. Its output will be original message bits.

Watermark Extraction Algorithm

- Compute forward DCT and extract 8x8 blocks.
- Compute energy for each block. Select the block if energy exceeds the predefined threshold. (Criteria shared with embedder).
- Divide extracted 8 x 8 blocks by derived quantization matrix.
- Set the hidden bit to ‘0’ if DCT coefficient in a selected block is even, else if coefficient is odd, than the hidden bit is ‘1’.
- Pass the detected bit stream to the outer RS decoder.
- Feed the stream to inner convolution decoder.

Results

The watermarked image is subjected to following attacks:

- JPEG attacks
- Gaussian noise addition with zero mean and variance of 0.01.
- Image tampering (part of cameraman image is replaced by lena).
- Rotation of cover image by -45° and cropping.
- Low pass filtering with block size of 10 x 10
- Wiener filtering with block size of 5 x 5.

The result of experimentation is shown in Figure 4. Table 3 indicates variation of performance parameters CR, SNR and PSNR against Q for Lena. The performance parameters are defined as follows.

Root Mean Square Error: It is measured as the average of square of error introduce.

$$RMSE =$$

$$\left(\frac{1}{MN} \sum_{r=0}^{M-1} \sum_{c=0}^{N-1} \{f(r, c) - f'(r, c)\}^2 \right)^{0.5}$$

Signal to Noise Ratio: It is a ratio of signal power to noise power.

$$SNR =$$

$$10 \log \left(\sum_{r=0}^{M-1} \sum_{c=0}^{N-1} \{f^2(r, c)\} / \sum_{r=0}^{M-1} \sum_{c=0}^{N-1} \{f(r, c) - f'(r, c)\}^2 \right)$$

Peak Signal to Noise Ratio: It is a ratio of maximum signal power to noise power.

$$PSNR = 20 \log (2^n - 1 / RMSE)$$

Figure 4. Various attacks on an image

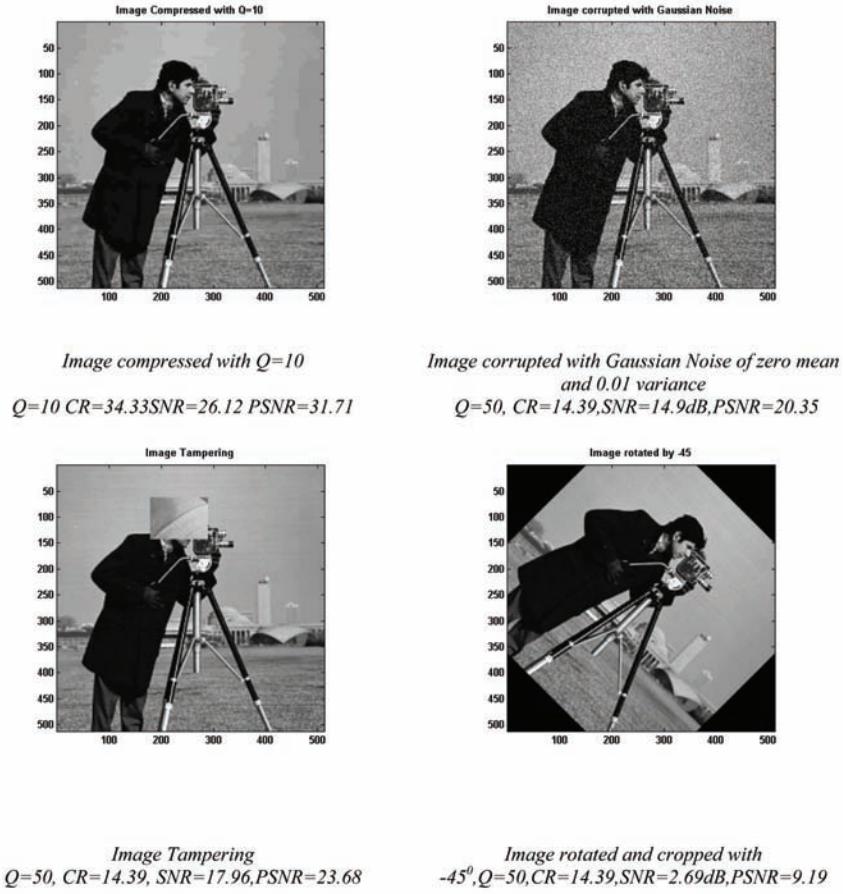


Table 3. Variation of performance parameter with Q for Cameraman

Q	Compression Ratio (CR)	SNR (dB)	PSNR (dB)
10	34.33	26.12	31.71
20	23.93	29.50	35.10
40	16.51	32.54	38.13
50	14.39	33.55	39.14
70	10.59	35.76	41.36
80	8.43	37.53	43.12
90	5.74	40.85	46.45
100	2.32	52.71	58.31

For gray scale image $n = 8$. $PSNR = 20 \log(255 / RMSE)$

Compression Ratio: It indicate the amount of compression in data.

$CR = \text{original image size} / \text{compressed image size}$

Where $M \times N$ is size of the image. $f(r;c)$ and $f'(r;c)$ denotes row element “r” and column element “c” of original and watermarked image.

Observations

- To improve upon adaptability of data hiding technique and security, a unique quantization matrix from the statistical parameter

- of the cover image is derived. This matrix is used as a quantization matrix for QIM scheme.
- Robustness of the technique is achieved by implementing a double-layered error control coding.
 - The method has become robust to various different types of attacks due to error control.
 - Watermark survives JPEG compression. All 5000 bits were recovered with value of Q=10. The PSNR is also extremely low (31.71 dB)
 - SNR and PSNR improve with increase in value of Q. The maximum value for SNR is 52.71 dB.
 - All 5000 bits are recovered even when cover image is subjected to high intensity Gaussian noise.
 - The method is capable of recovering from the tampering attack even though SNR and PSNR values are low (17 and 23 dB respectively)
 - The method is robust to high degree of rotation and cropping. All 5000 bits were recovered with -45 degree of rotation of watermarked image even with poor SNR and PSNR.

FUTURE RESEARCH DIRECTIONS

Application of channel coding to the domain of watermarking has opened up many new possibilities. Channel coding has shown applicability domain of watermarking. Codes with different properties are explored for each of use. However author feels that following are the areas where challenging work can be carried out in this domain:

1. Better modeling and statistical analysis of channel codes applied to watermarking techniques / scenarios/ applications.

2. Studying and modeling various transforms properties for better design of detector / decoder.
3. Benchmarking of channel codes with respect to watermarking applications.
4. Better strategies for Joint source and channel coding, and its modeling with respect to watermarking application.
5. Channel adaptive coding schemes.

CONCLUSION

Error correcting coding increases the code separation in the alphabet for the multi-symbol codes. The main features governing performance are minimum distance and redundancy introduced by the codes. Due to this not all the sequences in the alphabet will be used in the coding process. This will increase the hamming distance between the code words and thus the noise immunity will also improve. The performance will tend towards the random code. Turbo like codes (LDPC, RA) has found an extensive application among the various watermarking scenarios. This is due to the various advantages they have over other types of codes. One of the important factor the channel coding affects is the capacity of the watermarking scheme. It becomes a restrictive feature in the case when a very high capacity is desirable and nearly complete capacity is to be utilized for embedding like in naïve steganography application. Thus a coding scheme which is adaptive to the channel condition is also desirable thus depending on the channel condition the code rate can be varied relieving the burden on the capacity. But in general it can be observed that the channel coding provides far more advantages to the various watermarking application scenarios than its disadvantages.

REFERENCES

- Balado, F., Pérez-González, F., & Scalise, S. (2001). Turbo coding for sample-level watermarking in the DCT domain. In *Proceedings of IEEE Int. Conf. on Image Processing*, Thessaloniki, Greece (pp. 1003-1006).
- Barni, M., Bartolini, F., & Piva, A. (1998). Copyright protection of digital images by means of frequency domain watermarking. *Proceedings of the Society for Photo-Instrumentation Engineers*, 3456, 25–35.
- Bastug, A., & Sankur, B. (2004). Improving the payload of watermarking channels via LDPC coding. *IEEE Signal Processing Letters*, 11(2), 90–92. doi:10.1109/LSP.2003.819350
- Baudry, S., Delaigle, J.-F., Sankur, B., Macq, B., & Maitre, H. (2001). Analyses of error correction strategies for typical communication channels in watermarking. *Signal Processing*, 81, 1239–1250. doi:10.1016/S0165-1684(01)00041-X
- Chou, J., Pradhan, S. S., & Ramchandran, K. (1999). On the duality between the distributed source coding and data hiding. In 33rd Asilomar conference on Signals, Systems and Computers, 2, 1503-1507.
- Clarke, R. J. (1985). *Transform Coding of Images*. New York: Academic Press.
- Cox, I., Miller, M., & Bloom, J. (2008). Digital Watermarking and steganography 2/e Burlington M.A: Morgan Kaufmann.
- Das, T. S., Mankar, V. H., & Sarkar, S. K. (2007). Performance evaluation of spread spectrum watermarking using error control coding [Dr. M G R University, Chennai, Tamilnadu, India.]. *IET-UK ITCES, 2007*, 708–710.
- Davey, M. C., & Mackay, D. J. C. (2001). Reliable communication over channels with insertions, deletions, and substitutions. *IEEE Transactions on Information Theory*, 47(2), 687–698. doi:10.1109/18.910582
- Hernandez, J. R., Amado, M., & Perez Gonzalez, F. (2000). DCT domain watermarking techniques for still images: Detector performance analysis and a new structure. *IEEE Transactions on Image Processing*, 9(1), 55–68. doi:10.1109/83.817598
- Hernandez, J. R., & Perez Gonzalez, F. (1999). Statistical analysis of watermarking schemes for copyright protection of images. *Proceedings of the IEEE*, 87(7), 1142–1146. doi:10.1109/5.771069
- Hernández, J. R., Delaigle, J.-F., & Macq, B. (2000). *Improving data hiding by using convolutional codes and soft-decision decoding*. SPIE(pp. 24–48). San Jose, CA: Security and Watermarking of Multimedia Contents II.
- Lee, J., & Won, C. S. (2000). A watermarking sequence using parities of error control coding for image authentication and correction. *IEEE Transactions on Consumer Electronics*, 46(2), 313–317. doi:10.1109/30.846663
- Loo, P., & Kingsbury, N. (2003). Watermark detection based on the properties of error control codes. *IEE Proceedings. Vision Image and Signal Processing*, 150(2), 115–121. doi:10.1049/ip-vis:20030167
- Solanki, K., Jacobsen, N., Madhow, U., Manjunath, B. S., & Chandrasekaran, S. (2004). Robust image-adaptive data hiding using erasure and error correction. *IEEE Transactions on Image Processing*, 13(12), 1627–1639. doi:10.1109/TIP.2004.837557
- Solanki, K., Sarkar, A. & Manjunath, B. S. (2007). YASS: yet another steganographic scheme that resists blind steganalysis. In *9th International Workshop on Information Hiding*, Saint Malo, Brittany, France.
- Zeng, W. (2006). *Multimedia security technologies for digital rights management*. Academic press. Elsevier.

ADDITIONAL READING

- Chen, B., & Wornell, G. W. (2001). Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, 47(4), 1423–1443. doi:10.1109/18.923725
- Cox, I., Kilian, J., Leighton, T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673–1687. doi:10.1109/83.650120
- Cox, I. J., Miller, M. J., & McKellips, A. L. (1998). Watermarking as communications with side information. *Proceedings of the IEEE*, 87(7), 1127–1141. doi:10.1109/5.771068
- Eggers, J. J., Bumbl, R., Tzschooppe, R., & Girod, B. (2003). Scalar Costa scheme for information embedding. *IEEE Transactions on Signal Processing*, 51(4), 1003–1019. doi:10.1109/TSP.2003.809366
- Ghouti, L. Bouridane, A. Ibrahim, & M.K. Boussakta. (2006). Digital image watermarking using balanced multiwavelets. *IEEE Transactions on Signal Processing*, 54(4), 1519–1536. doi:10.1109/TSP.2006.870624
- Herley, C. (2002). Why watermarking is nonsense? *IEEE Signal Processing Magazine*, 19(5), 10–11. doi:10.1109/MSP.2002.1028346
- Inoue, H., Miyazaki, A., Yamamoto, A., & Katsura, T. (1999). A digital watermark based on the wavelet transform and its robustness on image compression and transformation. *IEICE Transaction Fundamentals of Electronics, Communication, Computer Science. E (Norwalk, Conn.)*, 82-A, 2–10.
- Langelaar, G. C., & Lagendijk, R. L. (2001). Optimal differential energy watermarking of DCT encoded images and video. *IEEE Transactions on Image Processing*, 10(1), 148–158. doi:10.1109/83.892451
- Lin, C. Y., Wu, M., Bloom, J. A., Cox, I. J., Miller, M. L., & Lui, Y. M. (2001). Rotation, scale and translation resilient watermarking for images. *IEEE Transactions on Image Processing*, 10(5), 767–782. doi:10.1109/83.918569
- Lu, C.-S., & Liao, H.-Y. M. (2001). Multipurpose watermarking for image authentication and protection. *IEEE Transactions on Image Processing*, 10(10), 1579–1592. doi:10.1109/83.951542
- Mahalingam Ramkumar & Ali.N Akansu. (2001). Capacity estimates for data hiding in compressed images. *IEEE Transactions on Image Processing*, 10(8), 1252–1263. doi:10.1109/83.935040
- Malvar, H. S., & Florencio, D. A. F. (2003). Improved spread spectrum, a new modulation technique for robust watermarking. *IEEE Transactions on Signal Processing*, 51(4), 898–905. doi:10.1109/TSP.2003.809385
- Miller, M. L., Doerr, G. J., & Cox, I. J. (2004). Applying informed coding and embedding to design a robust high-capacity watermark. *IEEE Transactions on Image Processing*, 13(6), 792–807. doi:10.1109/TIP.2003.821551
- Moulin, P. (2003). Comments on why watermarking is nonsense. *IEEE Signal Processing Magazine*, 20(6), 57–59. doi:10.1109/MSP.2003.1253555
- Moulin, P. R. Koetter (2005). Data-hiding codes. *Proceedings of the IEEE*. 93(12). 2083-2126.
- D. Mukherjee, J. J. Chae, S. K. Mitra, B. S. Manjunath(2000). A source and channel- coding framework for vector-based data hiding in video. *IEEE Transaction on Circuits and systems for video technology*, 10(4), 630-645.
- Petitcolas, F. A. P. R. J. Anderson. & M. G. Kuhn (1999). Information hiding a survey. *Proceedings of the IEEE. special issue on identification and protection of multimedia information*. 87(7). 1062 -1078.

- Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, 27, 623–656.
- Shannon, C. E. (1958). Channels with side information at the transmitter. *IBM Journal of Research and Development*, 2, 289–293. doi:10.1147/rd.24.0289
- Solachidis, V., & Pitas, I. (2001). Circularly symmetric watermark embedding in 2-D DFT domain. *IEEE Transactions on Image Processing*, 10(11), 1741–1753. doi:10.1109/83.967401
- Swanson, M. D., Kobayashi, M., & Tewfik, A. H. (1998). Multimedia data-embedding and watermarking technologies. *Proceedings of the IEEE*, 86(3), 1064–1087. doi:10.1109/5.687830
- Wang, Y., Doherty, J. F., & Van Dyck, R. E. (2002). A wavelet-based watermarking algorithm for ownership verification of digital images. *IEEE Transactions on Image Processing*, 11(2), 77–88. doi:10.1109/83.982816
- Watson, A. B. (1993). DCT quantization matrices visually optimized for individual images. *Proceedings of the Society for Photo-Instrumentation Engineers*, 1913, 202–216.
- Wolfgang, R. B. C. I. Podilchuk, & E. J. Delp (1999). Perceptual watermarks for digital images and video. *Proceedings of the IEEE: Special issue on Identification and Protection of Multimedia Information*, 87(7), 1108-1126.
- Wu, M., & Liu, B. (2003). Data hiding in images and video, Part I – fundamental issues and solutions. *IEEE Transactions on Image Processing*, 12(6), 685–695. doi:10.1109/TIP.2003.810588
- Wu, M., & Liu, B. (2003). Data hiding in images and video, Part II – design and applications. *IEEE Transactions on Image Processing*, 12(6), 696–705. doi:10.1109/TIP.2003.810589
- Yuan, H., & Zhang, X. P. (2006). Multiscale fragile watermarking based on the Gaussian mixture model. *IEEE Transactions on Image Processing*, 15(10), 3189–3200. doi:10.1109/TIP.2006.877310

KEY TERMS AND DEFINITIONS

Active Steganography: It is covert form of communication in which “warden” is believed to be active and may tamper with the secret ongoing communication.

Content Authentication: This fragile form of watermarking is used to check the **integrity** of received digital content and content is discarded if found tampered.

Copyright Protection: Watermarking carries the information about the content owner and it should survive intentional or unintentional manipulation. This will help to prove the copyright of the owner if required.

Data Hiding: This term encompasses the general idea for hiding the data within the digital content. It includes the domain of watermarking, steganography, fragile watermarking, and reversible watermarking.

Error Control Codes: These are codes which are applied in the channel coding phase to recover from the errors that may occur due to super imposition of noise in communication channel.

Image Tampering: If some part of the image is cropped or replaced with some other digital content it is termed as the digital image tampering. This is used to check the integrity of the image at the receiver.

Watermarking: This is the data which is hidden in the digital content with a message that “content is mine”. This is an application which is targeted for ownership verification and copyright protection.

Chapter 17

Hardware Implementations of Image/Video Watermarking Algorithms

Fayez M. Idris
German-Jordanian University, Jordan

ABSTRACT

Digital watermarking is a process in which a secondary pattern or signature, called a watermark, is hidden into a digital media (e.g., image and video) such that it can be detected or extracted later for different intentions. Digital watermarking has many applications including copyright protection, authentication, tamper detection, and embedding of electronic patient records in medical images. Various software implementations of digital watermarking algorithms can be built. While software implementations can address digital watermarking in off-line applications, they cannot meet the requirements of many applications. For example, in consumer electronic devices, a software solution would be very expensive. This has motivated the development of hardware implementations of digital watermarking. In this chapter, the authors present a detailed survey of existing hardware implementations of image and video watermarking algorithms. Fundamental design issues are discussed and special techniques exploited to enhance efficiency are identified. Future outlooks are also presented to address the challenges of hardware architecture design for image and video watermarking.

INTRODUCTION

The proliferation of the World Wide Web and advances in digital technologies have led to the widespread of digital media (text, audio, image, and video). This has allowed the development of new services and business models, which has a profound

effect on our social, political, and economical lives. We have become better connected (any where any time) over recent years. On our desktops, laptops, or personal digital assistants (PDAs), we have the potential of accessing and reaching numerous resources to communicate, do business, learn, or have fun. However, the availability of digital content which can be easily duplicated, manipulated, and widely redistributed has given birth to large-scale

DOI: 10.4018/978-1-61520-903-3.ch017

piracy. Illegal piracy of copyrighted content may cause financial loss and cause many legal issues. Therefore issues such as authentication, tamper detection, and copyright protection are becoming increasingly important. Although many laws and regulations exist for protecting intellectual property, complementary technical measures are needed.

Protection of analogue content has been based on binding the content and its physical medium. Mass reproduction of analogue content is not feasible because it is time-consuming and generates a loss of quality. In comparison to analogue data, manipulation of digital data is simpler and more flexible, reproduction results in perfect copies and mass distribution is very feasible. A non-experienced user, for example, can make perfect duplicate of digital media and change its content using inexpensive or freely distributed tools and applications. Moreover, digital media can be easily made available to millions of people through boundless distribution systems such as e-mails and the Internet. This may result in infringement of copyrights, where the owners lose control after releasing their copyrighted content for distribution.

Two technological techniques have been used to protect digital content. We note that each technique has a different goal. The first is based on preventing illegal users from accessing the content. A physical blockade may be used to prohibit a user from reading the bits that represent the content. For example, a proprietary format enables the detection of a copied medium and prevents access to the media stored on it. The second is based on cryptography, where digital media is changed into incomprehensible form. Encryption allows accessing the media, but it prevents accessing the meaning of their semantics, a secret key is required to convert the media to intelligible form. However, once the content is decrypted, it is unprotected. In addition, devices must be compliant with certain standards and mechanisms to protect decryption keys are required (Maes, Kalker, Linnartz, Talstra, Depover, & Haitsma, 2000).

Physical blockade and encryption provide good protection as long as the content is in digital form. Once the digital media is converted to analogue in order to play or view it, it can be recorded and digitized. This is known as the “digital hole” and it is a major source of illegal duplication and redistribution (Deskshare, 2005). Digital watermarking is considered a promising technique to solve the “digital hole” problem and the most prominent technologies in forensic Digital Rights Management (DRM) (Böhle, Rader, Weber, & Weber, 2008). Digital watermarking basically consists of hiding a pattern or a message, called the watermark, into digital media in an imperceptible way. A detection algorithm can retrieve the watermark. Unlike the first two methods, in watermarking a general user is allowed to access the content but cannot claim the ownership. A watermark serves many purposes. For example, a watermark could hold the identity of the copyright owner or copy control information.

In digital watermarking algorithms, the computational complexity per pixel is low, but the computations have to be performed at image/video rate (Maes, Kalker, Linnartz, Talstra, Depover, & Haitsma, 2000). The video rates ranges from 352×240 pixels at 30 frames/sec for VCD to 4096×2034 pixels at 30 frames/sec for HDTV (Deskshare, 2005; Wiegand, Sullivan, Bjontegaard, & Luthra, 2003). Hence, digital watermarking algorithms are compute intensive necessitating the use of special purpose architecture for real time implementations. Recently, special purpose architectures that implement image/video watermarking have been reported in the literature. This chapter presents a detailed survey of hardware implementations of image and video watermarking algorithms.

The rest of this chapter is organized as follows. To start with, an overview of image and video watermarking is presented and general requirements for different applications are briefly discussed. Then, the design issues and implementation challenges in image and video watermarking

are discussed with emphasis on computational complexity aspects. This is followed by a classification and detailed survey of the different reported hardware implementations and identifying the exploited techniques to improve efficiency. Future perspectives to address the challenges of hardware architecture design for image and video watermarking are then discussed. Finally, the conclusions are drawn.

BACKGROUND

A watermarking system consists of an embedder and a detector (or extractor). Given a host image or a video frame, \mathbf{H} , and a watermark, \mathbf{W} . The watermarked image, \mathbf{H}^* , is obtained by an embedder function, $E(\mathbf{H}, \mathbf{W}, \mathbf{O})$, where \mathbf{O} represents optional parameters that depends on the algorithm. For example, to enhance the security of the watermark, \mathbf{W} may be encrypted, in this case, a key is required. In addition, \mathbf{W} may be encoded using an error correcting code. The watermark can be visible or invisible. A visible watermark is detectable by a human observer, while an invisible watermark is not. In addition, the watermark can be robust or fragile. A robust watermark is designed to defy premeditated and unpremeditated attacks that cause data loss such as tampering or lossy compression.

The watermark extraction or detection process can be described by a function $D(\mathbf{H}^*, \mathbf{O})$. Note that $D(\cdot)$ produces the watermark (extractor) or it indicates the existence or nonexistence of the watermark (detector). Algorithms that need the original host image/video to extract the watermark are dubbed non-blind techniques, while those that can extract the watermark without the host image/video are called blind algorithms. The design of the decoder depends on the embedded watermark type (Potdar, Han, & Chang, 2005). For example, if the watermark is a pseudo-random sequence, then the detector examines the correlation between

the original watermark, \mathbf{W} , and the extracted watermark, \mathbf{W}' .

Watermarking algorithms can be broadly classified into two main categories: spatial domain algorithms and frequency domain algorithms (Prasad & Koliwad, 2009). In spatial-domain techniques, the watermark is embedded directly into image/video pixels, while in frequency domain techniques; the watermark is inserted into selected transform coefficients. Frequency transform techniques include the Discrete Cosine Transform (DCT), the Discrete Wavelet Transform (DWT), and the Discrete Fourier Transform (DFT). The motivation for using DCT and DWT is mainly because they are employed in image and video compression standards such as MPEG-2 and JPEG2000, while the DFT provides rotation, scaling, and translation invariant. Frequency domain techniques are more robust than spatial domain ones (Potdar, Han, & Chang, 2005).

A large number of watermarking algorithms has been reported in the literature for many applications including copyright protection, copy control, authentication, broadcast monitoring, tamper detection, and embedding of electronics patient record in medical images (Navasd & Sasikumar, 2007) and (Prasad & Koliwad, 2009). Research has mainly focused on how to balance three conflicting requirements: imperceptibility, robustness and capacity (Prasad & Koliwad, 2009). Robustness is the ability to recover the data in spite of intentional and accidental data loss, imperceptibility is the perceptual undetectability of the watermark and capacity is the amount of data that can be embedded. Perceptual models have been exploited to make watermarks less perceptible, evaluation studies (El Areef, Heniedy, & Ouda, 2006) and benchmarks (Kim, Ogunleye, Guitart, & Delp, 2004) have been released to evaluate robustness, channel models have been studied to obtain a theoretical bound for the embedding capacity (Zhanga, Panb, Caoa, Zhenga, & Wu, 2008).

The choice of the algorithm type (visible/invisible, robust/fragile, and/or blind/nonblind) is dictated by the application. For example, invisible fragile watermarks are mainly used in authentication applications, which require the algorithm to reveal any alteration of the media. On the other hand, invisible robust watermarking is used in copyright protection applications, where the proof of ownership is required to be present regardless of common attacks. Typical image and video watermarking applications are listed below.

- **Copyright protection:** this is the very first targeted application of digital watermarking. The purpose is to prevent other parties from claiming ownership by embedding information that identifies the intellectual property holder.
- **Fingerprinting:** to prevent illegal copies, the watermark identifies the buyer of the digital media and helps in tracking the source of illegal copies.
- **Broadcast monitoring:** the watermark is detected by a system that monitors different distribution channels to report when and where the media appear s.
- **Copy control:** the watermark carries information about usage rights and is used to determine whether it is allowed to copy the media or not
- **Labeling:** the watermark is a text (metadata) that describes the contents for storage and retrieval in image/video databases. The metadata could store patient records in medical images
- **Authentication:** the watermark encodes information required to determine whether the digital media is authentic or not.

DESIGN AND IMPLEMENTATION CHALLENGES

The implementation of image and video watermarking systems is not a simple task, and it de-

pends on the targeted application. We recall from the previous section that a good watermarking algorithm has some performance metrics such as imperceptibility, robustness, and capacity. From an implementation point of view, the main issues are the computational complexity of the employed embedding and detection algorithms and the physical size of the embedder and detector used in a system. For example, in broadcast monitoring, embedding and detection must be done in real time, while in copyright protection applications; detection time is not a crucial factor for a practical implementation.

Computational complexity measures the amount of processing required to realize an algorithm. Analyzing the computational complexity is very significant, as it has a direct influence on the architecture design and implementation decisions of the watermarking algorithm. A low complexity algorithm might be implemented on a general purpose processor, while a complex algorithm might need a dedicated hardware to achieve real time performance. We model the total complexity of a watermarking algorithm, C_{total} , by

$$C_{total} = C_{pre} + C_{gen} + C_{emb} + C_{post} \quad (1)$$

Where C_{pre} is the complexity of preprocessing (such as transformation), C_{gen} is the complexity of generating and/or encoding the watermark, C_{emb} is the complexity of embedding the watermark, and C_{post} is the complexity of postprocessing (e.g., inverse transformation). In the development of a watermarking algorithm, not only the number of operations is important; the type of operations also plays an important role (e.g., addition executes faster than multiplication). A category of low complexity algorithms are spatial domain replacement-based algorithms, where the watermark replaces some parts of the host image. For example, the least significant bits of the host image are replaced by the watermark bits (Schyndel, Tirkel, & Osborne, 1994). The complexity, C_{total} , is equal to $C_{emb} = O(N)$ logical operations, where N is

the number of bits in the watermark. The capacity of this algorithm is high; however, it is not robust. In order to improve the quality attributes, more complex algorithms are needed. For example, to improve robustness, the watermark is modulated with the host image (Smith & Comiskey, 1996). In this case the complexity is $O(M)$ addition and multiplication operations, where M is number of pixels in the image to be watermarked. The preprocessing complexity depends on the type of processing, for example, in the frequency domain; watermarking algorithms involve transformation from the spatial domain to the frequency domain (Corvi & Nicchiotti, 1997). In this case, C_{pre} depends on the transform type (DCT, DWT, or other). For example, the calculation of the DCT coefficients of an 8×8 block, requires 192 and 464 multiplications and additions, respectively (Yaqin, Zhilu, Guanghui, & Xuemai, 2002). Watermarking in the frequency domain is more robust than spatial domain and most importantly embedding can be carried out during image or video compression. The embedding complexity might also includes the complexity of locating the best pixel to embed (e.g., activity measure, edge detection), the complexity of finding the scaling parameters, and the complexity of inserting the watermark.

We note that software implementation of any given watermarking algorithm is a straightforward task. To achieve real-time watermarking, several video algorithms have been optimized and implemented on dedicated powerful processor. Strycker et al. (Strycker, et al., 2000) have presented a real time implementation for JAWS (Just Another Watermarking System) video watermarking, for television broadcast monitoring. The implementation of JAWS is performed on a Trimedia TM-1000 VLIW processor with 4 BOPS (billion operations per second) developed by Philips Semiconductors. A fractal based watermarking of image has been reporte by Petitjean et al. (Petitjean, Dugelay, Gabriele, Rey, & Nicolai, 2002). The watermarking code is optimized and ported on an Intel PIII 733 MHz, STMicroelectronics VLIW 250 MHz, and

STMicroelectronics DSP 200 MHZ. The time to watermark a 512×512 image is 0.35, 0.43, and 0.96 seconds on the PIII, VLIW, and DSP processors, respectively. To achieve real time video watermarking a co-processor is designed to perform fractal operations. Echizen et al. (Echizen, Yamada, Fujii, Tezuka, & Yoshiura, 2005) have evaluated watermarking on personal computers. An NTSC video is captured, watermarked, and encoded using MPEG-4 in QVGA, 1 Mbps, 30 fps. Real time performance is achieved for MPEG-4 in QVGA format. Burnton et al. (Brunton & Zhao, 2005) have presented a real-time watermarking implementation on programmable graphics hardware. The implemented algorithm is based on a modified version of the algorithm reported in (Wong, 1998). A 30 frames/sec video sequences of 320×240 and 640×480 pixels are tested on an ATI Radeon 9500 Pro (512 MByte) and NVidia GeForce 6800 (1 GByte), respectively. Watermark insertion time is 1.45 and 2.59 millisecond for the 320×240 and 640×480 sequences, respectively. Kim et al. (Kim, Lee, IM, & Lee, 2008) have implemented spatial watermarking on an Intel P-IV CPU with 3.6 GHz, 2 GB RAM, and ATI X1600 graphics card. The watermarking algorithm is based on a simplified and optimized human visual system (HVS) and dithering to realize robust real time performance. The implementation utilizes the MMX of the P-IV processor. The watermarking time is 0.0107 seconds per HDTV frame (1920×1080 pixels).

Software implementations are very flexible, different algorithms to be executed on the same hardware by only software modifications. However, the penalties of flexibility are additional hardware cost and higher power consumption. In addition, software implementations do not meet the requirements of some applications. For example, a news reporter who is reporting an event to a newspaper or a television station, the watermark should be embedded in the hardware of the used camera rather than sending the image/video to the newspaper/station for watermarking.

Table 1. ASIC and FPGA features and implementation tradeoffs

Technology	Performance	Chip Area	Power Consumption
ASIC	High	Low	Low
FPGA	Medium	High	High

Anything may happen between the location of the event and the newspaper/station.

The application of image and video watermarking in consumer devices, such as digital cameras, video games, and video players, demands real-time performance, low cost, small chip area, low power consumption, and ease of integration with existing products. Dedicated hardware architectures using Application Specific Integrated Circuit (ASIC) and Field Programmable Gate Array (FPGA), are derived by full customization to a specific algorithm. The choice of a particular technology is a trade-off between performance, chip area, and power consumption as shown in Table 1.

HARDWARE IMPLEMENTATIONS OF IMAGE WATERMARKING

We recall from the previous section, that image and video watermarking involves different tasks such as preprocessing and embedding. The design of efficient dedicated hardware implementations for image and video watermarking starts with a comprehensive analysis of the target algorithm. This is followed by the utilization of special computational characteristics desirable for VLSI implementation. These characteristics include linearity, regularity, modularity, and parallelism. Individual tasks are then mapped onto different modules and each module is optimized to achieve high performance, small chip area, and low power consumption.

In order to utilize the desirable computational characteristic, a complete and detailed analysis of the algorithm is carried out. This analysis has two purposes. The first is to calculate the computa-

tional complexity of each task and to capture the contribution of each task to the overall algorithm complexity. This can be achieved by individually analyzing each task as described in the previous section. The second is to understand the computational characteristics of each task. We note that watermarking tasks are low-level tasks involving pixel operations on a limited neighborhood of the current pixel and characterized by regular computations. As a result of this analysis, the algorithm might go under modification to lower the complexity and/or to have one or more of the desirable VLSI characteristics. The algorithm modifications should result in minimum quality degradation in comparison to the quality obtained by the original algorithm.

At the architecture design level, the dataflow of the watermarking algorithm to be implemented is analyzed and the architecture to achieve high performance is developed. There are several approaches to achieve this. The first approach is to take advantage of inherent parallelism present in the algorithm. In this approach, parallel processing elements are used to process more than one set of data concurrently. This approach reduces the execution time at the expense of increasing hardware (chip area). The second approach is to use pipeline architecture. A pipeline is an implementation technique in which multiple computations are overlapped in execution. Here, the computation is divided into stages, where the output of one stage is fed into the next stage. After an initial latency, output is generated for every clock cycle. Another approach is to use integer arithmetic instead of floating point arithmetic. This reduces the hardware complexity; however, this might reduce watermarking quality attributes.

In this section, we present the hardware implementations of image watermarking algorithms. The implementations are classified into two categories: spatial domain (or pixel domain) and frequency domain (or transform domain) implementations. This categorization is based on whether the watermark is embedded in the spatial domain or the frequency domain.

Spatial Domain Implementations

In this watermarking category, the watermark is embedded directly into the image pixels. Taking into account that an image might go under further processing, the implemented algorithms are chosen such that they can resist different levels of compression and filtering techniques. The computational complexity of spatial domain watermarking is low compared to frequency domain. Hence, dedicated architectures can achieve the highest silicon efficiency with minimum hardware overhead and lower power consumption.

Visible Watermarking Implementations

Visible watermarking methods mark a logo or text on the image of interest to indicate the owner of the content. In this section we survey hardware implementations of visible image watermarking.

A VLSI architecture for visible watermarking has been implemented by Mohanty et al. (Mohanty, Ranganathan, & Namballa, A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S²DC) Design, 2005) in the context of secure digital camera. Two visible watermarking algorithms have been implemented. The first implementation is based on the algorithm reported by Braudaway et al. (Braudaway, Magerlein, & Mintzer, 1996). Here, the host image, H , is altered by adding a scaled gray value of the watermark image, W . The scaling is done such that the host

image pixels are altered to a perceptual equal degree according to the following:

$$H^*(i, j) = \begin{cases} H(i, j) + \alpha W(i, j)H(i, j) / 903.3 & H(i, j) \leq 2 \\ H(i, j) + \alpha C_1 W(i, j)H(i, j) / 6.0976 & 2 < H(i, j) \leq 64 \\ H(i, j) + \alpha C_2 W(i, j)H(i, j) / 6.0976 & 64 < H(i, j) \leq 128 \\ H(i, j) + \alpha C_3 W(i, j)H(i, j) / 6.0976 & 128 < H(i, j) \leq 192 \\ H(i, j) + \alpha C_4 W(i, j)H(i, j) / 6.0976 & 192 < H(i, j) \leq 256 \end{cases} \quad (2)$$

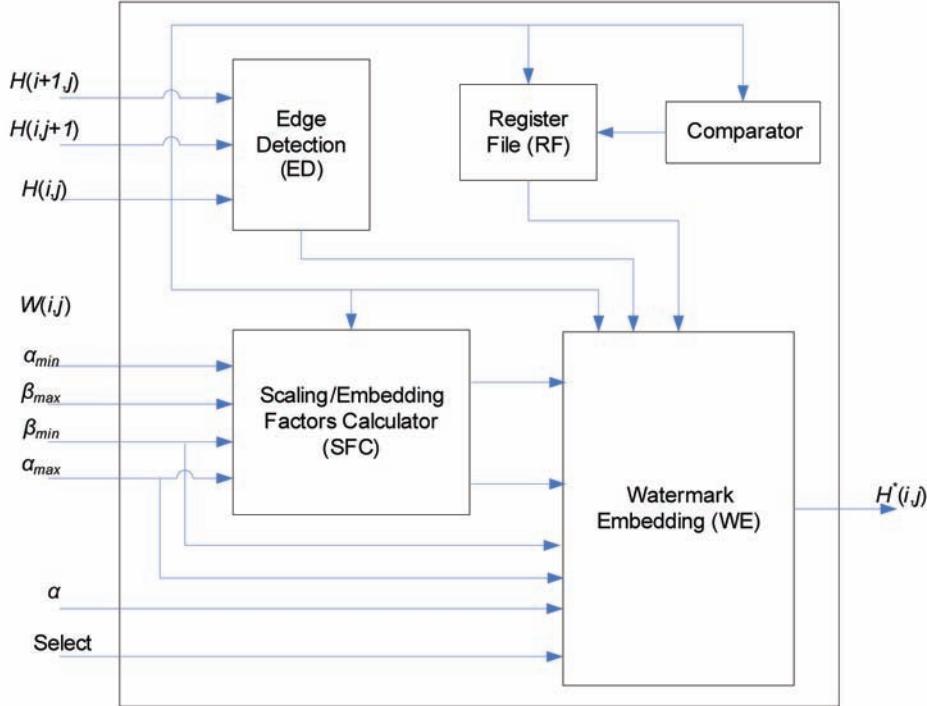
Where α is a scaling factor that controls the strength of the watermark and C_1, C_2, C_3, C_4 are linear regression coefficients. The coefficients are best approximate the cubic root (Mohanty, Ranganathan, & Namballa, A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S²DC) Design, 2005).

The second implementation is based on the watermarking algorithm reported by Mohanty et al. (Mohanty, Ramakrishnan, & Kankanhalli, A Dual Watermarking Technique for Images, 1999). In this implementation, the pixel values of the host image are modified based on local and global statistics. Both the host image and the watermark are partitioned into blocks of equal sizes. The k^{th} watermarked image block, H_k^* , is obtained by altering the k^{th} host image block, H_k , according to the following

$$H_k^*(i, j) = \alpha_k H_k(i, j) + \beta_k W_k(i, j) \quad (3)$$

Where W_k is the k^{th} watermark image block. The scaling factor α_k and the embedding factor β_k of the k^{th} block depend on the mean μ_k and the variance σ_k of the k^{th} host image block, H_k . The factors α_k and β_k are determined based on certain characteristics of the human visual system such that the perceptual quality is not degraded due to the addition of the watermark (Mohanty, Ranganathan, & Namballa, A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S²DC) Design, 2005). To determine α_k and β_k without the need

Figure 1. Block diagram of a visible watermarking architecture



to wait until all pixels are covered to find local statistics of all blocks, α_k and β_k are calculated based on the following local statistics: normalized block mean $\hat{\mu}_k$; normalized block variance $\hat{\sigma}_k$; and normalized host image mean $\hat{\mu}$:

$$\alpha_k = \begin{cases} \alpha_{\max} & \text{edge block} \\ \alpha_{\min} + (\alpha_{\max} - \alpha_{\min}) \frac{1}{\hat{\sigma}_k} \exp(-(\hat{\mu}_k - \hat{\mu})^2) & \text{non-edge block} \end{cases} \quad (4)$$

$$\beta_k = \begin{cases} \beta_{\min} & \text{edge block} \\ \beta_{\min} + (\beta_{\max} - \beta_{\min}) \hat{\sigma}_k (1 - \exp(-(\hat{\mu}_k - \hat{\mu})^2)) & \text{non-edge block} \end{cases} \quad (5)$$

Where α_{\min} and α_{\max} are the minimum and maximum values of α_k , and β_{\min} and β_{\max} are the minimum and maximum values of β_k . This eliminates hardware performance degradation without compromising image quality (Mohanty, Ranganathan, & Namballa, A VLSI Architecture for Visible

Watermarking in a Secure Still Digital Camera (S²DC) Design, 2005).

The architecture is shown in Figure 1. The implementation includes a selection input to select one of the two algorithms. The Select input is used to control which watermarking algorithm is used. The Watermark Embedding (WE) embeds the watermark according to Equations (2) and (3) for the first and second implementations, respectively. The constants 1/903.3, $C_1/6.0976$, $C_2/6.0976$, $C_3/6.0976$, and $C_4/6.0976$ (Equation (2)) are stored in a 5-word register file (RF). The Comparator determines the range of the input pixel such that the corresponding constant is selected from the RF unit. The Edge Detection (ED) module calculates the first order derivative to determine whether a block is an edge block or not. The Scaling/Embedding Factors Calculator (SFC), calculates α_k and β_k using Equations (4) and (5), respectively. The control unit is implemented as a finite state machine with 5 states.

The architecture is implemented using 0.35μ technology and found to operate at 292 MHz and consumes 6.9 mW (3.3 V), the area 3.34 by 2.89 mm². Simulation results are performed using C_1 , C_2 , C_3 , C_4 , α_{min} , α_{max} , β_{min} , β_{max} , and α values of 0.339644, 0.21988, 0.185746, 0.172925, 0.95, 0.98, 0.02, 0.7, and 0.03, respectively and found that both algorithms are comparable in terms of PSNR (Mohanty, Ranganathan, & Namballa, A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S²DC) Design, 2005).

Invisible Watermarking Implementations

While visible watermarking schemes provide means for explicit assertion of ownership with logos, invisible schemes provide hidden protection of these rights. Unlike visible watermarks, the invisible watermarks could not be removed from the media because they became an integral component of the content after being embedded. Invisible watermarks alter the media in a way that they are perceptually unnoticeable. An appropriate detection method is used to detect them. They identify the owner of the digital media. Proof of ownership is another application area for invisible watermarks; however, it needs a higher level security than owner identification. In this section we present a survey of hardware implementations of invisible image watermarking techniques.

Garimella et al. (Garimella, Satyanarayana, Kumar, Murugesh, & Niranjan, 2003) have presented an ASIC implementation of an invisible fragile watermarking in the spatial domain. The implementation is designed for watermarking 8-bit gray level images. The watermark is a text encoded using the ASCII code. To increase security and reduce the dynamic range of the watermark, the text is encrypted using differential pulse code modulation (DPCM). The bit stream of the encrypted text is swapped with the least significant bits (LSBs) of the gray level pixel values in the host image (each 8-bits replace the LSBs of eight consecutive pixels). The watermark can be

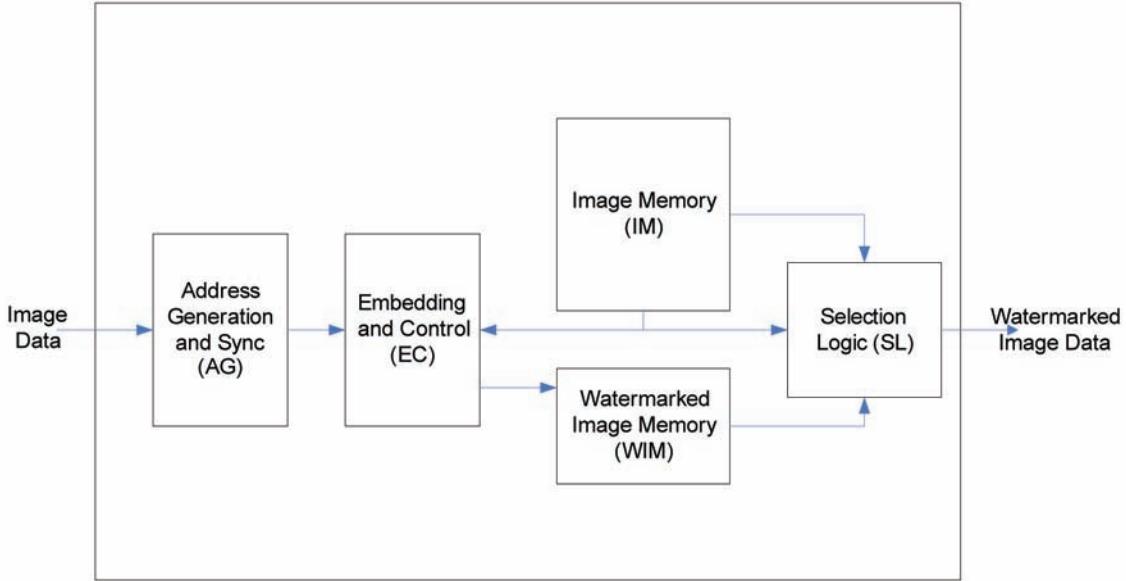
extracted blindly by accumulating the LSBs of the altered pixels, and decrypting the text message.

A block diagram of the architecture is shown in *Figure 2*. The watermark is permanent and is stored in an internal register in the Embedding and Control module (EC). The host image is stored in the Image Memory module (IM). The maximum image size that can be held in the IM module is 200×200 pixels. The 2048 consecutive pixels that are altered by the watermarking process are stored in the Watermarked Image Memory (WIM), which is addressed internally by the lower 11 address bits. The watermark is embedded pixel by pixel. The same external control signals are used for both IM and WIM to minimize the number of external pins. The image is fed pixel by pixel into IM. The EC encodes the stored watermark and embeds it in the first 2048 pixels of the image. The SL module is used to select the output source (from IM or WIM).

The ASIC is implemented using 0.13μ CMOS and it can handle images of size 200×200 pixels and a watermark of size 2 Kbits. The area of the ASIC is $3453 \times 3453 \mu\text{m}^2$ and consumes $37.6 \mu\text{W}$. The advantage of this implementation is that it has very low power consumption. The disadvantages are the maximum image size that can be handled is 200×200 pixels, the use of a fixed watermark, and the pixel-by-pixel operation.

To support online digital watermarking of color images, Garimella et al. (Garimella, Satyanarayana, Murugesh, & Niranjan, 2004) have presented an implementation of a watermarking engine. The watermarking is invisible fragile one, and the watermark is an ASCII text, which is encrypted using DPCM. The host image pixels are converted from 24-bit RGB to 24-bit YUV format. The watermark is embedded in the Y component. Here, the two LSBs of the Y component are used for watermarking. Each watermark bit is swapped with the first LSB of the Y component. The complement of the watermark bit is swapped with the second LSB. Every 8-bit of encrypted text replaces the LSBs of the Y component of 8

Figure 2. Invisible fragile watermarking architecture for gray level images



consecutive host image pixels. The YUV is converted to RGB format. Having two bits for the watermark, where one bit is the complement of the other, enables blind detection without having the original image or the watermark.

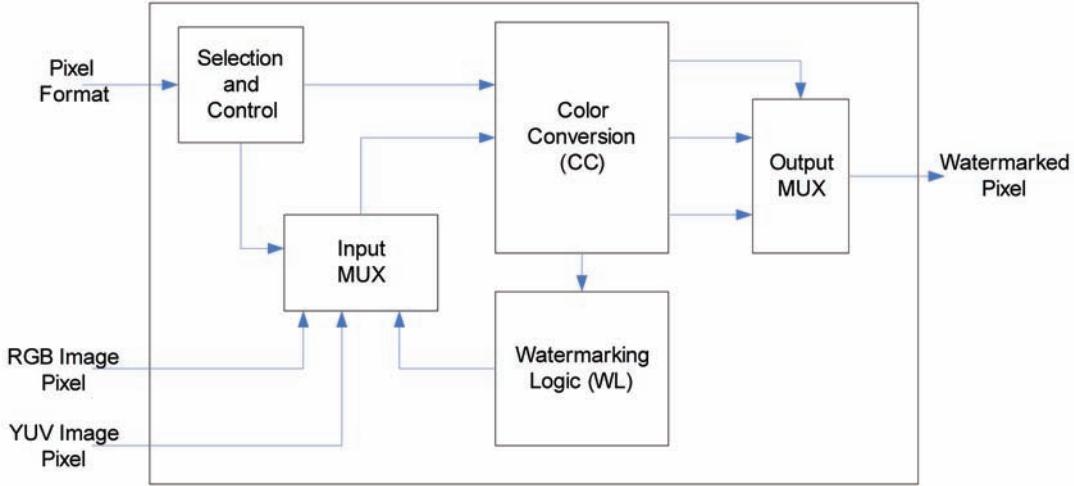
A block diagram of the implemented pixel-wise architecture is shown in *Figure 3*. The Color Conversion module (CC) receives the value of the input pixel in RGB or in YUV format. The CC module converts the RGB format to YUV and sends the value of the Y channel to the Watermarking Logic module (WL). The WL module embeds the watermark in the two LSBs of the Y channel. The CC module converts watermarked YUV to RGB format. The output, Watermarked Pixel, can be in RGB or YUV format. A 3-stage pipeline (multiplication, addition/subtraction, and scaling) is designed to perform color conversion. To reduce the hardware complexity, the same pipeline is used to convert color format from RGB to YUV and from YUV to RGB.

The architecture of the pixel-wise watermarking engine is implemented using 0.13μ CMOS technology. The area of the chip is $545 \times 525 \mu\text{m}^2$.

The operating voltage of the ASIC is 1.2 V, it operates 166.6 MHz, and it consumes 9.2 mW. The implementation can be used as a macro or as a part of a complex chip (Garimella, Satyanarayana, Murugesh, & Niranjan, 2004). The disadvantage of this implementation is the use of a fixed size permanent watermark and the pixel-by-pixel operation.

With the objective to develop low power, real time, reliable and secure watermarking systems, Mohanty et al. (Mohanty, Kumara, & Nayak, FPGA Based Implementation of an Invisible-Robust ImageWatermarking Encoder, 2004) have presented an FPGA implementation of the algorithm reported in (Tefas & Pitas, 2001). The algorithm is an invisible-robust spatial domain watermarking of gray level images. The watermark image $W(i, j)$ is a ternary image having {0, 1, or 2} pixel values which is generated by a pseudo-random sequence generator using a digital key. The watermark embedding process is carried out by altering the pixels of the host image, $H(i, j)$, according to the following equation:

Figure 3. Block diagram of pixel-wise watermarking of color images



$$H^*(i, j) = \begin{cases} H(i, j) & \text{if } W(i, j) = 0 \\ G_1(H(i, j), H_N(i, j)) & \text{if } W(i, j) = 1 \\ G_2(H(i, j), H_N(i, j)) & \text{if } W(i, j) = 2 \end{cases} \quad (6)$$

Where $H_N(i, j)$ denotes a function that depends on the neighborhood of (i, j) and the embedding functions, G_1 and G_2 , are suitably designed functions based on $H(i, j)$ and $H_N(i, j)$. The functions G_1 and G_2 are given by

$$\begin{aligned} G_1(H(i, j), H_N(i, j)) &= (1 - \alpha_1)H_N(i, j) + \alpha_1 H(i, j) \\ G_2(H(i, j), H_N(i, j)) &= (1 - \alpha_1)H_N(i, j) + \alpha_2 H(i, j) \end{aligned} \quad (7)$$

Where α_1 and α_2 are scaling factors. The neighborhood image pixel value, $H_N(i, j)$, is the average gray value of neighboring pixels of the host image $H(i, j)$ of radius r . To avoid the use of complex hardware for the division circuitry, the following equation is employed to calculate $H_N(i, j)$:

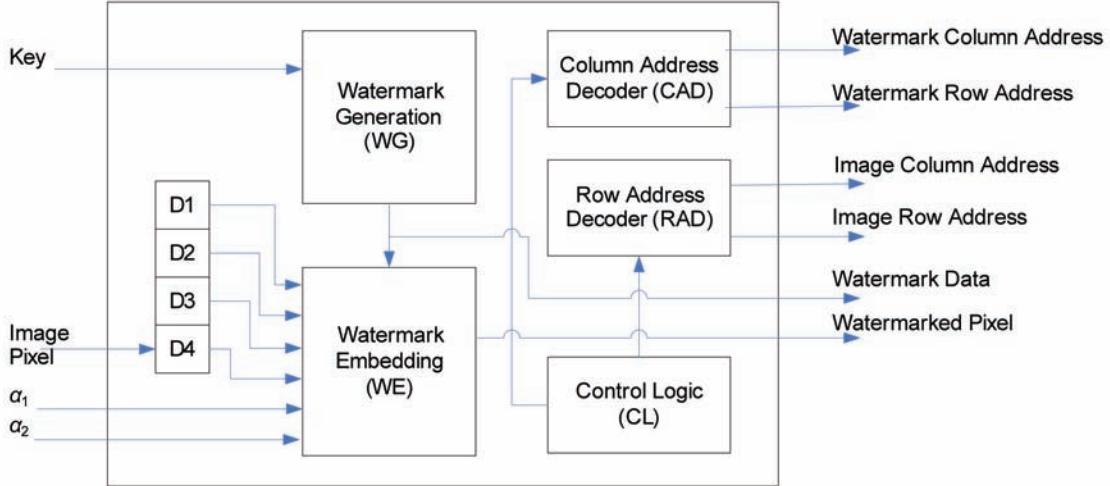
$$H_N(i, j) = 0.5 * (0.5 * (H(i+1, j) + H(i+1, j+1)) + H(i, j+1)) \quad (8)$$

This provides a proper trade-off among accuracy, cost of computation, and hardware cost.

The architecture is shown in Figure 4. The Watermark Generation module (WG) takes the key as an input and generates the watermark using 8-bit linear feedback shift register (LFSR). To reduce the worst case delay, the LFSR is designed to use one-to-many feedback structure to generate the required random sequence values (Mohanty, Kumara, & Nayak, FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder, 2004). The Watermark Embedding module (WE) is designed by mapping the equations that performs the embedding into a sequence of addition and division, multiplication, followed by addition (Equation (8) followed by Equation (7)). A multiplexer is used to implement Equation (6) based on the watermark value. The data, D1, D2, D3, and D4 corresponds to image pixels $H(i, j)$, $H(i+1, j)$, $H(i, j+1)$, and $H(i+1, j+1)$, respectively. The division is implemented by a one bit shift right operation. The Control Logic (CL) is implemented as a finite state machine with 8 states. The address decoders, CAD and RAD, are used to decode the memory address to access two external RAMs to store the host image and the watermark.

The architecture was synthesized using Synplify Pro targeting Xilinx VIRTEX-II technology with

Figure 4. Invisible robust image watermarking architecture



XCV50-BG256-6. VHDL was used to model the implementation. Simulation results have shown that the FPGA can operate at a frequency of 50.4 MHz. The disadvantage here is that processing is performed pixel-by-pixel.

Mohanty et al. (Mohanty, Ranganathan, & Namballa, VLSI Implementation of Invisible Digital Watermarking Algorithms Towards the Development of a Secure JPEG Encoder, 2003) and (Mohanty, Kougianos, & Ranganathan, 2007) have presented an implementation of both invisible robust and invisible fragile watermarking in a single chip. The user can select between the two watermarking algorithms. The watermarks are embedded in the spatial domain but are designed to be robust for JPEG compression (Mohanty, Kougianos, & Ranganathan, VLSI Architecture and Chip for Combined Invisible Robust and Fragile Watermarking, 2007). The watermarking algorithms that were implemented are the invisible robust and the invisible fragile algorithms proposed by Tefas et al. (Tefas & Pitas, 2001) and Mohanty et al. (Mohanty, Ramakrishnan, & Kankanhalli, A Dual Watermarking Technique for Images, 1999), respectively. The invisible robust algorithm was described earlier and it is summarized by Equations (6)-(8). In the invis-

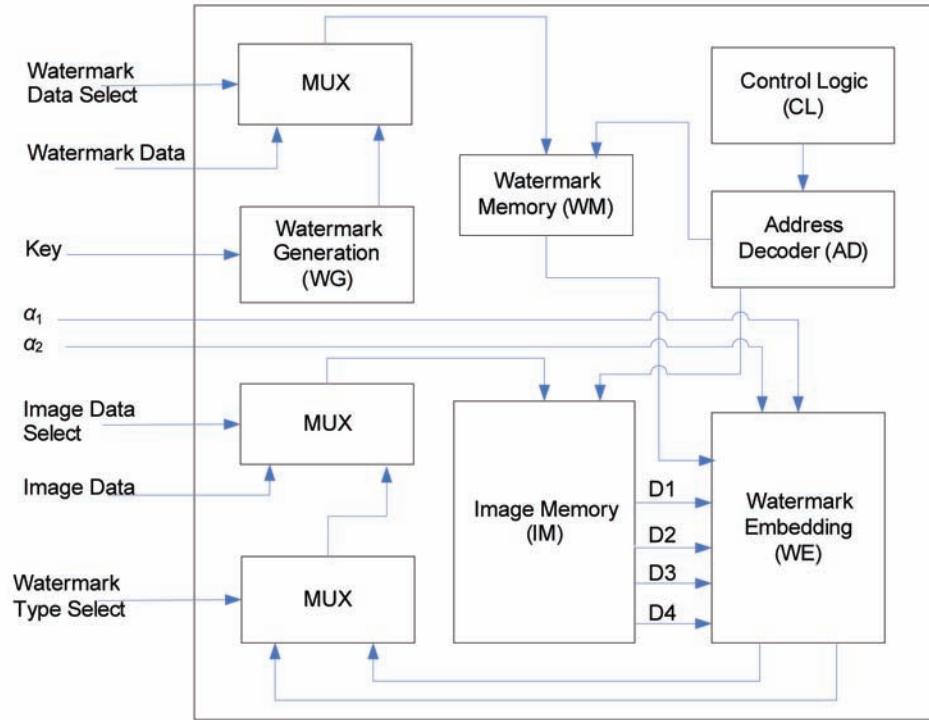
ible fragile watermarking, The watermark image, $W(i,j)$, is a binary image and is generated using a pseudo-random number generator. It is assumed that the watermark image and the host image are of the same size. Bit-plane decomposition is used to decompose the host image (8-bit gray level) is decomposed into 8 binary images $\{H[k], 0 \leq k \leq 7\}$. A bit-plane, k , which is selected to embed the watermark, is modified according to the following:

$$H^*[k](i,j) = H[k](i,j) \oplus W(i,j) \quad (9)$$

An iterative process is required to find the best bit-plane to embed the watermark image such that the PSNR is higher than a predefined threshold. In the proposed implementation, the third bit-plane is selected to eliminate the need for iterations. This results in area-efficient and high-performance hardware (Mohanty, Kougianos, & Ranganathan, VLSI Architecture and Chip for Combined Invisible Robust and Fragile Watermarking, 2007).

A block diagram of the proposed architecture of both invisible robust and invisible fragile is shown in Figure 5. Two static RAM modules, IM and WM, are employed for storing the host image and watermark. The IM is 8-bit 256×256 locations and the WM is 2-bit 128×128 locations.

Figure 5. Block diagram of both invisible robust and invisible fragile watermarking architecture



Using the Watermark Data Select, the watermark can be provided externally or it can be generated using an 8-bit linear feedback shift register (LFSR). The LFSR is designed to use one-to-many feedback structure to reduce the worst-case delay. The Watermark Generation module is designed by mapping the equations that performs the embedding into a sequence of addition, multiplication, addition/subtraction, followed by XOR. The data, D1, D2, D3, and D4 corresponds to image pixels $H(i, j)$, $H(i+1, j)$, $H(i, j+1)$, and $H(i+1, j+1)$, respectively. The controller (CL) is implemented as a finite state machine with 5 states. The watermark type can be selected using the Watermark Type Select input. If the user selects invisible robust watermarking, the invisible fragile part is disabled and vice versa. The fragile and the robust algorithms can be used for authentication and copyright protection applications, respectively.

The implementation is carried out using 0.35μ SCN3M SCMS technology from MOSIS. The

chip area is $15.012 \times 14.225 \text{ mm}^2$ and consumes 2.0547 mW when operating at 3.3 V and 0.545 GHz frequency.

Frequency Domain Implementations

We note that digital images are huge in size and it is expected that images will be compressed in order to reduce transmission and memory requirements. In order to apply spatial domain algorithms, compressed images must be decompressed before embedding a watermark, and recompressed after watermarking. This increases the computational complexity and may degrade the quality of the watermark due to the use of lossy image compression. To eliminate the need for compression/decompression, frequency domain watermarking algorithms embed a watermark in the transform coefficients. In comparison with watermarking in the spatial domain, frequency domain has higher robustness and imperceptibility. Frequency

domain techniques have higher computation complexity than spatial domain techniques; however, they are compatible with international compression standards. In this section, we present a review of implementations of image watermarking algorithms in the frequency domain.

DCT Domain Implementations

The motivation for using DCT is that DCT is employed in image and video compression standards such as JPEG2000 and MPEG-2. Lim et al. (Lim, Park, Kang, & Cho, 2003) have presented an FPGA implementation of a DCT-based invisible semi-fragile watermarking algorithm. The goal is to design an authentication algorithm which is robust against a certain amount of JPEG compression. The implemented algorithm is based on an invariant property of the DCT coefficients quantization and carried out in the context of building a digital camera. Given the DCT coefficients of an 8×8 block, $\{C(i,j), 0 \leq i, j \leq 7\}$, and the quantization matrix, $\{Q(i,j), 0 \leq i, j \leq 7\}$, Lin et al. (Lin & Chang, 2000) have shown that if a DCT coefficient, $C(i,j)$, is modified to an integral multiple of $Q(i,j)$, the DCT coefficient can be reconstructed if $Q(i,j)$ is larger than subsequent quantization steps used later in JPEG compression. The host image is divided into 8×8 non-overlapping blocks and the DCT for each block is obtained. The blocks are quantized using $Q(i,j)$. A secret key is used to a set of pseudo-random numbers. The watermark bits are encrypted by XOR-ing the watermark with the pseudo-random binary numbers. The encrypted watermark bits are then embedded into the least significant bits of the DCT coefficients of the host image in the medium frequency range. The blocks are de-quantized and IDCT (inverse DCT) is applied to obtain the watermarked image, which can be used as an input to JPEG encoder for compression. The captured image is portioned into 8×8 blocks. The color components of a block are converted from RGB to $Y\text{C}_b\text{C}_r$ format. The luminance component, Y , is

used as a host to embed the watermark. The 2-D DCT is implemented separately as a 1-D across the rows of the input block followed by a 1-D DCT along each column. The permutations used in the generation of the pseudo-random numbers are stored in a look up table and a linear feedback shift registers are used to generate the numbers. The architecture is captured using VHDL, simulated using ModelSim tools and synthesized and loaded using an FPGA from the ALTERA Flex family, EPF10K100A. The gate occupation rate is 49%. This low rate is due to the small size of the DCT core, which represent most of the computation in the architecture (Lim, Park, Kang, & Cho, 2003). The A maximum operation frequency of 50 MHz is achieved.

An implementation that can insert visible or invisible watermark in the DCT domain has been reported by Mohanty et al. (Mohanty, Ranganathan, & Balakrishnan, 2006). The invisible and visible water marking are based on the algorithms presented by Cox. et. al. (Cox, Kilian, Leighton, & Shamoon, 1997) and Mohanty et al. (Mohanty, Ramakrishnan, & Kankanhalli, 2000), respectively. The two algorithms are modified for efficient implementation, high performance, and reduction of chip area without degrading image quality (Mohanty, Ranganathan, & Balakrishnan, 2006). In the invisible watermarking algorithm, the host image is partitioned into non-overlapping blocks. The watermark is a randomly generated sequence of 1000 numbers, $\{w_i, 0 \leq i \leq 999\}$, where each element is selected according to a normal distribution of 0 mean and 1 variance. For the k^{th} block, the three largest AC coefficients, $\{H_{DCT,k}^*(m), 0 \leq m \leq 2\}$, are located. Each coefficient is added to the corresponding scaled watermark according to the following

$$H_{DCT,k}^*(m) = H_{DCT,k}(m) + \alpha w_{m+k*3} \quad (10)$$

In the visible watermarking algorithm, the watermark is inserted in the perceptually significant

regions of the image. The watermark is generated using LFSR. The DCT coefficients of the k^{th} watermarked image block, $H_{DCT,k}^*$ is obtained by altering the DCT coefficients of the k^{th} host image block, $H_{DCT,k}$, according to the following

$$H_{DCT,k}^*(i,j) = \alpha_k H_{DCT,k}(i,j) + \beta_k W_{DCT,k}(i,j) \quad (11)$$

Where $W_{DCT,k}$ is the DCT coefficients of k^{th} watermark image block. To determine α_k and β_k without the need to wait until all pixels are covered, α_k and β_k are calculated based on: normalized block mean $\hat{\mu}_{DC,k}$; normalized block variance of AC coefficients $\hat{\sigma}_{AC,k}$; and normalized host image mean $\hat{\mu}$ using the following:

$$\alpha_k = \begin{cases} \alpha_{\max} & \text{edge blocks} \\ \sigma_{AC,k} \exp(-(\hat{\mu}_{DC,k} - \hat{\mu})^2) & \text{non-edge blocks} \end{cases} \quad (12)$$

$$\beta_k = \begin{cases} \beta_{\min} & \text{edge blocks} \\ \frac{1}{\sigma_{AC,k}} (1 - \exp(-(\hat{\mu}_{DC,k} - \hat{\mu})^2)) & \text{non-edge blocks} \end{cases} \quad (13)$$

Where α_{\min} and α_{\max} are the minimum and maximum values of α_k , and β_{\min} and β_{\max} are the minimum and maximum values of β_k . The exponentials are approximated using Taylor series. The factors, α_k and β_k , are scaled. A block is classified as an edge block if the absolute value of the mean of the AC coefficients is larger than the maximum AC coefficient in the block multiplied by a threshold τ , i.e.,

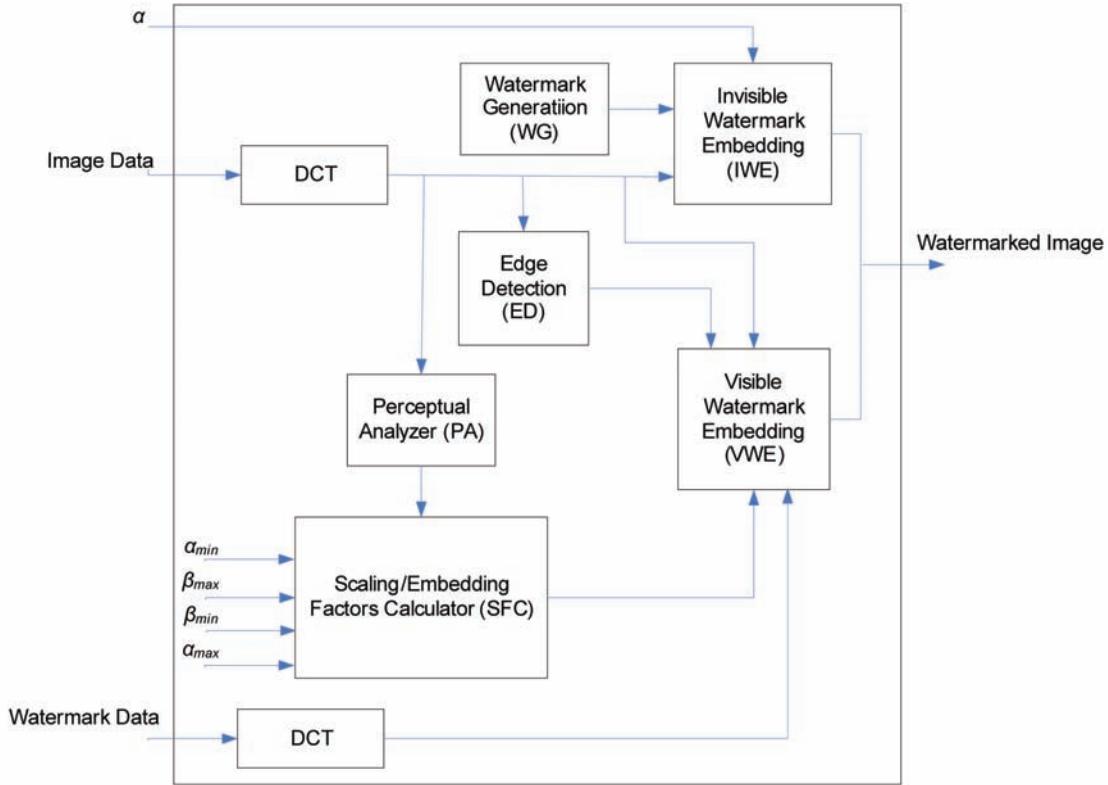
$$|\mu_{AC,k}| > \tau |\mu_{AC,max}| \quad (14)$$

The architecture is shown in *Figure 6*. The DCT module calculates the 2-D DCT transform coefficients for a 4×4 block. The 1-D row DCT is calculated followed by the 1-D column DCT of the block. An LFSR is used to generate the

pseudo-random numbers (Watermark Generation). The Invisible Watermark Embedding module implements Equation (10) to insert the invisible watermark. The Edge Detection module determines whether the block is an edge block or not using Equation (14). The Perceptual Analyzer module calculates $\hat{\mu}_{DC,k}$ and $\hat{\sigma}_{AC,k}$. To calculate the mean, a division by 16 is implemented by a shift-right by 4-bit positions. The Scaling/Embedding Factors Calculator module evaluates the Taylor series approximation of the factors, α_k and β_k as in Equations (12) and (13). The values of the factors, α_k and β_k are scaled based on a fixed range from $(\alpha_{\min}, \alpha_{\max})$ to $(\beta_{\min}, \beta_{\max})$. The Visible Watermark Embedding module implements Equation (11). The implementation employs different design techniques such as dual voltage, dual frequency, clock gating, and pipelining to achieve high operating frequency and low power consumption. To exploit parallelism and improve the overall performance, pipelining is employed. The invisible watermarking is designed as 3-stage pipeline, while the visible watermarking is designed as a 5 stage pipeline. A prototype has been design and verified using 0.25μ technology and 0.3 mW average dynamic power. The estimated dual frequency of the chip was estimated to be 280 MHz and 70 MHz, and at a dual frequency of 1.5 V and 2.5 V.

Another implementation of the algorithm reported by Mohanty et al. (Mohanty, Ramakrishnan, & Kankanhalli, 2000) has been presented by Adamo et al. (Adamo B., Mohanty, Kouglanos, Varanasi, & Cai, 2006) and (Adamo O. B., Mohanty, Kouglanos, & Varanasi, 2006). The secure digital camera is based on embedding two watermarks, an invisible watermark and a visible watermark into an image. The invisible watermark is key-based biometric information (e.g., fingerprint, eye iris). The key is encrypted using the Advanced Encryption Standard (AES) and then is embedded as a visible watermark in the form a barcode on the image. The architecture

Figure 6. Invisible/visible watermarking architecture in the DCT domain



was modeled, simulated and synthesized using VHDL, Modelsim XE III 6.0a tools, and VIRTUEX-II technology with xc2v500-6fg256 target, respectively. The estimated maximum frequency is 96.3 MHz was obtained.

Towards the development of a secure digital camera, Mohanty et al. (Mohanty, Adamo, & Kougianos, VLSI Architecture of an Invisible Watermarking Unit for a Biometric-Based Security System in a Digital Camera, 2007) have presented a VLSI architecture for an invisible biometric watermarking. Both the host image and the watermark image are partitioned into equal number of non-overlapping blocks. The block sizes of the host image and the watermark images are 8×8 and 2×2 blocks, respectively. Each block of the host image is transformed using DCT. The watermark, biometric image is inserted in the perceptually significant DCT coefficients, the DC component

and the first three AC components. Given the DC and the first three AC coefficients of the k^{th} block of the host image, $\{H_{DCT,k}(i,j), 0 \leq i, j \leq 2\}$, and the corresponding block of the watermark, $\{W_k(i,j), 0 \leq i, j \leq 2\}$, the watermark is inserted as follows:

$$H_{DCT,k}^*(i,j) = \begin{cases} H_{DCT,k}(i,j) + \alpha_{ij} H_{DCT,k}(i,j) & \text{if } W_k(i,j) = 1 \\ H_{DCT,k}(i,j) - \alpha_{ij} H_{DCT,k}(i,j) & \text{if } W_k(i,j) = 0 \end{cases} \quad (15)$$

Where $\alpha_{ij} = 0.1$ and $\alpha_{ij} = 0.02$ for AC and DC coefficients, respectively. The watermark is encrypted using AES before transformation.

The DCT module calculates the 1-D DCT across the rows followed by 1-D DCT across the columns. The watermark insertion module inserts the watermark according to Equation (15). Parallelism is exploited to insert a watermark in 2 clock cycles. This is achieved by calculating in

parallel the values of $(1 + \alpha_{ij})$ and $(1 - \alpha_{ij})$ and then selecting one of them for multiplication. A finite state machine with 7-states is used to implement the controller. A Prototype was implemented and synthesized using VHDL and Xilinx Vertex II technology (xc2v500-5fg256), respectively. Parallelism and resource-sharing (the multiplication unit was shared between the DCT and insertion modules) are used to achieve a maximum operating frequency of 256 MHz.

Motivated by the availability of graphics cards equipped with powerful processors (graphics processing units), Mohanty et al. (Mohanty, Pati, & Kougianos, 2007) have proposed an architecture for a GPU co-processor for real-time watermarking applications. The architecture is based on the blind invisible watermarking algorithm reported by Piva et al. (Piva, Barni, Bartolini, & Cappellini, 1997). The co-processor was simulated in Matlab, but not implemented.

DWT Domain Implementations

The motivation for using the discrete wavelet transform (DWT) is that DWT used in the JPEG2000 image compression standard. JPEG2000 was designed to achieve higher performance than JPEG, however, the computational complexity of JPEG2000 is substantially higher than JPEG.

Fan et al. (Fan, Van, Huang, & Tsao, 2005) have presented a hardware architecture of the wavelet-based adaptive visible watermarking algorithm reported in (Hu & Kwong, 2001). In the wavelet-based adaptive visible watermarking algorithm, the host and the watermark images are transformed by a discrete wavelet transform (DWT). The DWT coefficients of the host image, H_k^* , are obtained by embedding of the DWT coefficients of the watermark, W_w , in the host image, H_k , based on the following

$$H_k^*(i, j) = S(i, j)H_k(i, j) + (1 - S(i, j))W_w(i, j) \quad (16)$$

The scaling factor $S(i, j)$, is determined depending on the frequency subband using the following

$$S(i, j) = \begin{cases} \frac{\|H_w^*(i, j) - H(i, j)\|}{H(i, j)} \geq k \frac{\Delta I}{I} & \text{low frequency subband (LL)} \\ d^{(r_{\max} - r)} \sigma_x & \text{high frequency subbands (orientation = LH, HL, HH)} \end{cases} \quad (17)$$

In the low frequency subband, $S(i, j)$ is calculated based on the Weber fraction $\Delta I/I$ and the visible strength factor k . In the frequency subbands (frequency orientations LH, HL, and HH), $S(i, j)$ depends on the decomposition level, r ; the maximum decomposition level, r_{\max} ; the decay factor, d ; and σ_x . The decay factor yields smaller value in level one and larger values in higher levels (Fan, Van, Huang, & Tsao, 2005). The context modeling method is used to estimate the standard deviation σ_x (Fan & Tsao, A Dual Pyramid Watermarking for JPEG-2000, 2005).

The architecture of wavelet-based adaptive visible watermarking employs approximation, numerical reduction and resource sharing techniques to reduce hardware complexity. The host image, H , and the watermark image, W , are decomposed into three level multiresolution decomposition using DWT. Two parallel structures are used to embed the watermark, the first is for processing the frequency subbands $LL_3, LH_3, HH_3, LH_2, HL_2, HH_2$, and LH_1 , and the second is for processing HL_1 and HH_1 . In order to reduce hardware complexity, $S(i, j)$ values are pre-calculated and restricted to four values for each decomposition level depending on four different range of the wavelet coefficients. Shift registers are used to approximate the values of the scaling factors $S(i, j)$. Resource sharing techniques are employed to use the shift registers to calculate the scaling factors ($1 - S(i, j)$). The direct implementation of the algorithm reported in (Hu & Kwong, 2001) requires 24, 12, 3, 1, and 2, additions, multiplications, divisions, radical operation, and shift registers, respectively. The proposed architecture needs 30 additions and 5 shift registers.

A progressive invisible watermarking module has been reported by Hsiao et al. (Hsiao, Tai, & Chang, 2000) as part of a VLSI architecture for zerotree wavelet image encoder/decoder. The watermark is a sequence of pseudo-random bit sequence that are generated using a LFSR. The watermark bits are embedded sequentially; a watermark bit is inserted in the bit position next to the first nonzero bit of each significant wavelet coefficient. The watermark can be detected based on the correlation between the received watermark sequence and the original watermark. Watermark can be performed progressively from partially received image data.

Walsh Transform Domain

An FPGA implementation of spread spectrum invisible-fragile watermarking algorithm has been reported in (Maity, Banerjee, Abhijit, & Kundu, 2007) and (Maity, Kundu, & Maity, 2009). The host image is divided into 8×8 non-overlapping block. The size of the block was selected to be 8×8 in order to make the algorithm compatible with the JPEG image compression standard. Each block is transformed using Walsh transform. A set of pseudo-noise code patterns is generated using LFSR (Linear feedback shift register). The total number of patterns, N , is equal to the number of bits in the watermark. A 64-bit code pattern, $\{P_n(i, j), 1 \leq i, j \leq 8\}$, $1 \leq n \leq N$, is used to spread each watermark bit into the Walsh transform coefficients. Given the Walsh transform of 8×8 block of the host image, $\{H_{WT}(i, j), 1 \leq i, j \leq 8\}$, and a binary watermark, $\{b_1, b_2, \dots, b_N\}$, the watermarked block in the Walsh transform is given by:

$$H_{WT}^*(i, j) = H_{WT}(i, j) + \alpha \sum_{n=1}^N b_n P_n(i, j) \quad (18)$$

where α is the gain factor or modulation index. The proper selection of α will optimize the maximum

amount of allowed distortion.

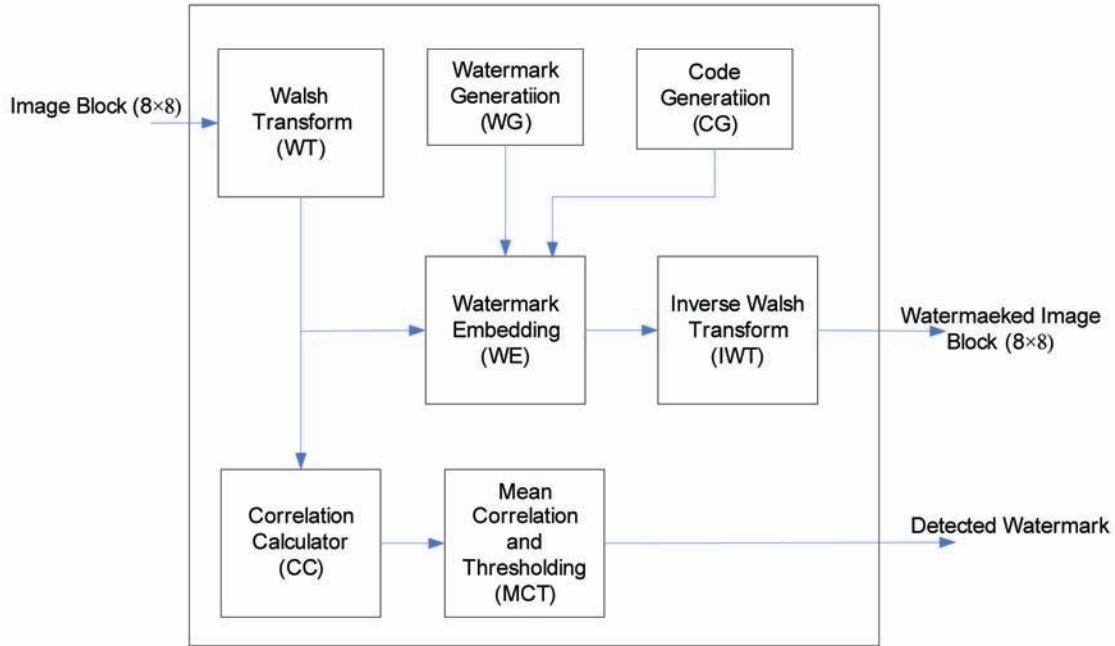
The architecture is shown in *Figure 7*. The Walsh Transform and Inverse Walsh Transform modules compute the forward and the inverse Walsh transform of the input block, respectively. A fast Walsh transform algorithm similar to the Fast Fourier transform computation is used. The Code Generation module consists of two submodules; each submodule generates two code patterns of length 64. The Watermark Embedding module adds the output from code generation module to the output from the Walsh transform module to obtain the coefficients of the watermarked block. To detect the watermark, the Correlation Calculator module calculates the correlation between the spreading functions and Walsh coefficients. The correlation values are fed into the Mean Correlation and Thresholding module.

A VLSI design is implemented for gray level image of size 8×8 and a 4-bit binary watermark. Xilinx SPARTAN series FPGA (XCS40) is used to implement the design. The implementation used 730 CLBs out of the 784 CLBs available in the chip. The chip can operate at a maximum frequency of 80 MHz and the data rate is 930.232 Kbits/s. Achieving a higher throughput requires mapping the proposed architecture to higher end FPGA (Maity, Kundu, & Maity, 2009). The implementation can be extended to larger image size by using appropriate number of modules in parallel (each module can handle 8×8 pixels). The implementation also includes a watermark decoding unit. We note that this architecture is suffers from the same disadvantages of spatial domain techniques as it does not use the transforms used by image compression standards.

HARDWARE IMPLEMENTATIONS OF VIDEO WATERMARKING

As video is composed of consecutive frames, video watermarking can be achieved by watermarking each frame as a still image, using image

Figure 7. Block diagram architecture of a Walsh transform based watermark embedding and detection



watermarking algorithms. However, video data is massive; for example, a digital video of 720×480 pixels with 3 bytes (24-bit) of color data per pixel and 30 frames/second has a rate of 248 Mbps. This high rate might make the extension of image watermarking techniques and architectures inefficient to handle video watermarking. This has motivated researchers to devise low complexity video watermarking algorithms and efficient hardware implementations. Similar to image watermarking, a watermark can be embedded into a video stream in the spatial domain or in the frequency domain. Hence, hardware implementations for video watermarking are divided into two categories: spatial domain implementations and frequency domain implementations.

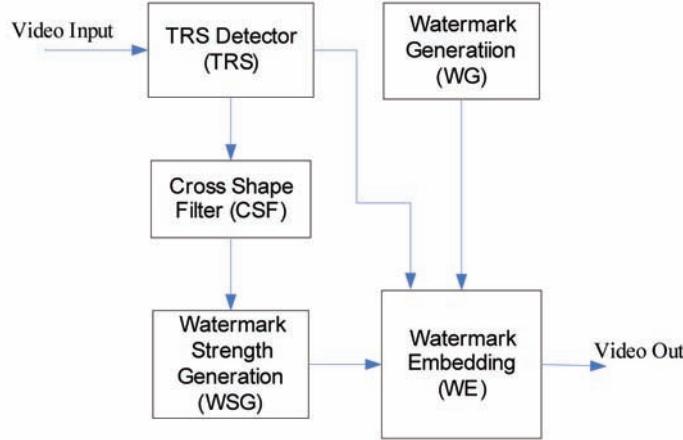
Spatial Domain Implementations

In this section, we present spatial domain video watermarking algorithms implementations, while frequency domain techniques are discussed in the next section.

Invisible Video Watermarking Implementations

Mathai et al. (Mathai, Sheikholeslami, & Kundur, 2003) have presented an ASIC implementation of the JAWS watermark embedding and detection. In JAWS, the watermark is embedded in the spatial domain. A base watermark is generated by using the input payload to modulate a pseudo-random noise pattern. The base watermark is then perceptually shaped for each frame so that the watermark remains perceptually invisible. This is done by high-pass filtering a frame to determine the embedding depth of the watermark based on the activity measure of the frame (e.g., complex texture has high activity, flat area has low activity). The watermark is obtained by pixel-wise multiplication of the embedding depth and the base watermark. Finally, the watermark is embedded into the original frame by pixel-wise addition of the video frame and the watermark. Detection of the watermark is achieved by computing FFT and IFFT to obtain peaks of the normally distributed

Figure 8. Standard and high definition video watermarking architecture



reference pattern and watermark pattern. Peaks orientations provide sign information of the embedded bits.

The implementation is based on 0.18μ CMOS process with a core area of 3.53 mm^2 . The chip operates at 75 MHz and it can watermark a stream of video at 30 frames/sec and 320×320 pixels/frame in real-time. The power consumption of the watermark embedded and detector are 60 mW and 100 mW, respectively.

A real-time video watermarking chip for watermarking of standard and high definitions video has been presented by Jeong et al. (Jeong, Moon, & Kim, 2007). The implemented video watermarking algorithm is based on the algorithm reported by Kutter et al. (Kutter & Winkler, 2002). Here, to embed a binary sequence $\{b_i, 0 \leq i \leq N-1\}$, the watermark $W(i, j)$ is calculated by

$$W(i, j) = \sum_{l=0}^{N-1} (-1)^{b_l} \varphi_l(i, j) \alpha(i, j) \quad (19)$$

Where $\varphi_l(i, j)$ and $\alpha(i, j)$ are modulation function and watermark strength, respectively. The watermarked image is calculated as

$$H^*(i, j) = H(i, j) + W(i, j) \quad (20)$$

In the presented implementation, a Hadamard sequence is used to realize the modulation function instead of using pseudo-random function.

To control the strength of the watermark, the image is high pass filtered by a cross shape filter (CSF). The watermark is embedded with a relatively low strength in low detail areas, while it is embedded with a higher strength in areas of high details (e.g., contours and edges). To reduce the computational complexity, integer arithmetic is used. A block diagram of the proposed architecture is shown in Figure 8. The input video is SDI format, the Y component is extracted and high pass filtered by the CSF module. This filtering operation detects the edges in the frame. The Watermark Strength Generation module generates the watermark strength for each pixel of the filtered image. The filter outputs are mapped into different floating point intervals. Each interval is mapped into an integer value. A scalar quantizer is realized by a simple lookup table. The watermark strength is adjusted to 6 levels. The watermark generator generates the watermark. Hadmarad sequences are stored in a ROM (256×256 matrix) and a table lookup is used to select the appropriate sequence according to the provided key.

The implementation is carried out using Altera STARTIX II FPGA device family. Real-time op-

eration is achieved for a frame size of 720×487 pixels.

Video watermarking in digital cinema application is a real challenge. In such application the resolution of frames to be watermarked can have a size of 4096×2160 pixels or more (Rouvroy, Standaert, Lefebvre, Quisquater, Macq, & Legat, 2004). Hence, high throughput implementations are essential. Rouvroy et al. (Rouvroy, Lefebvre, Standaert, Macq, Quisquater, & Legat, 2004) have presented an FPGA implementation for video fingerprinting of digital cinema. The implementation is based on the watermarking algorithm developed by Lefebvre et al. (Lefebvre, Gueluy, Delannay, & Macq, 2001). The 64-bit original message is encoded to 128-bit using a convolutional code. A 40-bit key (K_0) is used to generate an MLS (maximum shift register) pseudo-random sequence. From the convolutional code and the MLS code a 1-D cyclic sequence, $P_1(i)$ of size 2^{15} is generated. A 2-D cyclic pattern $P_2(i,j)$ is generated using two 8-bit secret keys (K_1 and K_2) as follows:

$$P_2(i, j) = P_1[(i * K_1 + j * K_2) \bmod \text{length}(P_1)] \quad (21)$$

This algorithm is robust against image processing operations and against cropping and translation (Rouvroy, Lefebvre, Standaert, Macq, Quisquater, & Legat, 2004).

The block diagram of the fingerprinting architecture for digital cinema is shown in *Figure 9*. Once the PG1 module generates the 1-D pattern $P_1(i)$, the PG2 module will start to compute the 2-D pattern, $P_2(i,j)$, assuming the pixels are arrived in raster scan fashion. The $P_2(i,j)$ pattern is stored in a RAM (organized as 2 RAM blocks). The Pixel Activity (PA) module calculates the activity of a pixel (i,j) as the difference between the pixel's intensity and the mean of the 8 neighbouring pixels. The Watermark Embedding (WE) module, applies the Weber-Fechner law (stored in a ROM) and inserts the watermark depending

on the value of $P_2(i,j)$. The WE module also ensures that the value of watermarked pixel is between 0 and 255. Each module is designed as a pipeline to ensure real time watermarking of a frame size of 2048×1024 .

The synthesis of the design is carried out using Synplify Pro 7.2. The architecture is implemented on a Xilinx Virtex-II XC2V500-6 FPGA. The chip operates at a maximum frequency of 143.9 MHz. The main advantage of this chip is that it is capable of watermarking 182.98 and 68.62 frames/sec of size 1024×768 and 2048×1024 pixels, respectively.

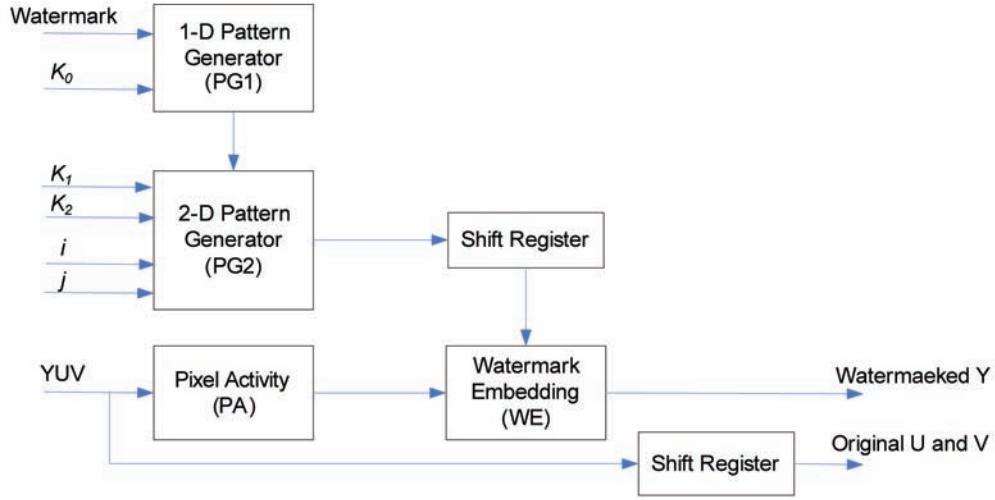
Frequency Domain Implementations

Due to high bandwidth requirement, video is usually stored and transmitted in compressed domain. Different encoding standards are currently used for video compression, like H.261, H.263, MPEG-2, MPEG-4 and motion JPEG2000. The H.264 is the latest video compression standard. It has higher rate distortion in comparison with the previous standard. In comparison with previous standards, H.264 supports higher video rates and it has much higher computational complexity.

Motivated by the need to support watermarking in the compressed domain, an FPGA implementation to insert a broadcaster's logo in video streams has been proposed by Mohanty et al. (Mohanty, S. P., Koulianios, Cai, & Ratnani, 2009). The watermarking algorithm is based on the algorithm presented by Mohanty et al. (Mohanty, Ramakrishnan, & Kankanhalli, A DCT Domain Visible Watermarking Technique for Images, 2000).

The architecture is implemented on an Altera Quartus for a Cyclone-II FPGA. The maximum frequency of the chip is 100MHz. Simulation results demonstrated that the chip can process NTSC television video at a rate of 43 frames/sec. The implementation integrates video compression and video watermarking. The implementation can be used real-time applications such as IP-TV and

Figure 9. Fingerprinting architecture for digital cinema



video broadcasting (Mohanty S. P., Kougianos, Cai, & Ratnani, 2009).

Karmani et al. (Karmani, Djemal, & Tourki, 2009) and (Karmani, Djemal, & Tourki, A Blin Watermarking Algorithm Implementation for Digital Images and Video, 2007) have proposed an FPGA architecture for image/video watermarking in the wavelet domain. The frame to be watermarked is decomposed using a 3-level DWT to obtain the following subbands: $\text{HH}_3, \text{HL}_3, \text{LH}_3, \text{LL}_3, \text{HH}_2, \text{HL}_2,$

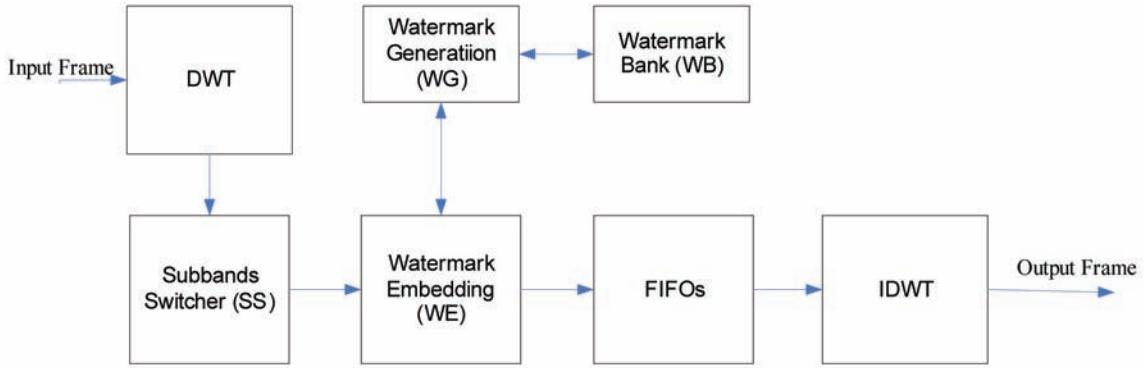
$\text{LH}_2, \text{HH}_1, \text{HL}_1, \text{LH}_1$. The watermark $W(i,j)$, a 256×256 image, is decomposed using a 3-level 2-D discrete wavelet transform to obtain the frequency subbands $\text{hh}_3, \text{hl}_3, \text{lh}_3, \text{ll}_3, \text{hh}_2, \text{hl}_2, \text{lh}_2, \text{hh}_1, \text{hl}_1$, and lh_1 . A set of 16 watermarks, $\{w_0, \dots, w_{15}\}$, each of size 64×64 is generated by partitioning each subband into non-overlapping blocks (1/16 of each subband). Each water mark is decomposed into bit-planes. A pseudo-random permutation of the decomposed bit-plane is carried out to enhance the security. The bit-planes of w_i are inserted into a number of consecutive frames (8 bits/coefficient means 8 consecutive frames). The insertion is performed by the coefficient sets quantization to represent the watermark bit (Karmani, Djemal, & Tourki, 2009). The insertion in the middle fre-

quency subbands ($\text{HL}_3, \text{HL}_3, \text{HL}_2$, and LH_2, HL_1 , and LH_1). The insertion is performed at different levels. In the first level, hh_1 and hl_1 subbands are embedded into HL_1 and lh_1 is inserted into LH_1 . In the second level, hh_2 and hl_2 are embedded into HL_2 and lh_2 is inserted into LH_2 . In the third level, hh_3 and hl_3 are embedded into HL_3 .

A block diagram of the proposed architecture is shown in Figure 10. The DWT and IDWT modules evaluate the 3-level forward and inverse discrete wavelet transform, respectively. The DWT module is implemented by calculating the row-wise followed by the column-wise 1-D DWT. The Watermark Generation module performs bit-plane decomposition and pseudo-random permutation of the watermark which are stored in the Watermark Bank (WB). The WB is organized to implement the pseudo-random permutation of the bit-planes. The Watermark Embedding (WE) consists of 6 insertion blocks (corresponds to 6 middle subbands). Each insertion block has a finite state machine. Although it watermarking is performed in the wavelet domain, the final frame is in spatial domain.

The architecture is implemented on Altera STARTIX-II EP2S606C57ES FPGA for a frame size of 256×256 pixels and a watermark of the

Figure 10. DWT-based video watermarking architecture



same size. Watermarking of a grey level frame of 256×256 pixel can be achieved in 8.2 ms using 100 MHz clock frequency.

FUTURE RESEARCH DIRECTIONS

During the past few years, the need to design efficient Digital Rights Management systems has encouraged research work in digital watermarking. Different research tracks are still emerging at both the algorithmic and architectural levels. Current image and video compression standards are based on DCT and DWT. To apply DCT-based techniques on DWT compressed images, for example, require decompressing the image/video and then re-compressing it. This solution is inefficient and may degrade image quality. Extensions of image watermarking algorithms to support video might not be efficient, especially with the development of new compression standards such as the H.264. Hence efficient techniques are required in both DCT and DWT domains. The new techniques should address robustness to mixed operations such as camera operations, cropping, and image/video scalability.

Many hardware implementations have been reported, we note that each implementation is useful for certain application. The application of image and video watermarking in consumer elec-

tronics such as digital cameras and video players demand low cost, small chip size, and low power consumption. In addition, one of the economic concerns in the design of embedders and detectors is the different processing power capabilities of different devices (PDA, digital camera, etc.). To reduce cost, it is worthwhile to invest in a single architecture that can be scaled (in terms of performance and power consumptions) for the various application areas. Reconfigurable computing and hardware-software co-design techniques might be very useful to overcome implementation issues and achieve a better trade-off between cost and performance.

Implementations in spatial domain are efficient mainly because of the low computational complexity of spatial domain algorithms. However, it is expected that images and videos to be compressed before storage and/or transmission. More work is required in the implementations of watermarking in the frequency domain, particularly in the DCT and DWT domains. The suitability of the reported watermarking architectures for inclusion in codec systems should be investigated. At the system level architecture, the design of combined codec and watermarking architectures with embedding and extraction features should be explored.

Finally, for digital watermarking to be useful in many applications, an infrastructure and set

of standards for digital watermarks needs to be created.

CONCLUSION

Digital watermarking is the imperceptible, robust and secure embedding of a pattern or a signature, dubbed as the watermark, in a digital media. The watermark is embedded during production or distribution and can be extracted or detected for different purposes including copyright protection, monitoring, authentication, and access control. The data rates of image and video makes watermarking algorithms computationally intensive. The use of watermarking in consumer products and real-time applications dictates the development of hardware architectures. This chapter has presented a survey of existing implementations of image and video watermarking. With advances in VLSI technologies, it is possible to develop cost effective image and video watermarking for consumer products.

REFERENCES

- Acharya, T., & Chakrabarti, C. (2006). A survey on lifting-based discrete wavelet transform architectures. *Journal of VLSI Signal Processing Systems*, 42(3).
- Adamo, B., Mohanty, S. P., Kougianos, E., Varanasi, M., & Cai, W. (2006). VLSI architecture and FPGA prototyping of a digital camera for image security and authentication. In *Proceedings of the IEEE Region 5 Technology and Science Conference*, (pp. 154-158).
- Adamo, O. B., Mohanty, S. P., Kougianos, E., & Varanasi, M. (2006). VLSI architecture for encryption and watermarking units towards the making of a secure camera. In *Proceedings of the IEEE International SOC Conference*, (pp. 141-144).
- Bilgin, A., & Marcellin, M. (2006). JPEG2000 for digital cinema. In *Proceedings of the IEEE International Symposium on Circuits and Systems*, (pp. 3881 - 3885).
- Böhle, K., Rader, M., Weber, A., & Weber, D. (2008). *Looking Forward in the ICT & Media Industries*. European Technology Assessment Group.
- Braudaway, G. W., Magerlein, K. A., & Mintzer, F. (1996). Protecting publicly available images with a visible image watermark. In *The SPIE Conference on Optical Security and Counterfeit Deterrence Technique, SPIE-2659*, (pp. 126 – 132).
- Brunton, A., & Zhao, J. (2005). Real-time video watermarking on programmable graphics hardware. In *Canadian Conference on Electrical and Computer Engineering*, (pp. 1312 - 1315).
- Chakrabarti, C., Vishwanath, M., & Owen, R. M. (1995). A survey of architectures for the discrete and continuous wavelet transforms. *International Conference on Acoustics, Speech, and Signal Processing*, 5, (pp. 2849 - 2852).
- Charoensak, C., & Sattar, F. (2005). Design of low-cost FPGA hardware for real-time ICA-based blind source separation algorithm. *EURASIP Journal on Applied Signal Processing*, 18, 3076–3086. doi:10.1155/ASP.2005.3076
- Corvi, M., & Nicchiotti, G. (1997). Wavelet-based image watermarking for copyright protection. In *Proceedings of the Scandinavian Conference on Image Analysis*, (pp. 157 – 163).
- Cox, I. J., Kilian, J., Leighton, T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673–1687. doi:10.1109/83.650120
- Deskshare. (2005, October). *Vcd, svcd and dvd quality, capacity and media types*. Retrieved from http://www.deskshare.com/Resources/articles/dmc_VcdQuality.aspx

- Echizen, I., Yamada, T., Fujii, Y., Tezuka, S., & Yoshiura, H. (2005). Real-time video watermark embedding system using software on personal computer. In *Proceedings of the IEEE International Conference on System, Man and Cybernetics*, (pp. 3369 - 3373).
- ElAreef. T., Heniedy, H. S., & Ouda, O. M. (2006). Performance evaluation of image watermarking techniques. In *Proceedings of the 4th International Conference on Information & Communications Technology*, (pp. 1-1).
- ElZouka, H. (2008). FPGA based implementation of robust watermarking system. In *Fifth International Conference on Information Technology*, (pp. 1274 - 1278).
- Fan, Y.-C., & Tsao, H.-W. (2005). A dual pyramid watermarking for JPEG-2000. In *The First International Workshop on Information Networking and Applications*.
- Fan, Y.-C., Van, L.-D., Huang, C.-M., & Tsao, H.-W. (2005). Hardware-efficient architecture design of adaptive visible watermarking. In *Proceedings of the Ninth International Symposium on Consumer Electronics*, (pp. 399 - 404).
- Fretland, T., Fritsch, L., & Grove, A. K. (2008). *State of the art in Digital Rights Management*. MARIAGE.
- Furht, B., & Kirovski, D. (2006). *Multimedia Watermarking Techniques and Applications*. Boca Raton, FL: CRC Press.
- Garimella, A., Satyanarayana, M., Kumar, R., Murugesh, P., & Niranjan, U. (2003). VLSI implementation of online digital watermarking technique with difference encoding for 8-bit gray scale images. In *Proceedings of the 16th International Conference on VLSI Design*, (pp. 283 - 288).
- Garimella, A., Satyanarayana, M., Murugesh, P., & Niranjan, U. (2004). ASIC for digital color image watermarking. In *IEEE 11th Digital Signal Processing Workshop & IEEE Signal Processing Education Workshop*, (pp. 292 - 296).
- Haouzia, A., & Noumeir, R. (2008). Methods for image authentication: a survey. *Multimedia Tools and Applications*, 39(1), 1–46. doi:10.1007/s11042-007-0154-3
- Hsiao, S.-F., Tai, Y.-C., & Chang, K.-H. (2000). VLSI design of an efficient embedded zerotree wavelet coder with function of digital watermarking. *IEEE Transactions on Consumer Electronics*, 46(3), 628–636. doi:10.1109/30.883423
- Hu, Y., & Kwong, S. (2001, September). Wavelet domain adaptive visible watermarking. *Electronics Letters*, 37(20), 1219–1220. doi:10.1049/el:20010838
- Jeong, Y.-J., Moon, K.-S., & Kim, J.-N. (2007). FPGA based implementation of real-time video watermarking chip. *LNCS*, 4523, 133–141.
- Kalker, T., Depovere, G., Haitsma, J., & Maes, M. (1999). A video watermarking system for broadcast monitoring. In *Proceedings of the SPIE: Security and Watermarking of Multimedia Contents*, 3657, 103–112.
- Karmani, S., Djemal, R., & Tourki, R. (2007). A blind watermarking algorithm implementation for digital images and video. *International Journal of Soft Computing*, 2(2), 292–301.
- Karmani, S., Djemal, R., & Tourki, R. (2009). 2D-scan-based wavelet watermarking for image and video. In *Computer Standards & Interfaces* (pp. 801–811). Efficient Hardware Architecture of.
- Kejariwal, A., Gupta, S., & Nicolau, A. (2006). Energy efficient watermarking on mobile devices using proxy-based partitioning. *IEEE Transactions on Very Large Scale Integration Systems*, 14(6), 625–636. doi:10.1109/TVLSI.2006.878218

- Kim, H. C., Ogunleye, H., Guitart, O., & Delp, E. J. (2004). The watermark evaluation testbed (WET). In *Proceedings of SPIE Electronic Imaging*, 5306, 236–247.
- Kim, K.-S., Lee, H.-Y., IM, D.-H., & Lee, H.-K. (2008). Practical, real-time, and robust watermarking on the spatial domain for high-definition video contents. *IEICE Transactions on Informations and Systems*, (5), 1359 - 1368.
- Koch, E., & Zhao, J. (1995). Towards robust and hidden image copyright labeling. In *Proceedings of the International Workshop on Nonlinear Signal Image Processing*, (pp. 452 – 455).
- Kougianos, E., Mohanty, S. P., & Mahapatra, R. N. (2009, March). Hardware assisted watermarking for multimedia. *International Journal on Computers and Electrical Engineering*, 35(2), 339–358. doi:10.1016/j.compeleceng.2008.06.002
- Kutter, M., & Winkler, S. (2002). A vision-based masking model for spread-spectrum image watermarking. *IEEE Transactions on Image Processing*, 11, 16–25. doi:10.1109/83.977879
- Lefebvre, F., Gueluy, D., Delannay, D., & Macq, B. (2001). *A Print and Scan Optimized Watermarking Scheme* (pp. 511–516). Cannes, France: MMSP.
- Lim, H., Park, S.-Y., Kang, S.-J., & Cho, W.-H. (2003). FPGA Implementation of Image Watermarking Algorithm for a Digital Camera. *IEEE Pacific Rim Conference on Communications, Computers and signal Processing*, 2, (pp. 1000 - 1003).
- Lin, C.-Y., & Chang, S.-F. (2000). Semi-fragile watermarking for authenticating JPEG visual content. *SPIE Security and Watermarking of Multimedia Contents II*, 3971, 140–151.
- Macq, B., Dittmann, J., & Delp, E. (2004). Benchmarking of image watermarking algorithms for digital rights management. *Proceedings of the IEEE*, 92(6), 971–984. doi:10.1109/JPROC.2004.827361
- Maes, M., Kalker, T., Linnartz, J.-P., Talstra, J., Depover, G., & Haitsma, J. (2000, September). Digital watermarking for DVD video copy protection. *IEEE Signal Processing Magazine*, 47–57. doi:10.1109/79.879338
- Maity, S. P., Banerjee, A., Abhijit, A., & Kundu, M. K. (2007). VLSI design of spread spectrum watermarking. In *13th National Conference on Communication*, (pp. 251 - 257), IIT Kanpur, India.
- Maity, S. P., Kundu, M. K., & Maity, S. (2009). Dual purpose FWT domain spread spectrum. Image watermarking in real-time. *Computers & Electrical Engineering*, 35(2), 415–433. doi:10.1016/j.compeleceng.2008.06.003
- Mathai, N. J., Kundur, D., & Sheikholesla, A. (2003, April). Hardware implementation perspectives of digital video watermarking algorithms. *IEEE Transactions on Signal Processing*, 51(4), 925–938. doi:10.1109/TSP.2003.809382
- Mathai, N. J., Sheikholeslami, A., & Kundur, D. (2003). VLSI Implementation of a Real-Time Video Watermark Embedder and Detector. In *Proceedings of the 2003 International Symposium on Circuits and Systems*, 2, (pp. II-772- II-775).
- Mohanty, S., Kougianos, E., & Ranganathan, N. (2007). VLSI architecture and chip for combined invisible robust and fragile watermarking. *IET Computers & Digital Techniques*, 1(5), 600–611. doi:10.1049/iet-cdt:20070057
- Mohanty, S., Pati, N., & Kougianos, E. (2007). A Watermarking Co-Processor for New Generation Graphics Processing Units. *International Conference on Consumer Electronics*, (pp. 1 - 2).
- Mohanty, S. P. (1999). *Digital Watermarking: A Tutorial Review*. Bangalore, India: Department of Electrical Engineering, Indian Institute of Science.

- Mohanty, S. P., Adamo, O. B., & Kougianos, E. (2007). VLSI Architecture of an Invisible Watermarking Unit for a Biometric-Based Security System in a Digital Camera. In *The 25th IEEE International Conference on Consumer Electronics*, (pp. 485-486).
- Mohanty, S. P., & Bhargava, B. K. (2008). Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks. *CM Transactions on Multimedia Computing, Communications, and Applications*, 5(2), 12:1-12:22.
- Mohanty, S. P., Kougianos, E., Cai, W., & Ratnani, M. (2009). VLSI Architectures of Perceptual Based Video Watermarking for Real-Time Copyright Protection. In *The 10th IEEE International Symposium on Quality Electronic Design*, (pp. 527-534).
- Mohanty, S. P., Kumara, R. C., & Nayak, S. (2004). FPGA Based Implementation of an Invisible-Robust ImageWatermarking Encoder. *LNCS*, 344-353.
- Mohanty, S. P., Ramakrishnan, K. R., & Kankanhalli, M. S. (2000). A DCT Domain Visible Watermarking Technique for Images. In *Proceedings of the IEEE International Conference on Multimedia*, (pp. 1029 – 1032).
- Mohanty, S. P., Ranganathan, N., & Balakrishnan, K. (2006). A dual voltage-frequency VLSI chip for image watermarking in DCT domain. *IEEE Transactions on Circuits and Systems II*, 53(5), 394–398. doi:10.1109/TCSII.2006.870216
- Mohanty, S. P., Ranganathan, N., & Namballa, R. K. (2003). VLSI Implementation of Invisible Digital Watermarking Algorithms Towards the Development of a Secure JPEG Encoder. *IEEE Workshop on Signal Processing Systems*, (pp. 183 - 188).
- Mohanty, S. P., Ranganathan, N., & Namballa, R. K. (2005). A VLSI architecture for visible watermarking in a secure still digital camera (S2DC) design. *IEEE Transactions on Very Large Scale Integration Systems*, 13(8), 1002–1012. doi:10.1109/TVLSI.2005.857991
- Navasd, K. A., & Sasikumar, M. (2007). Survey of Medical Image Watermarking Algorithms. In *The 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications*, Tunisia.
- Petitjean, G., Dugelay, J., Gabriele, S., Rey, C., & Nicolai, J. (2002). Towards real-time video watermarking for system-on-chip. In *Proceedings of IEEE International Conference on Multimedia and Expo*, I, 597–600.
- Pirsch, P., Demassieux, N., & Gehrke, W. (1995). VLSI architectures for video compression: a survey. *Proceedings of the IEEE*, 83(2), 220–246. doi:10.1109/5.364465
- Piva, A., Barni, M., Bartolini, F., & Cappellini, V. (1997). DCT-Based watermark recovering without restoring to the uncorrupted original image. *International Conference on Image Processing*, III, (pp. 520 - 523).
- Potdar, V. M., Han, S., & Chang, E. (2005). A Survey of Digital Image Watermarking Techniques. *Proceedings of the 3rd International Conference on Industrial Informatics*, (pp. 709 - 716).
- Prasad, M., & Koliwad, S. (2009). A comprehensive survey of contemporary researches in watermarking for copyright protection of digital images. *International Journal of Computer Science and Network Security*, 9(4), 91–107.
- Rey, C., & Dugelay, J.-L. (2002). A survey of watermarking algorithms for image authentication. *EURASIP Journal on Applied Signal Processing*, (1): 613–621. doi:10.1155/S1110865702204047

- Rouvroy, G., Lefebvre, F., Standaert, F.-X., Macq, B., Quisquater, J.-J., & Legat, J.-D. (2004). Hardware Implementation of a Fingerprinting Algorithm Suited for Digital Cinema. *European Signal Processing Conference*, (pp. XXXV-2310).
- Rouvroy, G., Standaert, F.-X., Lefebvre, F., Quisquater, J.-J., Macq, B., & Legat, J.-D. (2004). Reconfigurable Hardware Solutions for the Digital Rights Management of Digital Cinema. In *Proceedings of the 4th ACM Workshop on Digital Rights Management* (pp. 40 - 53). Washington, DC: ACM.
- Sadeghi, A.-R. (2008). The Marriage of Cryptography and Watermarking -- Beneficial and Challenging for Secure Watermarking and Detection. In *Proceedings of the 6th International Workshop on Digital Watermarking*, (pp. 2 - 18).
- Schyndel, R. G., Tirkel, A. Z., & Osborne, C. F. (1994). A digital watermark. *Proceedings of the IEEE International Conference on Image Processing*, 2, 86–90.
- Smith, J. R., & Comiskey, B. O. (1996). Modulation and Information Hiding in Images. In *Proceedings of the First Information Hiding Workshop*, (pp. 207 - 226).
- Strycker, L. D., Termont, P., Vandewege, J., Haitsma, J., Kalker, A., & Maes, M. (2000). Implementation of a realtime digital watermarking process for broadcast monitoring on Trimedia VLIW processor. *IEE Proceedings. Vision Image and Signal Processing*, 147(4), 371–376. doi:10.1049/ip-vis:20000580
- Tefas, A., & Pitas, I. (2001). Robust spatial image watermarking using progressive detection. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, 3, 1973–1976.
- Tsai, T.-H., & Wu, C.-Y. (2003). An Implementation of Configurable Digital Watermarking System in MPEG Video Encoder. *IEEE International Conference on Consumer Electronics*, (pp. 216 - 217).
- Van Leest, A., Haitsma, J., & Kalker, T. (2003). On digital cinema and watermarking. *SPIE Proceedings Security and Watermarking of Multimedia Contents V*, 5020, 526–535.
- Wang, J., Liu, J. C., & Masilela, M. (2009). A real-time video watermarking system with buffer sharing for video-on-demand service. *Computers & Electrical Engineering*, 35, 395–414. doi:10.1016/j.compeleceng.2008.06.011
- Wiegand, T., Sullivan, G. J., Bjontegaard, G., & Luthra, A. (2003). Overview of the 264/AVC video coding standard. *IEEE Transactions on Circuits and Systems for Video Technology*, 13(7), 560–576. doi:10.1109/TCSVT.2003.815165
- Wong, P. W. (1998). A public key watermark for image verification and authentication. *Proceedings of the International Conference on Image Processing*, 1, 455–459.
- Xia, X. G., Boncelet, C. G., & Arce, G. R. (1998). Wavelet transform based watermarking for digital images. *Optics Express*, 3(1), 497–511. doi:10.1364/OE.3.000497
- Xie, R., Wu, K., Du, J., & Li, C. (2007). Survey of Public Key Digital Watermarking Systems. *Proceedings of the International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, (pp. 439 - 443).
- Yaqin, Z., Zhilu, W., Guanghui, R., & Xuemai, G. (2002). A New Approach of 2D Discrete Cosine Transform with Mobius Inverse Formula. *Proceedings of the 6th International Conference on Signal Processing*, 1, 162 - 165.

- Zhang, F., Pan, Z., Cao, K., Zheng, F., & Wu, F. (2008). The upper and lower bounds of the information-hiding capacity of digital images. *Information Sciences*, 178(14), 2950–2959. doi:10.1016/j.ins.2008.03.011
- Zheng, D., Liu, Y., Zhao, J., & El-Saddik, A. (2007). A survey of RST invariant image watermarking algorithms. [CSUR]. *ACM Computing Surveys*, 39(2). doi:10.1145/1242471.1242473
- Rey, C., & Dugelay, J.-L. (2002). A survey of watermarking algorithms for image authentication. *EURASIP Journal on Applied Signal Processing*, (1): 613–621. doi:10.1155/S1110865702204047
- Sadeghi, A.-R. (2008). The Marriage of Cryptography and Watermarking -- Beneficial and Challenging for Secure Watermarking and Detection. *Proceedings of the 6th International Workshop on Digital Watermarking*, (pp. 2 - 18).

ADDITIONAL READING

- Acharya, T., & Chakrabarti, C. (2006). A survey on lifting-based discrete wavelet transform architectures. *Journal of VLSI Signal Processing Systems*, 42(3).
- Bilgin, A., & Marcellin, M. (2006). JPEG2000 for Digital Cinema. *Proceedings of the IEEE International Symposium on Circuits and Systems*, (pp. 3881 - 3885).
- Chakrabarti, C., Vishwanath, M., & Owen, R. M. (1995). A Survey of Architectures for the Discrete and Continuous Wavelet Transforms. *International Conference on Acoustics, Speech, and Signal Processing*, 5, pp. 2849 - 2852.
- Fretland, T., Fritsch, L., & Grove, A. K. (2008). *State of the art in Digital Rights Management*. MARIAGE.
- Haouzia, A., & Noumeir, R. (2008). Methods for image authentication: a survey. *Multimedia Tools and Applications*, 39(1), 1–46. doi:10.1007/s11042-007-0154-3
- Pirsch, P., Demassieux, N., & Gehrke, W. (1995). VLSI architectures for video compression: a survey. *Proceedings of the IEEE*, 83(2), 220–246. doi:10.1109/5.364465
- Van Leest, A., Haitsma, J., & Kalker, T. (2003). On digital cinema and watermarking. *SPIE Proceedings Security and Watermarking of Multimedia Contents V*, 5020, 526–535.
- Wang, J., Liu, J., & Masilela, M. (2009). A real-time video watermarking system with buffer sharing for video-on-demand service. *Computers & Electrical Engineering*, 395–414. doi:10.1016/j.compeleceng.2008.06.011
- Xie, R., Wu, K., Du, J., & Li, C. (2007). Survey of Public Key Digital Watermarking Systems. *Proceedings of the International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, (pp. 439 - 443).
- Zheng, D., Liu, Y., Zhao, J., & El-Saddik, A. (2007). A survey of RST invariant image watermarking algorithms. [CSUR]. *ACM Computing Surveys*, 39(2). doi:10.1145/1242471.1242473

KEY TERMS AND DEFINITIONS

Spatial Domain: The domain in which each image value at location (i, j) is represented by its intensity, also known as pixel domain.

Frequency Domain: The domain in which each image value at location (i, j) represents the amount that the intensity values in image vary over a specific distance related to (i, j) , also known as transform domain.

Image Compression: The application of techniques to reduce the number of bits required to represent an image while maintaining an acceptable quality.

Pipeline: Is an implementation practice in which multiple computations are overlapped in execution.

Field Programmable Gate Array (FPGA): A semiconductor device (integrated circuit) that can be configured or programmed after manufacturing by a designer for a specific application.

Application Specific Integrated Circuit (ASIC): An integrated circuit that is designed and manufactured for a specific application.

Chapter 18

Spread Spectrum Watermarking: Implementation in FPGA

Santi P. Maity

Bengal Engineering and Science University, India

ABSTRACT

Spread spectrum (SS) watermarking has proven to be efficient, robust and cryptographically secure. Each bit of watermark information is embedded over wide spectrum of the host signal based on spectrum spreading concept of SS modulation in digital communication and can easily be integrated with many existing data transmission scheme. This has made SS watermarking method more attractive during recent times for many non-conventional applications such as broadcast monitoring, security in communication, authentication and blind assessment of quality of services (QoS) for multimedia signals in mobile radio network. These applications essentially demand development of low cost algorithms so that they can be implemented on real time system through hardware realization. Hardware realization offers advantages over software realization in terms of less area, low execution time, low power, real-time performance, high reliability and also ease of integration with existing consumer electronics devices. This chapter first presents a brief review on hardware implementation of digital watermarking algorithms, followed by development of hardware architecture for spatial domain and fast Walsh transform (FWT) domain SS watermark system design using field programmable gate array (FPGA). A brief sketch on hardware implementation for biorthogonal wavelet based Hilbert transform is also shown that may be extended to design SS watermarking based on the concept of two previous architectures. Few challenges for hardware design of watermarking algorithms are then mentioned with an objective to give an idea how to develop watermarking algorithms so that it can be implemented on hardware. The chapter ends with few open research problems on hardware architecture as scope of future research work.

DOI: 10.4018/978-1-61520-903-3.ch018

INTRODUCTION

Recent years have witnessed a prolific growth in digital techniques as well as in wireless communication system. Two-fold advantages, namely (i) the wide use, ease of copying, manipulation and distribution of multimedia signals over Internet, and (ii) worldwide mobility between the transmission and the reception system have now been achieved. Today various wireless mobile communication services offer data transmission along with voice-based applications (Hanzo, 2001). Two classes of problems have also been emerged, namely (i) how to protect the ownership, authenticity, integrity and security of the transmitted digital data, and (ii) how to ensure end-to-end quality of the offered multimedia services in third or future generation mobile communication system [IMT2000/Universal Mobile Telecommunication System (UMTS)] (Li, 2001). Digital watermarking scheme, though originally developed as a potential solution for copyright protection and authentication of digital data (Voyatzis, 1999; Dittman, 1999; Fridrich, 2000) has also been attempted in recent times for some non-conventional applications such as broadcast monitoring, security in communication, authentication and blind assessment of quality of services (QoS) for multimedia signals in mobile radio network.

Spread spectrum (SS) watermarking has proven to be efficient, robust and cryptographically secure (Maity, 2007). Spread spectrum communication has two characteristics that are important to watermarking, namely (i) it may help in achieving high document-to-watermark ratio (DWR) leading to low distortion due to watermark insertion and (ii) it can also help to achieve robustness against forced removal of hidden data. The concept of spectrum spreading principle of digital communication is exploited to convert anti-jamming and interference rejection attributes in the form of robustness, which in turn suggests that SS watermarking can easily be

integrated with many existing data transmission schemes. This integration, in other way, demands development of several fragile SS watermarking methods suitable for various non-conventional applications such as broadcast monitoring, security in communication, authentication and blind assessment of quality of services (QoS) for multimedia signals in mobile radio network. Such fragile SS watermarking methods with low computation cost may provide facility of real time implementation through hardware realization. Hardware implementation of digital watermarking offers advantages over software realization in terms of less area, low execution time, low power, real-time performance, high reliability and also ease of integration with existing consumer electronic devices (Koulianou, 2009). The software designer does not have direct control over the way random access memory (RAM) and processors interact, posing a limit on speed. A software designer must try to limit the total amount of RAM required, while a hardware designer has full control over timing operations into the RAM and direct control over the usage of expensive hardware resources (Mathai, 2003).

Although software implementation may be appealing due to faster implementation, there are a few compelling reasons for a move toward hardware implementation. For example, in consumer devices adding the watermark component through hardware implementation is economically beneficial as it consumes small dedicated area of silicon. On the other hand, software implementation often requires dedicated processor such as a digital signal processing (DSP) core that occupies considerably more area, consumes significantly more power, and may still not perform adequately fast (Mathai, 2003). If a chip is fitted in the digital devices, the output video or images can be marked right at the origin, although the same can be done using software after those videos or images downloaded to the computer. But in this case embedding software will take more time

compared to hardware. The example of TV broadcast will highlight the significance where digital media is to be marked in real time and hardware is the only solution.

The chapter briefly reviews the state-of-the-art hardware implementation aspect of digital watermarking methods followed by the description of two different architectures for spatial and transform domain SS watermarking using field programmable gate array (FPGA). A brief description on hardware architecture for biorthogonal wavelet based Hilbert transform is then presented with an objective that readers may develop suitable hardware architecture for quadrature carrier multiplexing (QCM)-SS watermarking from the two previous architectures. The overall objective is to give an idea how to develop low cost watermarking algorithms along with their hardware design for real-time applications.

BACKGROUND

Review of Hardware Based Watermarking

Over the past decade, several watermarking algorithms for the multimedia signals have been proposed for software implementation. However, only a few hardware implementations are presented in the literature. A hardware based watermarking system can be designed on a field programmable gate array (FPGA) board (Maity, 2007), Trimedia processor board (Maes, 2000), digital signal processor, or custom integrated circuit (IC) (Mohanty, 2003). Recently, the graphics processing unit (GPU) has also been explored for hardware assisted real-time watermarking (Mohanty, 2007a).

Strycker et al. (Stryker, 2000) proposed the implementation of a real time spatial domain watermark embedder and detector on a Trimedia TM-1000 VLIW processor. Pseudorandom numbers, in

the form of watermarks, are added to the incoming video stream based on the luminance value of each frame, and watermark detection is based on the calculation of the correlation values. The authors in (Cheung, 2003) proposed a watermark-based protocol for the document management in large enterprises. Fan et al. (Fan, 2005) have proposed a visible watermarking design based on an adaptive discrete wavelet transform. Host image is decomposed into three level multiresolution structures and is divided into two sequences with the same pattern length. Two-path parallel processing architecture is exploited to reduce processing time and the signal is sent to different processing elements by the demultiplexers. The authors in (Mathai, 2003) proposed the video watermarking algorithms through the hardware implementations of a well-known algorithm called just another watermarking scheme (JAWS) with $0.18\mu m$ CMOS technology. Tsai and Lu (Tsai, 2001) have proposed a discrete cosine transform (DCT) domain invisible watermarking chip with TSMC $0.35\mu m$ technology and has a die size of $3.064 \times 3.064\text{ mm}^2$. Garimella et al. (Garimella, 2003) have proposed a very large scale integration (VLSI) architecture for invisible fragile watermarking in the spatial domain. The application specific integrated circuit (ASIC) is implemented using $0.13\mu m$ technology. The area of the chip is $3453 \times 3453\mu m^2$, and the chip consumes $37.6\mu W$ of power when operated at $1.2V$. The critical path delay of the circuit is 5.89 ns.

Mohanty et al. (Mohanty, 2005a) have proposed watermarking hardware architecture that can insert two visible watermarks in images in the spatial domain. This architecture can insert either of the two watermarks depending on the requirements of the user. The chip is implemented with $0.35\mu m$ technology and occupies an area of $3.34 \times 2.89\text{mm}^2$ and consumes $6.9286mW$ when operated at $3.3V$ and $292.27MHz$. Mohanty et al. (Mohanty, 2006) have also proposed another VLSI architecture that can insert invisible or vis-

ible watermarks in images in the DCT domain. A prototype VLSI chip has been designed and verified using various Cadence and Synopsis tools based on TSMC 0.25 μm technology with 1.4M transistors and 0.3 mW of average dynamic power. Mohanty et al (Mohanty, 2007b) develop low-power, high- performance, real-time, reliable and secure watermarking systems, which can be achieved through hardware implementations. They have discussed the development of a very-large-scale integration (VLSI) architecture for a high-performance watermarking chip that can perform both invisible robust and invisible fragile image watermarking in the spatial domain. They prototyped the watermarking chips in two ways: (i) by using a Xilinx field-programmable gate array (FPGA) and (ii) by building a custom integrated circuit.

Maity et al (Maity, 2005) develop an FPGA based hardware realization for a low bit modulation (LBM) based spatial domain image watermarking scheme that employs channel coding scheme for hiding a gray scale image like information within a gray scale cover image. Maity et al (Maity, 2004; Maity, 2009b) also develop an FPGA based hardware realization for image-in-image communication, which does not directly embed any watermark but provides security for data transmission through images. Ghosh et al (Ghosh, 2009) develop a FPGA based architecture for block based multiple bit spatial domain spread spectrum image watermarking scheme where a gray scale watermark image is represented by less number of binary digits using novel channel coding and spatial biphasic modulation principle. Maity et al (Maity, 2007b; Maity, 2009a) also develop an FPGA based architecture for block based multiple bit SS watermark embedding using Fast Walsh transform. The algorithm serves the dual purposes of authentication in data transmission as well as QoS assessment for digital media through dynamic estimation of the wireless channel condition. Fast Walsh transform offers low computation cost for

implementation, smaller change in image (multi-media signal) information due to data embedding and ease of hardware realization (Maity, 2009c). A comparative performance results for the state-of-the art image and video signal watermarking chips is reported in Table 1.

There are very few hardware architecture implementations for watermarking available using FPGA boards. The choice between FPGA and cell based IC is a trade-off between cost, power consumption and performance. Hardware implementation using FPGA offers advantages of low investment cost, simpler design cycle, field programmability/re-configurability and desktop testing with moderate processing Speed (Maity, 2004)). On the other hand, due to lower unit cost, full custom capability and from an integration point of view custom based ASIC design may be more useful. The FPGA design flow eliminates the complex and time-consuming floor planning, place and route, timing analysis, and mask/respin stages of the project since the design logic is already synthesized to be placed onto an already verified and characterized FPGA device. During recent past, FPGAs were used to be selected for lower speed/ complexity/volume designs, but today's FPGAs easily push the 500 MHz performance barrier. With unprecedented logic density increases and a host of the features, such as embedded processors, digital signal processing (DSP) blocks, clocking, and high-speed serial at ever lower price points, FPGAs are a compelling proposition for almost any type of design. Moreover, the other limitation with the most of the existing watermarking hardware design is that they do not consider watermarking based on spread spectrum (SS) modulation which is not only efficient, robust and cryptographically secure but also can be integrated with the existing data transmission schemes. We now present a brief introduction on theory and characteristics of SS watermarking followed by special requirements for such technique on hardware design and associated complexity.

Table 1. Image and Video watermarking hardware proposed in the current literature

Research work	Design Type	Watermarking Type	Multimedia Object	Working domain	Chip statistics
(Girimella, 2003)	Custom IC	Invisible Fragile	Image	Spatial	0.13µm, 3453x 3453 mm ² , 1.2 V, 37.6 µW
(Girimella, 2004)	Custom IC	Invisible Fragile	Image	Spatial	0.13µm, 545 µm x 525 µm, 1.14 V, 166.6 MHz, 9.19 mW
(Mohanty, 2003; 2007b)	Custom IC	Invisible Robust/Fragile	Image	Spatial	0.35µ, 3.3 V, 545 MHz, 2.0547 mW
(Mohanty, 2004a)	FPGA board	Invisible Robust	Image	Spatial	Xilinx, Virtex, XCV50-BG256-6, 50.398 MHz
(Mohanty, 2004b; 2005a)	Custom IC	Visible	Image	Spatial	0.35µm, 3.34 x 2.89 mm ² , 3.3V, 292 MHz, 6.93 mW
(Nelson, 2005)	Custom IC	Invisible Robust	Image	Spatial	0.18µ, 1.8 V/3.3 V, 1122 µm x 1302 µm
(Lukac, 2005)	Custom IC	Visible/ Robust	Image	Spatial	NA
(Tsai, 2001)	Custom IC	Invisible Robust	Image	DCT	0.35µm, 3.064 x 3.064 mm ² , 3.3V, 50 MHz, 62.78 mW
(Mohanty, 2005b; 2006)	Custom IC	Invisible Robust, visible	Image	DCT	0.25µ, 16.2 mm ² , 1.5 V, 2.5 70, 280 MHz, 0.3 mW
(Mohanty, 2007a)	GPU	Invisible/Robust	Image	DCT	NA
(Hsiao, 2000a; 2000b)	Custom IC	Invisible/Robust	Image	Wavelet	NA
(Seo, 2003)	FPGA board	Invisible Robust	Image	Wavelet	82 MHz, 4037 LABs, 85 ESBs Altera APEX20KC
(Maity, 2005)	FPGA Board	Invisible Semi-fragile	Image	Spatial	XCS05, XCS05L, 95 CLBs
(Maity, 2007b; 2009)	FPGA Board	Invisible Robust/Semi-fragile	Image	FWT	XCS40, XCS40L, 730 CLB, 80 MHz
(Ghosh, 2009)	FPGA board	Invisible, fragile	Image	Spatial	xc4vlx25-10ff676, Max. Freq.219.542MHz, Delay: 103.346ns
(Strycker 2000; 1999)	DSP board	Invisible Robust	Video	Spatial Fourier	100 MHz
(Maes, 2000)	FPGA Board Custom IC	Invisible Robust		Spatial Fourier	17 KG Logic 14 KG Logic
(Tsai, 2003)	Custom IC	Invisible-Robust	Video	Spatial	NA
(Brunton, 2005)	GPU	Invisible Fragile	Video	Spatial	NA
(Mathai, 2003b)	Custom IC	Invisible Robust	Video	Wavelet	0.18 µ, 3.5 mm ² , 1.8V, 75MHz, 160mW
(Petitjean, 2002)	FPGA Board, DSP processor	Invisible Robust	Image Video	Fractal	50 MHz takes 6 µsec 250 MHz takes 118 µsec

Theory of Spread Spectrum Watermarking

The most interesting property of direct sequence (DS) SS watermarking technique lies in spreading effect of narrow band watermarks over many

frequency bins of the host image so that the energy of the embedded data in any given bin is very small and could hardly be detected. The efficiency of data spreading lies on the choice of transform for image decomposition and some specific properties of the spreading codes. Since

the SS watermarking methods for the applications mentioned here demand multiple bits embedding, we present briefly multiple bit SS watermark embedding and decoding here.

Let the symbol B denotes the binary valued watermark bit string as a sequence of M bits.

$$B = \{b_1, b_2, b_3, \dots, b_M\}, b_i \in \{1, 0\}$$

Let the symbol x denotes the original signal i.e. vector of length N in original domain or transform coefficients. A binary valued code pattern i.e. “chip sequence” u of length N with zero mean and whose elements are equal to $+\sigma_u$ or $-\sigma_u$, is used to spread each watermark bit. Thus a set P of M code patterns, each of length N , are generated to form the spread watermark sequence u_Q by performing the following operation

$$u_Q = \sum_{j=1}^m b_j \cdot u_j \quad (1)$$

The sequence u_j is added to or subtracted from x according to the variable $b_j \in \{1, 0\}$, mapped to +1 or -1. The watermarked signal s can be written as

$$s = x + \alpha u_Q = x \pm \alpha \sum_{j=1}^M b_j u_j \quad (2)$$

The above form is additive multiple bit SS watermarking, where α is the gain factor or modulation index and its proper choice will optimize the maximum amount of allowed distortion and the minimum watermark energy needed for reliable detection (Maity, 2007a). SS watermarking schemes can be called as signal adaptive or non-adaptive whether α is a function of original signal or not. The value of α may be positive or negative, integer or real and may vary continuously thus giving rise to the scope of setting embedding distortion to any desired value.

In SS watermarking, the detection reliability for the binary valued watermark data depends on the decision variable r_i obtained by evaluating the zero-lag spatial cross-covariance function between the watermarked signal s and each code pattern u_i . The decision statistics RI can be mathematically written as

$$r_i = \langle u_i - m_1(u_i), s - m_1(s) \rangle > (0) \quad (3)$$

where $m_1(L)$ represents the average of the sequence L . If the code patterns u_i are chosen so that $m_1(u_i) = 0$ for all i , the computation of r_i becomes;

$$\begin{aligned} r_i &= \langle u_i, [s + \alpha \sum_{j=1}^M b_j u_j - m_1(s)] \rangle \\ &= \langle u_i, s \rangle + \alpha \sum_{j=1}^N b_j \langle u_i, u_j \rangle - \langle u_i, m_1(s) \rangle \\ &= \langle u_i, s \rangle \end{aligned} \quad (4)$$

The first and the second terms in equation (4) represent the host signal interference (HSI) and multiple bit interference (MBI), respectively.

The i -th embedded bit is detected as follows:

$$\hat{b}_i = \text{sgn}(r_i) = \text{sgn}(\langle u_i, [s + \alpha \sum_{j=1}^M b_j u_j] \rangle > (0)) \quad (5)$$

where sgn represents signum function and acts as a hard detector. The bit b_i is detected as **0** if $r_i > 0$ and as **1** otherwise.

Equation (5), which results from equation (3) and improvement in detection reliability under multiple bit embedding show that the codes should satisfy the following properties (Maity, 2007a).

1. The code patterns u_i , $i=1,2,\dots, M$, should be distinct sequences with zero average.

2. The spatial correlations $\langle u_p, u_j \rangle, j \neq i$ should be minimum. Ideally, sequences u_i and u_j should be orthogonal whenever $j \neq i$.
3. If image prediction (for estimating the image distortion) is not used before evaluating the cross-correlation, it is desirable that u_i 's (for $i=1,2,\dots,M$) should be uncorrelated with the image block I .
4. Spatial correlation $\alpha. \langle u_p, b_i u_j \rangle$ should be maximized, although detection reliability and image distortion must be properly trade-off.

Pseudo random or pseudo noise (PN) sequences satisfy property (1) and (2) if only infinite length sequence is considered which is not feasible for practical image processing operations. Mayer et al. (Mayer, 2002) showed that robustness is improved for small size image block if spreading codes are generated from Hadamard basis and by Gram-Schmidt orthogonalization of pseudo random sequences. But under this circumstance the following problems may arise: (1) unauthorized decoding and possible removal of the embedded data due to the deterministic nature of Hadamard basis; (2) Better spectrum spreading is not possible for small size image block. SS watermarking techniques that may be developed to solve this problem is to modulate the code patterns using Hadamard basis function. Each PN code is exclusive-ORed with a row of Hadamard matrix of proper dimension. Property (3) can be satisfied provided the cover signal is properly decomposed so that it yields low correlation with the code patterns. Property (4) is satisfied by the choice of the value of embedding strength.

The reliability of bit detection in equation (5) is good when the effect of HSI and MBI become zero. The last term becomes zero for zero rate i.e. single bit embedding. In the context of multiple bit embedding, when cross correlation values among the code patterns are non-zero, the detection reliability suffers significantly. The detection

reliability can be improved too some extent if the integration operation at the decoder is done for a longer duration leading to a better threshold value. In the context of SS watermark decoding, in other words, a better stable threshold value 'T' can be determined by taking average for r_i values. The decision statistics r_i are then compared with respect to 'T'.

Special Requirements of Hardware Design And Complexity

Spread spectrum watermarking algorithms use random number or pseudo random number as spreading code. Designing of low power random number generators and reliable storage of random number keys in hardware is a design challenge (Kougianos, 2009). To tackle the problem, the commonly used hardware architecture for the generation of pseudo random numbers is the linear feedback shift register (LFSR). This is a sequential circuit with combinational feedback logic. It is essential to ensure that LFSR will not be getting stuck in the prohibited state and it would be eliminated.

Design of imperceptible and robust watermarking essentially demands decomposition of cover or original signal to obtain efficient watermark embedding space. Most of the widely used transforms for compression, like discrete cosine transform (DCT) and wavelet involve computationally expensive convolution operations during forward and inverse transform due to floating point kernel. It is challenging to implement floating-point operations for hardware design. Moreover, single hardware block may not be useful for the forward and the inverse operations as the kernels are different for most of the widely used transforms. From that perspective, Walsh transform is a preferable choice than commonly used DCT as floating point addition-multiplication operations are not required when the digital image or video signal is convolved with the signed integer valued

kernel during the forward and the inverse Walsh transform. Moreover, the kernel of one hardware block is sufficient to implement both forward and inverse transform, which is not possible in DCT based algorithm.

To remove the effect of HSI, the original signal is required at the decoder. The storage of original signal increases on-chip memory requirement. Increase in memory size increases power consumption and cost of the chip. Blind watermark decoding is preferable than non-blind one which is other important requirement for hardware design. For multiple bits watermark embedding, the correlation calculation for each bit followed by calculation of overall threshold further complicate the hardware design. The division and the multiplicative operations in watermarking algorithms consume much power compared to the addition and the subtraction operations, which in turn suggests to preferably select a watermarking algorithm with addition/subtraction operations more than division/multiplication operations. Minimum number of pipeline or parallel architecture is essential for the implementation of a watermarking algorithm, as such architecture consumes large amount of both leakage current and dynamic power. The value of α , *embedding strength*, may be positive or negative, integer or real; but the last one is desirable for imperceptible watermark design. However, the real value of α involves high computation cost leading to a problem in hardware design. So the value of α may be chosen as integers to simplify hardware design at the cost of imperceptibility. The rational α value may be the preferable choice in order to implement in hardware using simple shift-and-add operations.

We now describe hardware implementation of a spatial domain and transform domain SS watermarking algorithm using field programmable gate array (FPGA). VLSI architecture of biorthogonal wavelet based Hilbert transform is then briefly presented which can be extended for QCM-SS watermarking for payload improvement.

VLSI ARCHITECTURE OF SPATIAL DOMAIN SPREAD SPECTRUM WATERMARKING

Sometimes it is required to authenticate sender of the message or message itself. Fragile digital watermarking method intended for communication of hidden data may be used to serve the purposes. Ghosh et al (Ghosh, 2009) develop a block based multiple bit spatial domain spread spectrum image watermarking scheme. Gray scale image like information may be used as watermark, which may be used as sender information or message information. However, it is relatively difficult to develop a low cost hardware implementable watermarking architecture where a gray scale watermark image is embedded in a gray scale cover image. The difficulty of embedding a gray scale watermark image in a gray scale cover image may be solved by converting the former to a binary equivalent form and then embedding of this intermediate binary watermark using SS method. A novel method is proposed first where a gray scale watermark image is represented by less number of binary digits using novel channel coding and spatial bi-phase modulation principle. The hardware architecture of image watermarking algorithm may be applied for authentication as well as secured communication in real time environment. The algorithm is described first and then its VLSI architecture using FPGA is presented (Ghosh, 2009).

Watermarking Algorithm

A gray scale image like watermark information is converted into an equivalent binary watermark using channel coding and spatial biphasic modulation. The binary watermark is then embedded directly to the pixel values of each block of the host image using SS modulation. During decoding, watermark information is extracted using correlator and the extracted binary watermark is then converted to

the grayscale image using channel decoding and spatial bipahse demodulation.

Message Encoding and Watermark Embedding

Step 1: Binary Message Formation

The cover/host image (I) is divided into $k_1 \times k_1$ non-overlapping blocks where the value of k_1 may be 2, 4, 8, 16 etc. The most significant bit (MSB) plane of 2-D pixel values of each block are converted to 1-D string and are concatenated to form a large string of pixel values (string 1). Another binary string is formed using the different bit plane values of the gray-scale watermark image. An extended binary string (string 2) is made by incorporating different degree of redundancy (repeating by suitable odd number of times) among the various bits based on their relative significance. String 1 and String 2 are partitioned into sub strings of equal and fixed number of symbols. If there occurs more than 50% positional match of the symbols in the two respective sub strings of String 1 and String 2, a bit ‘1’ is assigned for the sub string, otherwise bit ‘0’. Bit ‘1’ indicates in-phase condition of two sub strings, while out of phase condition is denoted by bit ‘0’. Assigning a binary digit corresponding to each substring of particular number of symbols is called here as spatial biphasic modulation technique. The newly obtained binary string is the derived watermark to be embedded in the host signal.

Step 2: Watermark Embedding & Formation of Watermarked Image

It is preferable to use antipodal signaling scheme for data embedding in order to increase robustness performance. So, the data-embedding rule can be expressed as follows:

$$s = x \pm k \sum_i u_i \quad (6)$$

Where x is the pixel value of the cover image, s is the pixel value of the watermarked image, k is

the modulation index, u_i is the pseudo noise (PN) matrix corresponding to the watermark bit $b_i \in \{1, 0\}$, ‘±’ indicates antipodal data embedding and $i=1, 2, \dots, M$.

Watermark Dehiding and Message Decoding

The watermark recovery process requires the sets of PN matrices (u_i) that were used for data embedding. Different steps for watermark decoding are described as follows:

Step 1: Correlation Calculation

Correlation values between the watermarked image matrix and each code pattern of the set (u_i) are calculated. We have a total of M (equal to the number of watermark bits) correlation values (μ_i) where $i=1, 2, \dots, M$.

The decision rule for the decoded watermark bit is as follows:

If $\mu_i \geq 0$, the extracted bit is ‘0’, otherwise the extracted bit is ‘1’.

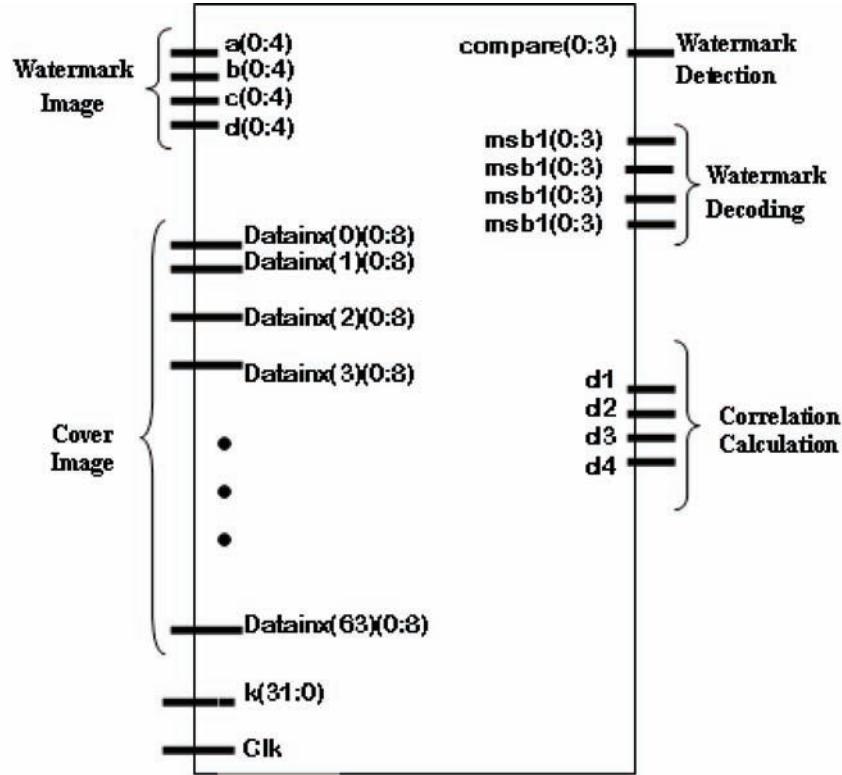
Step 2: Substring Decoding

MSB planes of the watermarked image or its distorted version is picked up in the same way as was used for binary message formation and are partitioned into substrings of fixed and equal number of bits. Biphasic demodulation scheme is used in this stage. Based on the value of a binary digit in the decoded watermark, the substring either remains unchanged (if detected bit is ‘1’) or complemented (if detected bit is ‘0’).

Step 3: Message Decoding

Each substring obtained is then partitioned into sub substrings (smaller substrings) according to the rules used during watermark embedding. Binary detection is then applied for each sub substring based on the majority decision rule i.e. if more than 50% symbols are ‘1’ in a sub substring, decision for decoding is ‘1’, otherwise ‘0’. The binary

Figure 1. Top-Level RTL schematic



digit of all the sub substrings of a substring are then converted to the pixel values and gray scale watermark image is decoded.

Digital Design of Proposed Method

The synthesis of both the watermark embedding and decoding have been implemented on Xilinx (ISE version 8.2i) based FPGA. Virtex series of FPGA is chosen to fit the complexities of the design. The device used is xc4vlx25-10ff676 for the implementation and the language used is Verilog hardware description language (VHDL). The behavioral simulation was done with Modelsim XE III 6.1e to verify the functionality of the design. A testbench was also written in VHDL to give the input vectors for the simulated program. Figure 1 shows the top-level RTL schematic.

Digital Design of Watermark Embedding

The VLSI design is made here for the cover image of size (256 x 256) with 8 bits per pixel. On the other hand, the watermark image size taken was (64 x 64), with 4 bits per pixel. Now, the cover image is partitioned in (8 x 8) non-overlapping blocks and the watermark image in (2 x 2) non-overlapping blocks. Say, the partitioned watermark images are a, b, c, d as shown in Figure 1. The partitioning of the cover and the watermark image followed by the conversion of the integer image data to binary was done with the help of MATLAB. With the binary image data for both the partitioned cover and the partitioned watermark image, we put them in the test bench as input cover and input watermark image. The partitioned cover and the watermark image data in binary form are padded with 0 in the sign bit to represent the signed image

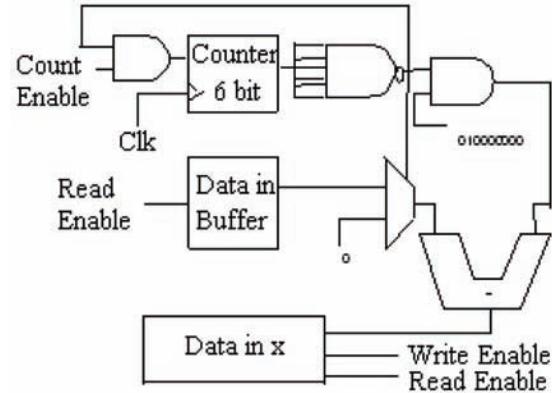
data. So, 8 bit/pixel gray scale cover image is now represented by 9 bits and 4 bits/pixel grayscale watermark image is represented by 5 bits. Then preprocessing is done for the pixel values of the cover image by subtracting 128 from each gray value and the circuit is shown in Figure 2. The operation enables the input sample data to obtain a nominal dynamic range centered about zero. This pre-processing operation not only prevents numerical overflow but also makes arithmetic coding, context specification etc. simpler. The corresponding redundancy addition to the respective bit plane of each pixel value for the watermark image is done through combination of D-flip-flops. The generation of pseudo noise (PN) code using linear feedback shift register (LFSR) is done using S-R flip flops and X-OR gates and is shown in Figure 3. Figure 4 shows the required circuits for watermark embedding.

Figure 4(a) takes cover image's pixel values as input and String 1 is formed from the MSB plane. Figure 4(b) shows the required circuit for the generation of four pseudo noise (PN) code patterns shown as 1, 2, 3, and 4. The four PN code patterns are used to embed four binary watermark bit patterns. Watermark image is fed to a, b, c, and d input terminals of addition of redundancy unit in Figure 4(c). Each one of a, b, c, and d terminal takes 4 bit data and generates outputs in ax, bx, cx, and dx where each one of the latter is of 16 bits length. Thus String 2 is formed. String 1 and String 2 are fed to an X-OR gate to generate bit '1' or '0' which are stored in D-flip flop. The counter counts number of '0' and '1' in the string and implements the spatial biphasic modulation. Finally, Figure 4(d) implements the actual data embedding operation using multiplication and addition/subtraction operation.

Digital Design of Watermark Decoding

Watermark decoding is accomplished by calculating the correlation values between the watermarked image block and respective LFSR output

Figure 2. Preprocessing circuit



matrices. The detailed circuit for correlation calculation is shown in Figure 5, yx_1 shown in the figure represents the LFSR output matrix coefficients. Similarly, block Embed x buffer shown in figure represents elements of embedded matrix. Blocks A, B and C shown in this figure represent the hardware for necessary multiplication and addition for correlation calculation. Block F indicates the accumulated sum for the correlation values and its output is divided by 64 (shown in G) to obtain normalized correlation value.

The behavioral simulation is done in Modelsim XE III 6.1e. The synthesis result is shown in Table 2. The minimum clock period is 4.555ns (Maximum Frequency: 219.542MHz). Maximum output required time after clock is 102.195ns. Maximum combinational path delay: 103.346ns.

VLSI ARCHITECTURE OF FWT BASED SS WATERMARKING

Transform domain methods become appealing to design robust and imperceptible watermarking system. Discrete cosine transform (DCT) and wavelet transforms become popular as the most common image compression techniques e.g. JPEG and JPEG 2000 are either based on DCT or wavelet. However, it is shown in (Maity, 2009a) that fast Walsh transform (FWT) offers low computation

Figure 3. PN code generator using LFSR

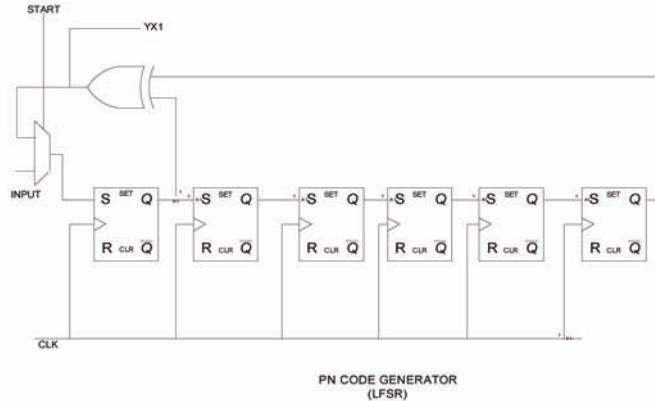
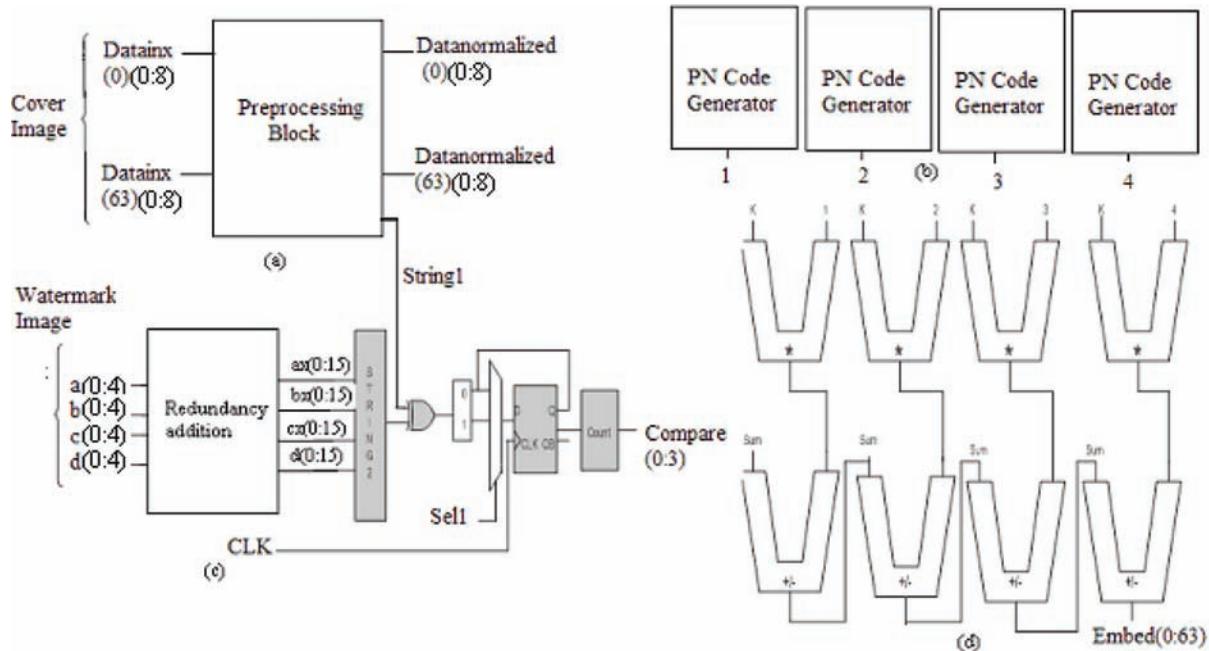


Figure 4. Circuit of watermark embedding block



cost as floating point addition-multiplication is not required when the digital image is convolved with the signed integer valued kernel during the forward and the inverse Walsh transform (Ho, 2003). Walsh transform shows an ascending of sequence analogous to Fourier transform and unlike random sequence of Hadamard transform (Ho, 2003). This provides the benefit of Walsh transform computation using fast algorithm, which

is identical to the fast Fourier transform (FFT) leading to the efficient hardware realization. The kernel of Walsh transformation being symmetric matrix with orthogonal rows and columns, the same algorithm can be used for both the 2-D forward and inverse Walsh transforms without modification. Hence, only one hardware block is sufficient to implement both forward and inverse transform, which is not possible in DCT based

Figure 5. Correlation calculation

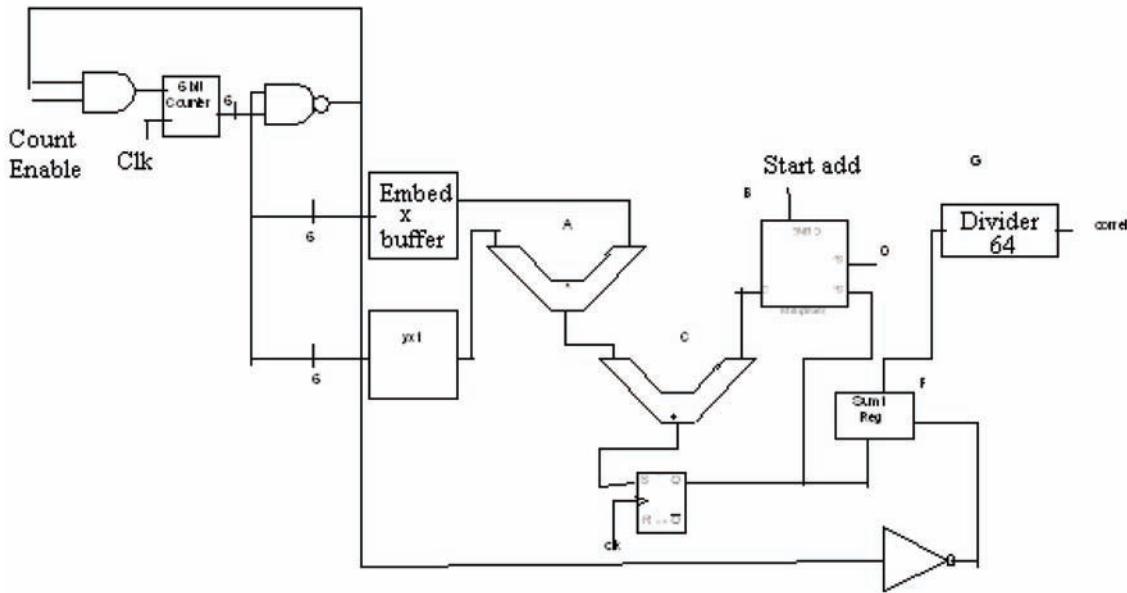


Table 2. Synthesis results from Xilinx ISE 8.2i

Logic Utilization	Used	Available	Utilization
Number of Slices	11536	10752	107%
Number of Slice Flip-Flops	296	21504	1%
Number of 4 input LUTs	21692	21504	100%
Number of bonded IOBs	649	448	144%
Number of GCLKs	2	32	6%

algorithm. It is also shown mathematically that data embedding process causes less change in image information when FWT is used as embedding domain compared to DCT as the former has two valued kernel while the latter has multivalued kernel (Maity, 2009c). Moreover, the wide usage of Walsh codes for implementation of CDMA in wireless communication makes Walsh transform more attractive for the development of SS watermarking integrated with the existing SS modulation techniques.

VLSI architecture of fast Walsh transform (FWT) based SS watermarking is now presented which can simultaneously serve the dual purposes of authentication and QoS assessment of multi-

media mobile communication services (Maity, 2009a). The proposed watermarking algorithm directly embeds a binary watermark on each (8 x 8) image block after decomposition using fast Walsh transform. The inverse Walsh transform is then done to obtain watermarked image. To improve detection reliability, watermark-decoding algorithm is made little different from the spatial domain algorithm and is described as follows.

Step 1: Watermarked Image Decomposition
The received watermarked image is partitioned into (8 x 8) non-overlapping blocks and is decomposed using fast Walsh transform.

Step 2: Correlation Calculation

Correlation values between Walsh coefficients matrix and each code pattern of the set (u_i) are calculated. We have a total of M (equal to the number of watermark bits) correlation values ‘ μ_i ’ where $i=1,2,\dots,M$.

Step 3: Mean Correlation Calculation and Threshold Selection

We calculate the mean correlation value (T) from these correlation values. This mean correlation value is used as the threshold or decision variable for binary watermark decoding. The decision rule for the decoded watermark bit is as follows:

1. for $\mu_i \geq T$, the extracted bit is ‘0’
2. for $\mu_i < T$, the extracted bit is ‘1’.

VLSI Design

The VLSI architecture of the proposed algorithm is designed using XILINX SPARTAN series FPGA. There are two main subblocks, one is the watermark-embedding unit and the other one is the watermark-decoding unit. The overall function of the watermark embedding unit is to decompose the image signal using Walsh transform and then embedding the watermark while the decoding unit decodes the embedded watermark. We develop here the architecture for the gray scale cover image of block size (8 x 8), 8-bits/pixels. The watermark consists of 4 bits binary pattern of 0101 and is embedded in this (8 x 8) image block.

Architecture for Watermark Embedding Unit

The VLSI architecture of the embedding unit for the proposed algorithm is shown in Figure 6. Hardware design consists of four subblocks or modules, namely: (1) Walsh transform module, (2) code generation module, (3) data embedding module, and (4) inverse Walsh transform module. Data i.e. pixel values of the cover image is fed to

the input pin G [15:0] of Walsh transform block with the clock C1. The MUX with control input M4 allows the resultant spreading code to be added with Walsh coefficients at desired time. The output from the adder is fed to the G [15:0] input pin of inverse Walsh transform block. Watermarked output is obtained at the output pin of this block. The other MUXs allow the various signals to flow into the inverse transform block at the desired time. The detailed architecture of each subblock is described below.

(1) Walsh Transform Module

Walsh transform is computed using fast algorithm given below which is nearly identical to the FFT (fast Fourier transform).

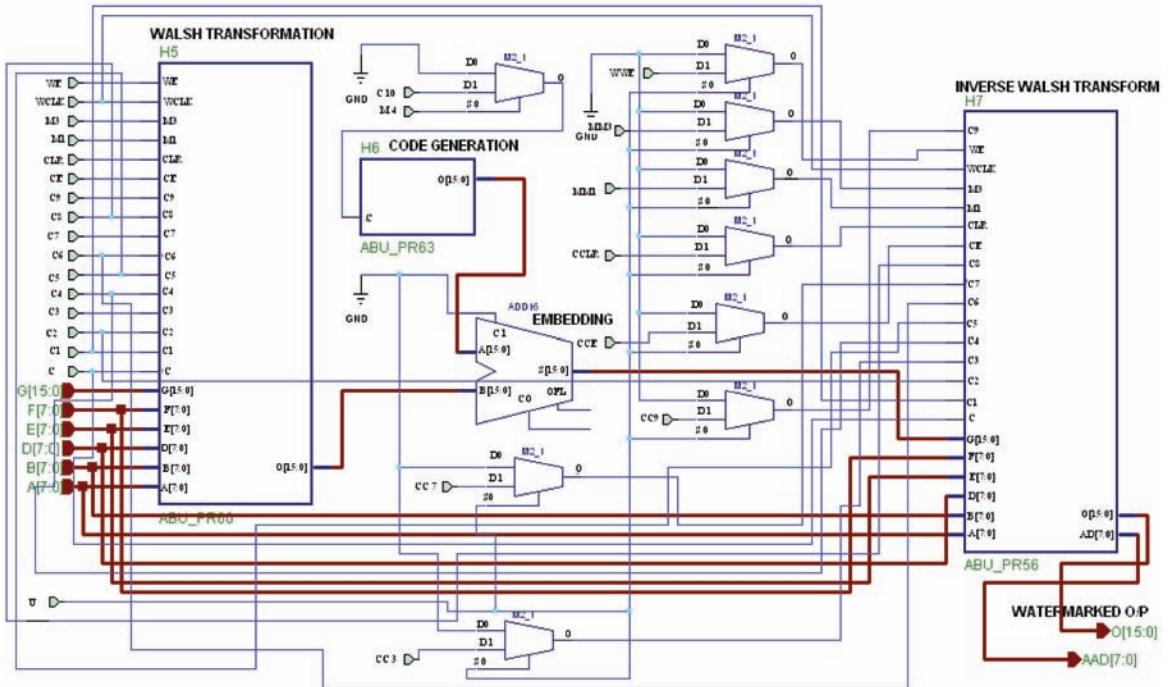
Subroutine for computing FWT is described as follows:

```

SUBROUTINE FWT (F, LN) .....01
REAL F [64], T... 02
N = 2LN...03
NV2 = N/2...04
NM1 = N - 1...05
J = 1...06
DO 3 I =1; NM1...07
IF (I ≥ J) GO TO 1...08
T = F(J)...09
F(J)=F(I)...10
F(I) = T...11
1 K = NV2...12
2 IF (K ≥ J) GO TO 3...13
J = J - K...14
K = K/2...15
GO TO 2...16
3 J=J+K...17
DO 5 L = 1, LN...18
LE =2L...19
LE1 =LE/2...20
DO 5 J = 1, LE1...21
DO 4 I = J, N, LE...22
IP = I + LE1...23
T = F(IP)...24
F(IP) = F(I)-T...25

```

Figure 6. VLSI architecture of watermark embedding unit



```

4 F(I) = F(I)+T...26
5 CONTINUE...27
DO 6 I = 1, N...28
6 F(I) = F(I)/FLOAT(N)...29
RETURN...30
END...31

```

Figure 7 shows the detailed hardware architecture of Walsh transform for an image block of size (8 x 8). In this algorithm, statements 03 through 05 are concerned with the initialization of the subroutine. Statements 07 through 17 accomplish bit reversal sorting. The hardware requirement to implement the bit reversal sorting using this algorithm is complex. The said function is implemented here using bit reversal block and WT2 block (RAM). The bit reversal block generates reversed addresses. At first C9 input of MUX-1 and C3 input of MUX-2 is kept high and low, respectively to allow the bit-reversed addresses to be fed to the address pins of the WT2 block.

WT2 is a 16-bit RAM with 96 locations out of which 64 locations are used here. The input data is fed to the input pin G[15:0] with the clock C1. The C7 input of MUX-5 is kept high to allow the original input data to be fed to the WT2 block. So the data are stored in RAM in a bit reversed order. The WT1 block generates the sequences of I and IP as given in statements 22 and 23. The detailed architecture of WT1 block is shown in Figure 8.

The outputs of WT1 block are fed into the MUX-3 with control input C2. Proper sequences of IP and I, which help to perform the statements 24 through 26, are obtained by applying proper state to the C2 input. The C3 input of MUX-2 is kept high to allow these address sequences to be fed into the address pins of RAM. The operations specified by the statements 24 through 26 are performed as follows: RAM is read from two locations specified by the addresses I and IP in two consecutive clocks of WCLK input pin of WT2. The values so obtained are added and subtracted.

Figure 7. VLSI architecture of Walsh transform

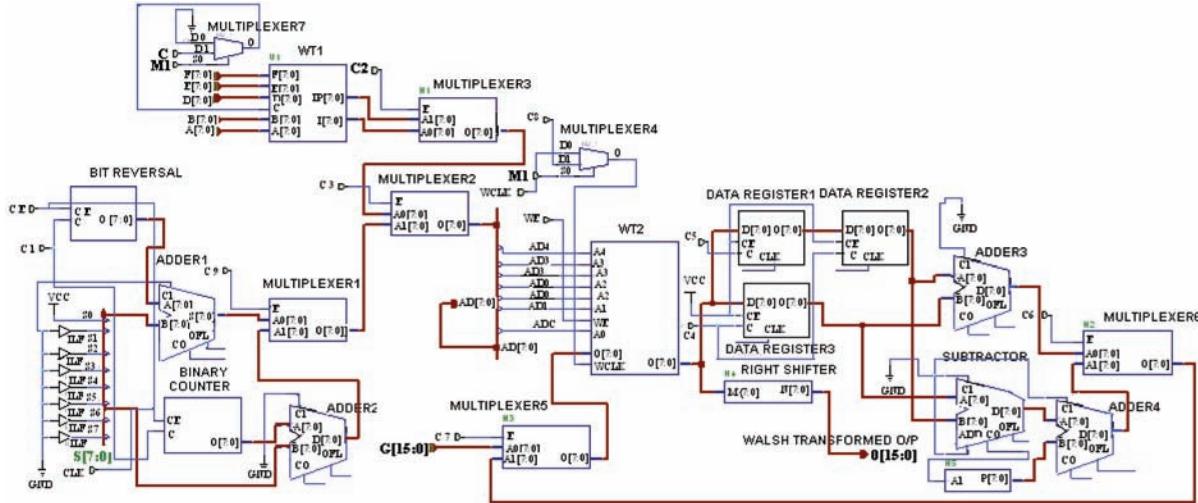
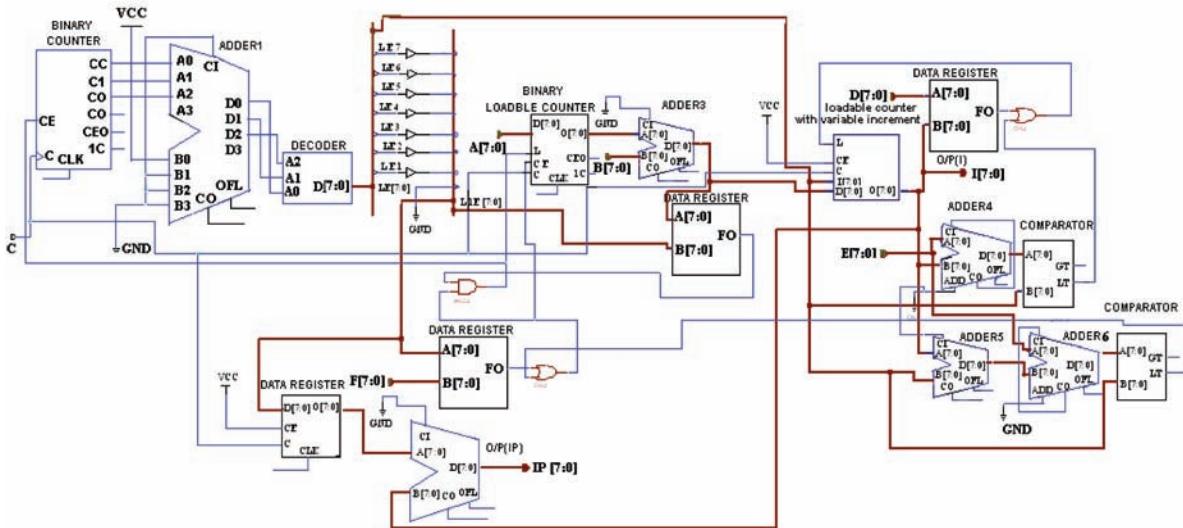


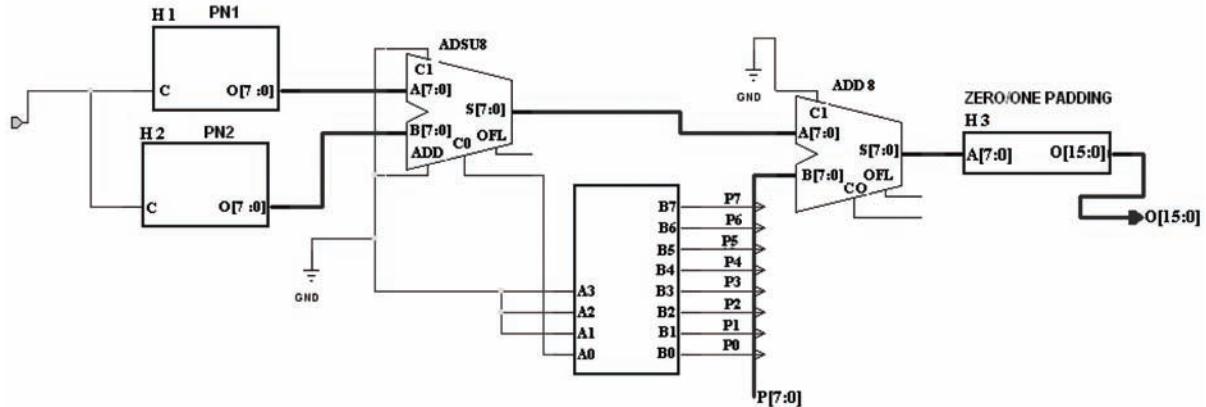
Figure 8. VLSI architecture of WT1



The results of addition and subtraction are stored back into the RAM in locations specified by I and IP, respectively. The complete operations are done using 3 data register, adder 3, subtractor, adder 4, MUX-5 and MUX-6. The read and write operation of RAM is controlled by WE (write enable) input. Finally, the output of the binary counter

passes through the MUX-1 and MUX-2 to the address pins of RAM at desired time. The data are read from RAM using these addresses. The output data of RAM is passed through the right shifter to perform the operation of statement 29. Walsh coefficients are obtained at the output pin of the right shifter. The required components for

Figure 9. VLSI Architecture of Code Generation and Spread Spectrum



Walsh transform module are two 1-bit MUX (2:1), five 8 bit MUX (2:1), four 8 bit adder, one 8 bit subtractor, one 8 bit binary counter, three 8 bit data registers, one right shifter, one bit reversal unit, one WT1 block, and one WT2 block.

(2) Code Generation Module

VLSI architecture of spreading code generation unit consists of the two major sub blocks, PN1 and PN2 blocks. Each block generates two set pseudo noise (PN) sequences of length 64. These PN sequences are added and are obtained at the output of each block. The outputs of PN1 and PN2 blocks are subtracted and the result is passed through a zero/one padding unit. The resultant PN sequence is obtained at the output of padding unit. Figure 9 shows code generation and spread watermark unit.

(3) Data Embedding Module

The output from code generation unit is added with the output from Walsh transform unit to obtain coefficients of the embedded data.

(4) Inverse Walsh transform module

The kernel of forward and inverse Walsh transform is identical. So the hardware requirements for performing both the operations are also the same

except an extra right shifter block that performs the division operation.

Architecture for Watermark Decoding Unit

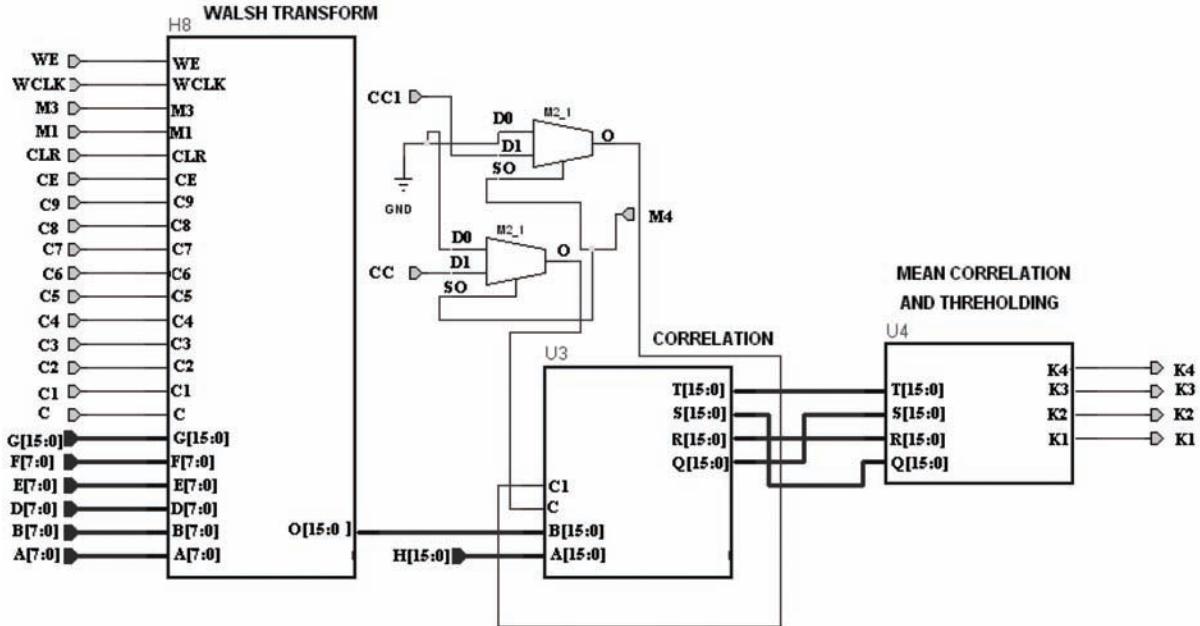
The VLSI architecture of watermark decoding is shown in Figure 10. The major sub blocks are: (1) Walsh transform module, (2) correlation calculation module, and (3) mean correlation and threshold calculation module.

Watermarked data is fed to the input pin G[15:0] of the Walsh transform block. The output of this block is passed through the correlation calculation block. The function of the correlation calculation block is to calculate the correlation between the spreading functions and Walsh coefficients block. Then the correlation values are passed through a mean correlation and threshold calculation block. At the output of the block, the message bits are detected.

(1) Walsh Transform Module

Walsh transform is applied to the watermarked image block. Theory and hardware architecture of this unit is exactly identical as described in watermark embedding section.

Figure 10. VLSI architecture of watermark decoding



(2) Correlation Calculation Module

The detailed hardware architecture of the correlation calculation block is shown in Figure 11. The same code generation units PN1 and PN2 used at watermark embedding unit are also used here. Input A[15:0] is set to zero. The Walsh coefficients are applied to the input pin B[15:0] with the clock C. The PN sequences coming from PN1 and PN2 are applied to the control input of MUXs. If the element of the code matrix is “1”, it allows the value of B [15:0] to pass through MUXs. On the other hand, if the element of the code matrix is “0”, it allows the value of A [15:0] to pass through MUXs. The outputs of the MUXs are fed to the one input of the adders unit. The outputs of the adders are fed to the data registers and outputs of the data register are fed back to the other inputs of the adders. Applying proper state sequence to C1, the correlation values Q [15:0], R [15:0], S [15:0] and T [15:0] are calculated. The required components of this unit are four MUXs (16 bit)-

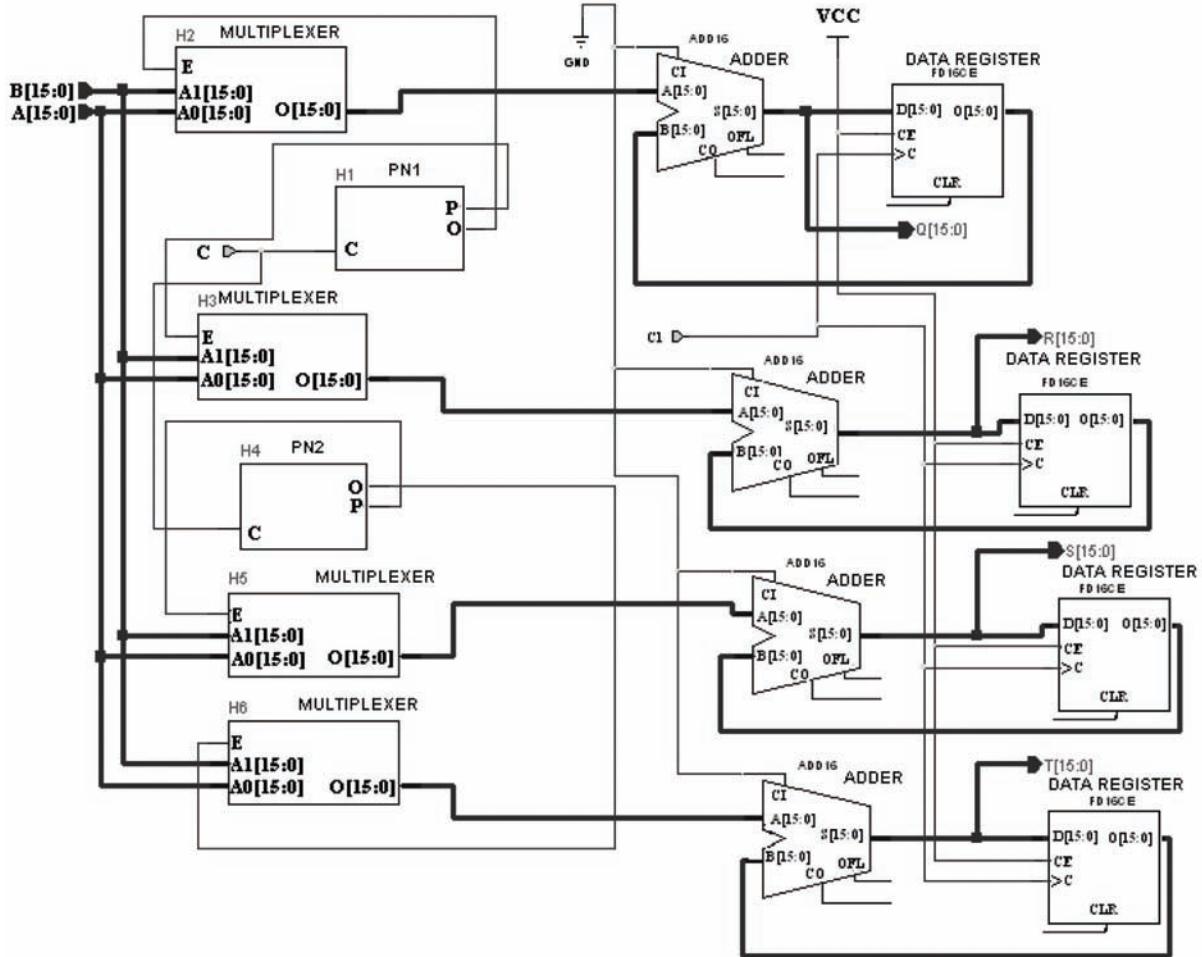
2:1, 4-adders (16 bit), 4 data registers (16 bit), PN1 and PN2 units.

(3) Mean Correlation and Threshold Calculation Module

The detailed architecture for mean correlation and threshold calculation is shown in Figure 12. The four correlation values are added using three adders. The result of addition is passed through a right shifter to obtain the mean correlation value. The output of the right shifter block is fed to the one input of each comparator. The other input of the comparators is the correlation values. Message bits are detected at the output of the comparator. The required hardware for this unit is three adders-16 bit, one right shifter, and four magnitude comparators-16 bit.

The running watermarking is updated with arrival of new sample i.e. after the completion of previous watermark decoding and each updating requires 86 clock cycles for (8 x 8) image block. This total clock cycle requirement includes 4-wa-

Figure 11. VLSI architecture of correlation calculation



termark bit embedding and decoding sequentially. However, as these two operations are done at embedder and decoder separately, the clock cycle requirement for individual operation is much less. Moreover, the operation may be done in parallel. The clock cycle requirement for watermark embedding and decoding are reduced significantly if single bit rather than 4 bits are embedded. The maximum clock frequency is 80 MHz and clock cycle 86 cycles/(8 x8). The data rate can be used is 930.232 Kbits/S. Input specifications of hardware realization is summarized in Table 3. The chip used is XCS40 and XCS40L, which contain 784 CLB, out of which 730 configurable logic

blocks (CLB) are consumed; 430 for watermark embedding unit and 300 units for watermark decoding. The design is fully portable and may be integrated into digital still camera framework. Throughput of the proposed architecture may seem to be low. However, higher throughput can be achieved if architecture is mapped to higher end FPGA available nowadays such as Virtex PRO etc. To the best of knowledge, this is the first FPGA based architecture for implementing fragile spread spectrum watermarking using fast Walsh transform. Moreover, hardware is designed for multiple bit embedding and the work serves the dual purposes of authentication and QoS

Figure 12. VLSI architecture of mean correlation and threshold calculation

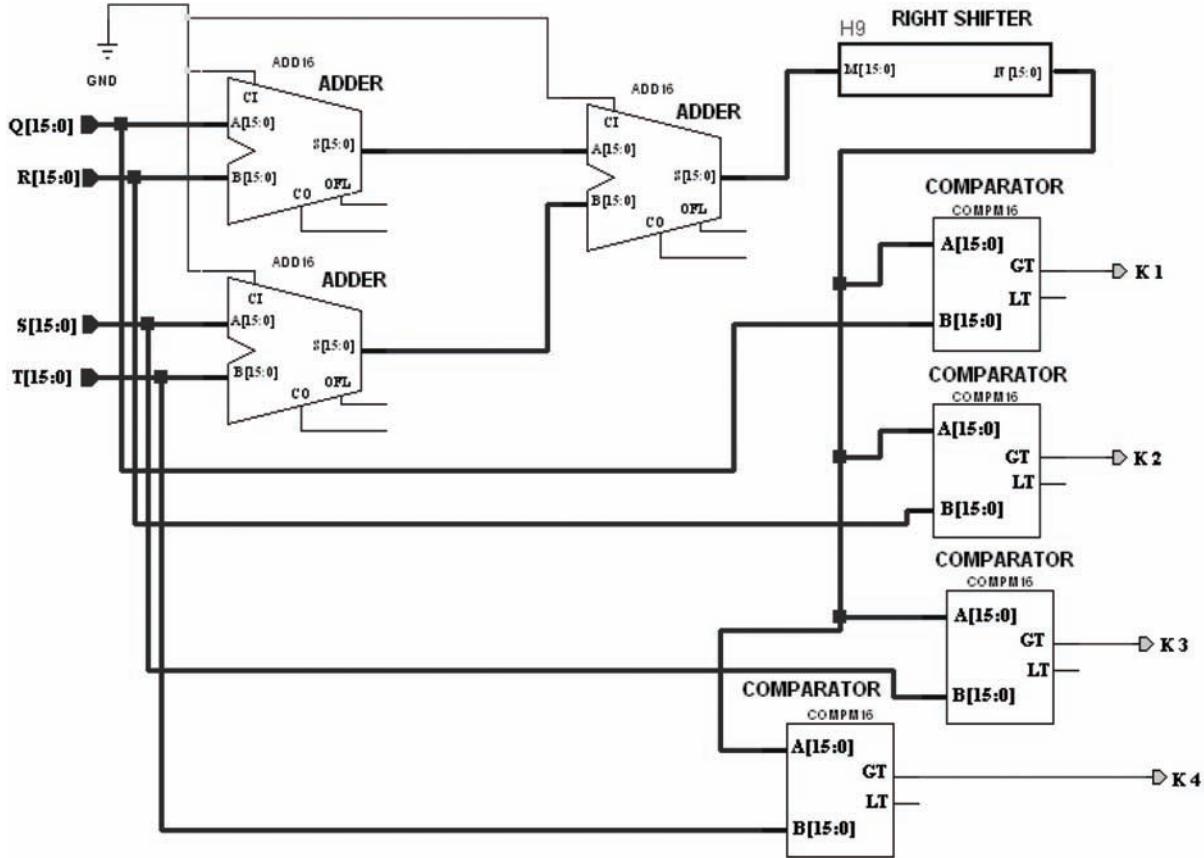


Table 3. Specification of hardware realization for low cost SS watermarking

System type	Block size	Implementation	CLB count	Clock freq. (Maximum)	Clock cycle
4 bit watermark	(8x8)	XCS40L	730	80 MHz	86 cycles

assessment, unlike the other hardware design of watermarking algorithms. Though the clock frequency used is low compared to the most of the other hardware designs reported in Table 1, the throughput is very high due to novelty of the proposed algorithm as well as the choice of FWT as the signal decomposition tool. The throughput would certainly be further increased if higher end FPGA were used. This high throughput makes the proposed hardware design attractive for the

present dual applications compared to other hardware design.

DIGITAL DESIGN OF BIORTHOGONAL WAVELET BASED HILBERT TRANSFORM

Recently discrete wavelet transform (DWT) of 2-band decomposition along with its various vari-

Table 4. The rational scaling filter coefficients of biorthogonal wavelets form Hilbert transform pair approximately

$h_0(n)$	$\hat{h}_0(n)$	$g_0(n)$	$\hat{g}_0(n)$
0	19/56	0	1/32
-1/128	57/128	-1/64	-1/32
3/64	-11/4	-1/64	-7/32
33/128	263/128	9/64	23/32
13/32	1325/128	25/64	23/32
33/128	263/128	25/64	-7/32
3/64	-11/4	9/64	-1/32
-1/128	57/128	-1/64	1/32
0	19/256	-1/64	0

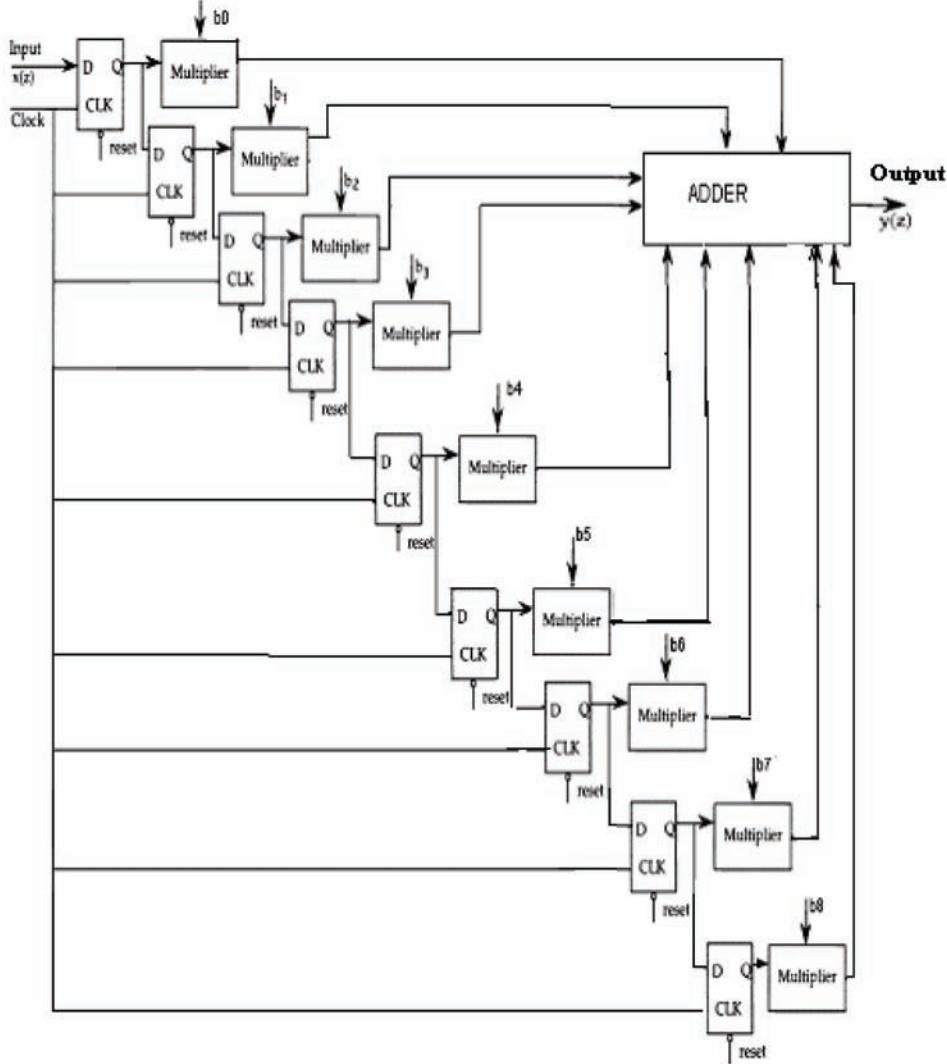
ants like M-band wavelets and wavelet packets find wide applications for detection, de-noising, and compression of multimedia signal etc. due to their better space-frequency localization, multi-resolution representation, superior HVS (human visual modeling) and adaptivity (Burris, 1997). Digital image and video watermarking is another interesting application of wavelets that has drawn attention of a group of researchers (Meerwald, 2001). Hilbert transform pairs of wavelets are the basic unit of many wavelet theories such as complex filter banks, complex wavelet and phaselet etc. Maity and Maity (Maity, 2008) propose an (i) algorithm for generation of low computation cost Hilbert transform pairs of symmetric filter coefficients using biorthogonal wavelets, (ii) approximation to its rational coefficients form for its efficient hardware realization and without much loss in signal representation, and finally (iii) development of QCM (quadrature carrier multiplexing)-SS image watermarking scheme for doubling the payload capacity.

Maity and Maity in (Maity, 2008) show that the filter coefficients for wavelet functions are smoother in case of biorthogonal wavelet bases. Furthermore, the coefficients of filters are symmetric which is quite advantageous to the various signal processing applications where shorter length and symmetric coefficients of filters can

reduce the computation efficiently to about one third of the original. Furthermore, the coefficients of two filter banks can be approximated to rational numbers, and their approximation to Hilbert transform pair is almost unchanged. It is possible to approximate the coefficients of two filter banks in all rational numbers. Table 4 shows rational scaling filter coefficients. Since the filter coefficients have the values with denominators in the form of 2^k , $k \in \mathbb{Z}$, computation for wavelet transform becomes easy requiring only addition and shift operations. The rational filter coefficients greatly simplify hardware design and are discussed in the next section.

Digital circuit is developed for one-dimensional input signal. It is assumed that each input is of 8-bits so as to represent the pixel values of a monochrome image, the number of filter coefficients 9 (based on the design), the number of bits allocated to represent the coefficient is 9 (one bit for sign and eight bits for magnitude). The detailed architecture for the wavelet analysis is depicted in Figure 13. The characteristics of such a filter are determined by a set of coefficients h_0, \dots, h_n applied respectively to each of the multipliers. Variation in the values of these coefficients allows the designer to control the characteristics of the wavelet transform operation. The multiplication is carried out using simple shift-and-add

Figure 13. Block circuit of analysis filter bank where b_0-b_8 are the coefficients of the filter

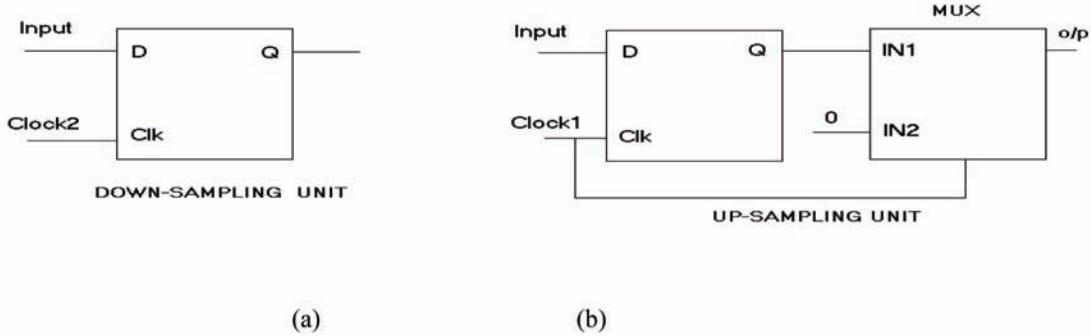


multiplier blocks. Since the multiplicands are signed, we use 2's complement arithmetic in all mathematical operations. It is observed that the denominators of all coefficients can be expressed in powers of 2. Hence the division operation can easily be accomplished using parameterized right-shifter blocks. Thus we have a right-shifter block tailing every multiplier unit in the filter bank design units. Although digital design of wavelet filter bank analysis is shown only in Figure 13, the circuit for the synthesis part is also identical

except wavelet coefficients are the input here and the corresponding outputs are the signal values in space or time domain, i.e. in original domain.

It is to be noted that the addition of a stream of zeroes between every two consecutive samples cannot be avoided. The buffer/latch is necessary for synchronization purposes and its length is equal to the data word length, which is 8-bit in this case. The bi-orthogonal wavelet based Hilbert transform makes use of 9-tap high precision floating-point filter coefficients. Hence filtering

Figure 14. Circuit diagram for (a) down sampling and (b) up sampling unit



operations during analysis and synthesis make estimation of the required memory resources difficult and consequently makes the design highly complicated. One possible solution to this problem is to approximate the coefficients of the filter banks as **rational** numbers such that no significant loss in signal integrity is encountered. Therefore, in this design, the **rational** numbers as filter coefficients are used. The circuit diagram of the 9-tap low pass analysis filter bank is shown in Figure 14. Since there are 9 filter coefficients, the hardware implementation needs 9 multipliers, 9 D flip-flops and one 16-bit signed adder unit. The circuit of decimation (down-sampling) and interpolation (up-sampling) are shown in Figure 14. In the decimator, a D flip-flop is used and the clock rate of the input must be equal to half the clock of the D flip-flop so that only every alternate input to the decimator is fed to the interpolator unit. In the interpolation block, i.e. the up-sampling block, the clock rate of the input must be equal to twice that of the clock for the D flip-flop so that a zero is inserted between every two successive inputs to the up-sampling block. Circuit models for the decimator and interpolator are shown in Figure 14.

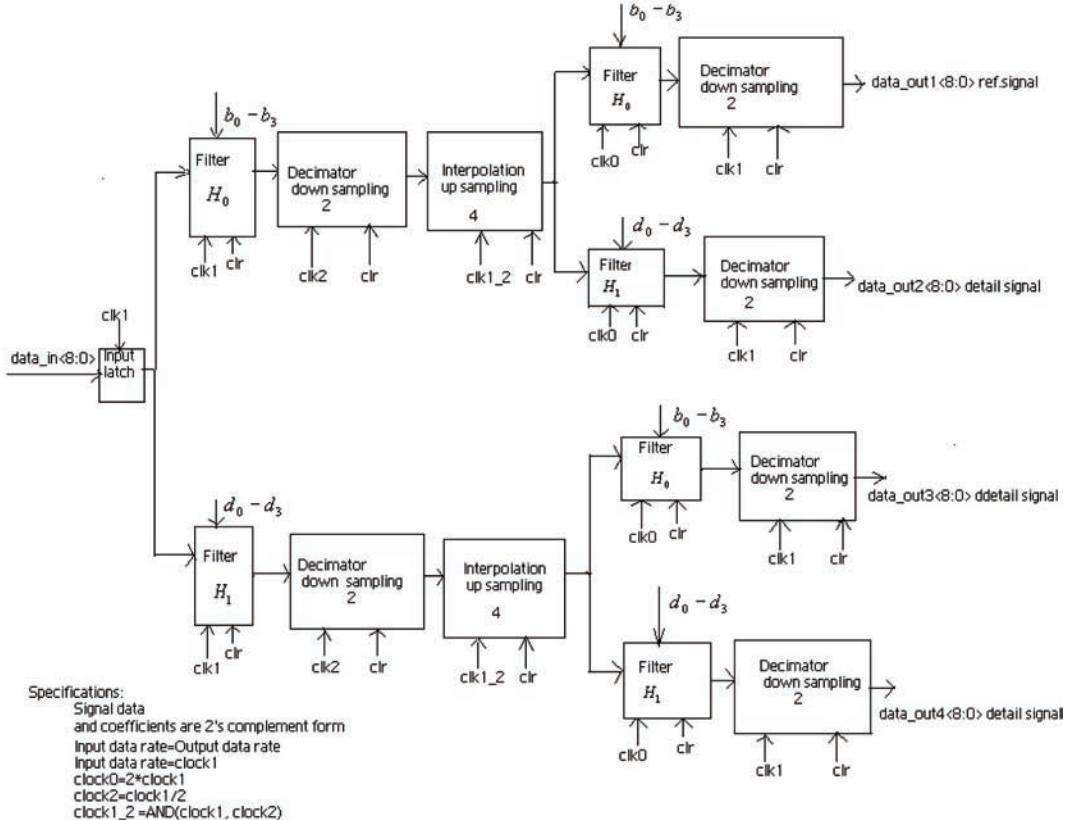
To keep the scalability feature of the architecture at a stage level, some considerations need to be made (even if only the analysis part is discussed, the approach is also valid for the syn-

thesis). The possible scheme is to preserve the data word-length. In this scheme, the filtered and the decimated data need to be truncated to the same data word-length (the initial data word-length). To fulfill the truncation requirement, the clock used for providing data words as inputs need to be set to zero (frozen) for an adequate number of cycles (according to the internal word-length). The control circuitry follows simple and regular design rules. It is to be mentioned that if the data word-length resulting from a filtering and decimating process is different from the original one, the scalability is lost.

This circuit design model can be extended to design a Hilbert transform system to process 2-D signals like still images. A possible circuit model for such a system is suggested in Figure 15.

To assess the effectiveness of the digital design, a single level of 1-D biorthogonal Hilbert transform pair, has been designed using Verilog HDL (hardware description language) and is implemented on the Xilinx XC4036 FPGA (field programmable gate array). The XC4036 consists of 36x36 arrays of configurable logic blocks (CLB). The input data and the multiplier are 8-bits and 9-bits in lengths. To get a compact layout and an optimal clock speed, the placement and timing constraints have been added to the design. The implementation report shows that discrete wavelet transform (DWT) stage occupies 58 CLBs for

Figure 15. Circuit block diagram for 2-D Hilbert transform analysis



frequencies of 100 MHz. Functional and timing simulations have been carried out by means of the Xilinx software tool (Foundation 2.1i). The device usage is normally reported in terms of number of look-up tables, I/O buffers, and flip-flops. The routing resource usage is not given by the place and route tools - higher device utilization implies greater routing resource utilization. The total numbers of CLBs used are a function of the device resources used and how densely they are packed. For example, on a CLB only a flip-flop could be used, but still it adds to the CLB count. The usages are given in Table 5.

This architecture is presented to serve two-fold purposes, (1) to extend the design for VLSI architecture of QCM-SS watermarking (Maity, 2006) for doubling the payload capacity in SS watermarking, and (2) to give an idea how to

develop rational filter coefficients that simplify hardware design, an aspect of challenge for developing watermarking algorithm in hardware platform and is discussed later.

HARDWARE DESIGN ASPECTS: CHALLENGES FOR WATERMARKING ALGORITHMS

Today it has been well accepted to the watermarking research community that hardware design of watermarking algorithms is essential for low power, real-time implementation, high reliability and low cost applications. However, hardware design aspect experiences a trade-off among the several requirements, namely power consumption, performance, memory space, silicon area

Table 5. Shows device utilization (target device- xc4036)

Logic utilization	Used	Availability	Utilization
No. of slices	1537	1920	80%
No. of slice FF	811	3840	21%
No. of 4 input LUT	1005	3840	26%
No. of bonded IOB	26	173	15%
No. of GCLks	3	8	37%
No. of CLBs	58	1296	4.4%

as well as integration in large scale. So, design of an efficient hardware architecture gets much thrust from the algorithm design of watermarking. Nowadays, digital watermarking (DWM) becomes a multidisciplinary research area involving theory of communications, signal processing, multimedia coding, information theory, cryptography, computer science and game theory etc. So the establishment of collaboration among these research groups, particularly the VLSI, signal processing and watermarking communities is essential. Similarly, for the design of hardware architecture of optimized watermarking system needs collaboration among the VLSI, computer science and watermarking research group. The VLSI implementation of watermarking algorithm is still at a relatively early stage of development and a lot more research is needed before a complete VLSI architecture with desirable characteristics is achieved. Some of the challenges for watermarking algorithms are pointed here that should be taken care for watermarking chip design.

1. The VLSI architecture discussed here is developed for a prototype smaller image. To achieve real-time watermarking for real life image and video signals, the chip design must be done using a pipelined or a parallel architecture. However, such architectures may consume large amount of both leakage and dynamic power. This requirement/restriction demands development of suitable efficient watermarking algorithms which

when mapped in hardware platform require as minimal a pipelining and parallel architecture as necessary.

2. The other important and challenging issue is the on-chip memory requirement. This is an important issue for non-blind scheme where the original multimedia data is required during detection process. Increase in memory size increases power consumption and cost of the chip.
3. It is also challenging to implement floating-point operations for hardware design. The division and multiplicative operations in watermarking algorithms consume much power compared to the addition and subtraction operations which in turn suggests to preferably selecting a watermarking algorithm with addition/subtraction operations more than division/multiplication operations. In other words, for a low power design, for example in mobile telephone system, a watermarking algorithm with more number of division/multiplication operations compared to addition/subtraction operations gives less room to the hardware designer for low power and high performance design. From that perspective, Walsh transform is a preferable choice than commonly used DCT as floating point addition-multiplication operations are not required when the digital image or video signal is convolved with the signed integer valued kernel during the forward and the inverse Walsh transform. Moreover, the

- kernel of one hardware block is sufficient to implement both forward and inverse transform, which is not possible in DCT based algorithm.
4. The selection of rational filter coefficients for transform (wavelet) domain watermarking provides much benefits for hardware realization. For example, the multiplication is carried out using simple shift-and-add multiplier blocks. The novelty in design for the scaling filter coefficients in Table 4 shows that the denominator of all the coefficients can be expressed in power of 2. Hence the division operation can easily be accomplished using parameterized right-shifter blocks.
 5. Most of the watermarking algorithms use random number or pseudo random number as watermark or key. Designing of low power random number generators and reliable storage of random number keys in hardware is a design challenge (Kougiannos, 2009). The commonly used hardware architecture for the generation of pseudo random numbers is the linear feedback shift register (LFSR), which is a sequential circuit with combinational feedback logic. It is essential to ensure that LFSR will not be getting stuck in the prohibited state and it would be eliminated.
 6. Over and above, the watermarking chip should be designed and placed in consumer electronic appliances such that normal operation of the host devices would not be affected.

FUTURE RESEARCH DIRECTIONS

Recently, hardware based image and video signal watermarking circuits and systems development become appealing due to its advantages over software realization in terms of less area, low execution time, low power, real-time performance, high reliability and also ease of integration with existing consumer electronics devices. A hardware

based watermarking system can be designed on a FPGA board, DSP board or custom integrated circuit ASIC. Most of the existing hardware architectures for watermarking are based on ASIC. However, due to unprecedented logic density increases and a host of features, FPGAs are a compelling proposition for almost any type of design. Moreover, very few hardware architectures are developed so far for SS watermarking, which is not only popular, robust, efficient and cryptographically secure but also can be integrated with the existing data transmission scheme. From that perspective, this chapter presents an insight how VLSI architecture for spatial and transform domain SS watermarking can be developed using FPGA. Followings are the few interesting research problems that can be taken into consideration as future research works.

1. FPGA based realization of biorthogonal Hilbert transform may be extended to develop QCM-SS watermarking following the concept of spatial or FWT domain SS watermarking architecture discussed here.
2. VLSI architectures developed and discussed here may be extended for hardware implementation of video signal watermarking.
3. Recently lifting technique is used widely for both designing fast wavelets and performing the discrete wavelet transform (DWT). The faster computation speed of lifting based technique over conventional DWT makes its hardware implementation easier. So, hardware architecture of lifting based watermarking for image and video signal based on ASIC or FPGA may be appealing for applications like fingerprinting, broadcast monitoring and secured transmission.
4. At present, a large number of color image and video signals are used for various applications and available on the web freely in the distributed archives. Moreover, the image and video signals are mostly stored and transmitted in compressed form. VLSI

- architecture of compressed color watermarked data for digital camera, world wide web alike or video-on-demand on broadcast network channel is quite appealing for real-time application.
- 5. Recently few watermarking algorithms for quality access control of compressed color images have been developed using lifting based wavelet and DCT. Both spread spectrum and quantization index modulation are used for design of efficient algorithm. These low cost algorithms may be mapped to hardware architecture for real-time applications.
 - 6. VLSI architecture for audio watermarking may be an interesting research work to explore.
 - 7. Optimization in watermarking becomes an important research topic for present days. Design of VLSI chip for optimized watermarking system using ASIC or FPGA may also be explored.
 - 8. Scarcity of power is an important issue for hand held mobile telephone system. Low power design of watermarking for multimedia mobile services may be explored for various applications.
 - 9. Watermarking algorithm should be designed in such a way that it can suitably be implemented in hardware with as minimal a pipelining and parallel architecture as necessary.

CONCLUSION

This chapter discusses hardware aspect of digital watermarking, particularly for SS watermarking, for various real-time applications like authentication, copyright protection, and QoS assessment of digital images. First, a brief review for the existing ASIC and FPGA based watermarking architectures for image and video signals are presented. The discussion is followed by a brief introduction on theory of SS watermarking along with associated

hardware design aspect and complexity. Then FPGA based SS watermark architectures are presented for spatial and FWT domain implementation for gray scale cover images with binary and gray scale watermark images. Wavelet based architecture is introduced which may be easily extended for VLSI architecture using the concept of spatial or FWT domain architecture. The hardware architectures for SS watermarking may be used efficiently for authentication, copyright protection and QoS assessment of multimedia mobile communication services. The need of low power, low cost, high performance real time operation, and high security with watermarking done at the data acquisition stage drives the VLSI implementation of the watermarking schemes. The feasibility of hardware implementation demands fulfillment of certain challenges for watermarking algorithms and some of these challenges are mentioned here. A few problems are also mentioned as scope of future research works. The VLSI implementation of watermarking algorithms is still at an early stage and a lot of collaborative works of the VLSI, signal processing and watermarking communities is required. Moreover, the scope and framework for digital watermarking systems addressing legal, political, business and deployment issues acceptable to different parties, such as content creators, music recording companies, movie production houses, the open source software development community, the consumer electronics industry, software companies, government organization, legal fraternity and end-users, is a large volume of works and needs to be completed sooner or later.

REFERENCES

- Brunton, A., & Zhao, J. (2005). Real-time Video Watermarking on Programmable Graphics Hardware. In *Proceedings of Canadian Conference on Electrical and Computer Engineering*, (pp. 1312–1315).

- Burrus, C. S., Gopinath, R. A., & Guo, H. (1997). *Introduction to Wavelets and Wavelet Transforms, A Primer*. Upper Saddle River, NJ: Prentice Hall.
- Cheung, S. C., & Chiu, D. K. W. (2003). A watermarking infrastructure for enterprise document management. In *Proceedings of 36th annual Hawaii international conference on system sciences* (pp. 105–114).
- Dittman, J., & Steinmetz, A. (1999). Content-based digital signatures for motion pictures authentication and content-fragile watermarking. In *Proceedings of the IEEE ICMCS*, Florence, (pp. 574–579).
- Fan, Y. C., Van, L. D., Huang, C. M., & Tsao, H. W. (2005) Hardware-efficient architecture design of wavelet-based adaptive visible watermarking. In *Proceedings of the 9th IEEE international symposium on consumer electronics*, (pp. 399–403).
- Fridrich, J., Goljan, M., & Baldoza, A. C. (2000). New fragile authentication watermark for images. In *Proceedings of the IEEE international conference of image processing (ICIP)*, (pp. 446–449).
- Garimella, A., Satyanarayan, M. V. V., Kumar, R. S., Murugesh, P. S., & Niranjan, U. C. (2003). VLSI implementation of online digital watermarking techniques with difference encoding for the 8-bit gray scale images. In *Proceedings of the international conference on VLSI design* (pp. 283–288).
- Garimella, A., Satyanarayana, M. V. V., Murugesh, P. S., & Niranjan, U. C. (2004). ASIC for Digital Color Image Watermarking. In *Proceedings of 11th IEEE Digital Signal Processing Workshop*, (pp. 292–295).
- Ghosh, S., Roy, P., Maity, S. P., & Rahaman, H. (2009). Spread Spectrum Image watermarking with Digital Design. In *Proceedings of IEEE International Advanced Computing conference (IACC 2009)*, Patiala, India, (pp. 868-873).
- Hanzo, L., Cherriman, P. J., & Streit, J. (2001). Wireless video communication: second to third generation systems and beyond. In *IEEE series on digital and mobile communication*. New York: IEEE.
- Ho, A. T. S., Shen, J., Chow, A. K. K., & Woon, J. (2003). Robust digital image-in-image watermarking using the fast Hadamard transform. In *Proceedings of the international symposium on circuits and systems (ISCAS 2003)*, (pp. 826–829).
- Hsiao, S. F., Tai, Y. C., & Chang, K. H. (2000a). VLSI Design of an Efficient Embedded Zerotree Wavelet Coder with Function of Digital Watermarking. In *Proceedings of the IEEE International Conference on Consumer Electronics*, (pp. 186–187).
- Hsiao, S. F., Tai, Y. C., & Chang, K. H. (2000b). VLSI Design of an Efficient Embedded Zerotree Wavelet Coder with Function of Digital Watermarking. *IEEE Transactions on Consumer Electronics*, 46(3), 628–636. doi:10.1109/30.883423
- Kougiannos, E., Mohanty, S. P., & Mahapatra, R. N. (2009). Hardware assisted watermarking for multimedia. [IJCEE]. *International Journal on Computers and Electrical Engineering*, 35(2), 339–358. doi:10.1016/j.compeleceng.2008.06.002
- Li, F. Y., Stol, N., Pham, T. T., & Andresen, S. (2001). A priority-oriented QoS management framework for multimedia services in UMTS. In *Proceedings of the fourth international IEEE symposium wireless personal multimedia communications*.
- Lukac, R., & Plataniotis, K. N. (2006). Secure single-sensor digital camera. *IEE Electronics Letters*, 42(11), 627–629. doi:10.1049/el:20060604
- Maes, M., Kalker, T., Linnartz, J. P. M. G., Talsstra, J., Depovere, G. F. G., & Haitsma, J. (2000). Digital watermarking for DVD video copyright protection. *IEEE Signal Processing Magazine*, 17, 47–57. doi:10.1109/79.879338

- Maity, S. P., Banerje, A., & Kundu, M. K. (2004). An image-in-image communication scheme and VLSI implementation using FPGA. In *Proceedings of IEEE Indian annual conference (INDICON 2004)*, (pp. 6–11).
- Maity, S. P., Banerjee, A., Abhijit, A., & Kundu, M. K. (2007). VLSI design of spread spectrum watermarking. In *Proceedings of 13th National conference on communication*, IIT Kanpur, India, (pp. 251–257).
- Maity, S. P. & Kundu, M. K. (2009b). Distortion free image-in-image communication with implementation in FPGA. *International Journal of Electronics and Communication*.
- Maity, S. P. & Kundu, M. K. (2009c). DHT domain digital watermarking with low loss in image information. *International Journal of Electronics and Communication Engg.*, 1-15.
- Maity, S. P., Kundu, M. K., & Das, T. S. (2007). Robust SS Watermarking with improved capacity. *Pattern Recognition Letters*, 28, 350–357. doi:10.1016/j.patrec.2006.04.004
- Maity, S. P., Kundu, M. K., & Maity, S. (2006). Capacity improvement in digital watermarking using QCM scheme. In *Proceedings of 12th National Conference on Communications (NCC 2006)*, IIT Delhi, India, (pp. 511–515).
- Maity, S. P., Kundu, M. K., & Maity, S. (2009a). Dual purpose FWT domain spread spectrum image watermarking in real-time. Special issues on Circuits & Systems for realtime security & copyright protection of multimedia. *Computers & Electrical Engineering*, 35(2), 415–433. doi:10.1016/j.compeleceng.2008.06.003
- Maity, S. P., & Maity, S. (2008). Wavelet based Hilbert transform with digital design and application to QCM-SS watermarking. *Radioengineering. Proceedings of Czech and Slovak Technical Universities*, 17(1), 64–72.
- Maity, S. P., Nandi, P. K., Kundu, M. K., & Banerjee, A. (2005). Low cost data authentication scheme and hardware realization. In *Proceedings of 11th National Conference on Communication (NCC-2005)*, (pp. 574–577).
- Mathai, N. J., Kundur, D., & Sheikholeslami, A. (2003a). Hardware implementation perspectives of digital video watermarking algorithms. *IEEE Transactions on Signal Processing*, 51, 925–938. doi:10.1109/TSP.2003.809382
- Mathai, N. J., Sheikholeslami, A., & Kundur, D. (2003b). VLSI Implementation of a Real-Time Video Watermark Embedder and Detector. In *Proceedings of the IEEE International Symposium on Circuits and Systems* (Vol. 2), (pp. 772–775).
- Mayer, J., Silverio, A. V., & Bermudez, J. C. M. (2002). On the design of pattern sequences for spread spectrum image watermarking. In *International Telecommunications Symposium- ITS2002*, Natal, Brazil.
- Meerwald, P., & Uhl, A. (2001). A survey of wavelet domain watermarking. In *Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III*, (vol. 4314).
- Mohanty, S. P. R. K. C., & Nayak, S. (2004a). FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder. In *Proceedings of Lecture Notes in Computer Science* 3356, (pp. 344–353).
- Mohanty, S. P., Pati, N., & Koulianios, E. (2007a). A watermarking Co-processor for new generation graphics processing units. [REMOVED HYPERLINK FIELD] In *Proceedings of the 25th IEEE International Conference on Consumer Electronics (ICCE)*, (pp. 303–304). Mohanty, S. P., Koulianios, E., & Ranganathan, N. (2007b). VLSI architecture and chip for combined invisible robust and fragile watermarking. *IET Computers & Digital Techniques (CDT)*, 1(5), 600–611.

- Mohanty, S. P., Ranganathan, N., & Balakrishnan, K. (2005b). Design of a Low Power Image Watermarking Encoder using Dual Voltage and Frequency. In *Proceedings of 18th IEEE International Conference on VLSI Design*, (pp. 153–158).
- Mohanty, S. P., Ranganathan, N., & Balakrishnan, K. (2006). A dual voltage-frequency VLSI chip for image watermarking in DCT domain. [TCASII]. *IEEE Transactions on Circuits and Systems II*, 53, 394–398. doi:10.1109/TCSII.2006.870216
- Mohanty, S. P., Ranganathan, N., & Namballa, R. K. (2003). VLSI implementation of invisible digital watermarking algorithms towards the development of a secure JPEG encoder. In *Proceedings of the IEEE workshop on signal processing systems*, (pp. 183–188).
- Mohanty, S. P., Ranganathan, N., & Namballa, R. K. (2005a). A VLSI architecture for visible watermarking in a secure still digital camera (S²DC) design. [TVLSI]. *IEEE Transactions on Very Large Scale Integration Systems*, 13, 1002–1012. doi:10.1109/TVLSI.2005.857991
- Mohanty, S. P., Rangnathan, N., & Namballa, R. K. (2004b). VLSI Implementation of Visible Watermarking for a Secure Digital Still Camera Design. In *Proceedings of the 17th International Conference on VLSI Design*, (pp. 1063–1068).
- Nelson, G. R., Jullien, G. A., & Pecht, O. Y. (2005). CMOS image sensor with watermarking capabilities. In *Proceedings of the IEEE International Conference on Circuits and Systems (ISCAS)*, (pp. 5326–5329).
- Petitjean, G., Dugelay, J. L., Gabriele, S., Rey, C., & Nicolai, J. (2002). Towards Real-time Video Watermarking for Systems- On-Chip. In *Proceedings of the IEEE International Conference on Multimedia and Expo* (Vol. 1), (pp. 597–600).
- Seo, Y. H., & Kim, D. W. (2003). Real-Time Blind Watermarking Algorithm and its Hardware Implementation for Motion JPEG2000 Image Codec. In *Proceedings of the 1st Workshop on Embedded Systems for Real-Time Multimedia*, (pp. 88–93).
- Strycker, L. D., Termont, P., Vandewege, J., Haitsma, J., Kalker, A., Maes, M., & Depovere, G. (1999). An Implementation of a Real-time Digital Watermarking Process for Broadcast Monitoring on a Trimedia VLIW Processor. In *Proceedings of the IEE International Conference on Image Processing and Its Applications* (Vol. 2), (pp. 775–779).
- Strycker, L. D., Termont, P., Vandewege, J., Haitsma, J., Kalker, A., Maes, M., & Depovere, G. (2000). Implementation of a real-time digital watermarking process for broadcast monitoring on trimedia VLIW processor. *IEE Proceedings. Vision Image and Signal Processing*, 147, 371–376. doi:10.1049/ip-vis:20000580
- Tsai, T. H., & Lu, C. Y. (2001). A systems level design for embedded watermark technique using DSC systems. In *Proceedings of the IEEE International Workshop on Intelligent Signal Processing and Communication Systems*.
- Tsai, T. H., & Wu, C. Y. (2003). An Implementation of Configurable Digital Watermarking Systems in MPEG Video Encoder. In *Proceedings of the IEEE International Conference on Consumer Electronics*, (pp. 216–217).
- Voyatzis, G., & Pitas, I. (1999). Protecting digital-image copyrights: a framework. *IEEE Computer Graphics and Applications*, 19, 18–24. doi:10.1109/38.736465

ADDITIONAL READING

- A., Alm, C., & Norman, P. (1999). Performance Measurements of a Real-time Digital Watermarking System for Broadcast Monitoring. In *Proceedings of the IEEE International Conference on Multimedia Computing and Systems* (Vol. 2), (pp. 220–224).
- Barni, M., & Bartolini, F. (2004). *Watermark System Engineering*. New York, USA: Marcel Dekker.
- Braudaway, G. W., Magerlein, K. A., & Mintzer, F. (1996). Protecting Publicly Available Images with a Visible Image Watermark. In *Proceedings of the SPIE Conference on Optical Security and Counterfeit Deterrence Technique* (Vol. SPIE-2659), (pp. 126–132).
- Chen, W. K. (2000). The VLSI Handbook. CRC Press, 2000.
- Cox, I. J., Miller, M. L., & Bloom, J. A. (2001). *Digital Watermarking*. San Francisco: Morgan Kaufmann.
- Depovere, G., Kalker, T., Haitsma, J., Maes, M., Strycker, L. D., Termont, P., et al. (1999). The VIVAProject: Digital Watermarking for Broadcast Monitoring. In *Proceedings of the IEEE International Conference on Image Processing* (Vol. 2), (pp. 202–205).
- Shoshan, Y., Fish, A., Li, X., Jullien, G. A., & Yadid-Pecht, O. (2008). VLSI watermark implementations and applications. *IJ Information and Knowledge Technologies*, 2, 379–386.
- Termont, P., Strycker, L. D., Vandewege, J., & Haitsma, J. Kalker, Maes, T., M., & Depovere, Langell, Vural, S., Tomii, H., & Yamauchi, H. (2005). Video Watermarking For Digital Cinema Contents, in: Proceedings of the 13th European Signal Processing Conference, (pp. 303–304).

Compilation of References

- Aabed, A., Awaideh, S. M., Elshafei, A. M., & Gutub, A. A. (2007). Arabic Diasritics Based Steganography. In *IEEE International Conference on Signal Processing and Communication (ICSPC 2007)*, (pp. 756-759).
- Abdallah, E. E., Ben Hamza, A., & Bhattacharya, P. (2007). *Spectral graph-theoretic approach to 3D mesh watermarking* (pp. 327–334). Proc. of the Graphics Interface.
- Abdallah, E. E., Hamza, A. B., & Bhattacharya, P. (2007). MPEG Video Watermarking using Tensor Singular Value Decomposition. In Kamel, M., & Campilho, A. (Eds.), *Image Analysis and Recognition* (Vol. 4633, pp. 772–783). Berlin: Springer-Verlag. doi:10.1007/978-3-540-74260-9_69
- Abdelnour, A. F., & Selesnick, I. W. (2001). Nearly symmetric orthogonal wavelet bases. In *Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing (ICASSP)*.
- Acharya, T., & Chakrabarti, C. (2006). A survey on lifting-based discrete wavelet transform architectures. *Journal of VLSI Signal Processing Systems*, 42(3).
- Adamo, B., Mohanty, S. P., Kougianos, E., Varanasi, M., & Cai, W. (2006). VLSI architecture and FPGA prototyping of a digital camera for image security and authentication. In *Proceedings of the IEEE Region 5 Technology and Science Conference*, (pp. 154-158).
- Adamo, O. B., Mohanty, S. P., Kougianos, E., & Varanasi, M. (2006). VLSI architecture for encryption and watermarking units towards the making of a secure camera. In *Proceedings of the IEEE International SOC Conference*, (pp. 141-144).
- Adelsbach, A., Katzenbeisser, S., & Sadeghi, A. (2002). Cryptography Meets Watermarking: Detecting Watermarks with Minimal or Zero Knowledge Disclosure. In *European Signal Processing Conference (EUSIPCO 2002)*, (Vol. I, pp. 446-449), TESA, France.
- Adelsbach, A., Katzenbeisser, S., & Veith, H. (2003). Watermarking schemes provably secure against copy and ambiguity attacks. In *3rd ACM Workshop on Digital Rights Management*, (pp. 111-119). New York: ACM.
- Agarwal, R., & Santhanam, M. S. (2006Submitted to). *Digital watermarking in the singular vector domain*. Elsevier.
- Ahlzen, L., & Song, C. (2003). *The sound blaster live! Book: A complete guide to the world's most popular sound card*. San Francisco, CA: No Starch Press, Inc.
- Ahmad, S. (2000). *Introduction to watermarking. Unpublished tutorial*. Islamabad, Pakistan: Pakistan Institute of Engineering and Applied Sciences.
- Ahmad, S. (2001). *Digital signatures and watermarking*. M.Sc. Thesis, Pakistan Institute of Engineering and Applied Sciences, Islamabad, Pakistan.
- Alattar, A. M. (n.d.). *Bridging Printed Media and Internet via Dimarc's Watermarking Technology*. Retrieved Feb 25, 2009, from https://www.digimarc.com/resources/docs/tech_papers/dmrc_media_bridge.pdf
- Alattar, A. M., & Alattar, O. M. (n.d.). *Watermarking Electronic Text Documents Containing Justified Paragraphs and Irregular Line Spacing*. Retrieved Feb 25, 2009, from https://www.digimarc.com/resources/docs/tech_papers/dmrc_text_watermarking.pdf

Compilation of References

- Alghoniemy, M., & Tewfik, A. H. (2000, July/August). *Geometric distortion correction through image normalization*. Paper presented at the IEEE International Conference on Multimedia & Expo (ICME), Hilton New York & Towers New York, NY.
- Alghoniemy, M., & Tewfik, A. H. (2004). Geometric invariants in image watermarking. *IEEE Transactions on Image Processing*, 13(2), 145–153. doi:10.1109/TIP.2004.823831
- Al-Khatib, T., Al-Haj, A., Rajab, L., & Mohammed, H. (2008). A robust Video Watermarking Algorithm. *Journal of Computer Science*, 4(11), 910–915. doi:10.3844/jcssp.2008.910.915
- Amano, T., & Misaki, D. (1999, September). A feature calibration method for watermarking of document images. In *Proceedings of the Fifth International Conference on Document Analysis and Recognition (ICDAR '99)*, (pp. 91-94).
- An, L. J., Lu, H., Yi, F. D. & XaioLin, G. (2008). A Text Digital Watermarking for Chinese Word Document. *IEEE Symposium on Computer Science and Computational Technology*, (pp. 348-351).
- Andrews, H., & Patterson, C. (1976). Singular Value decompositions and Digital Image Processing. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 24(1), 26–53. doi:10.1109/TASSP.1976.1162766
- Archambeau, C., Lee, J., & Verleysen, M. (2003). Convergence problems of the EM algorithm for finite Gaussian mixtures. In *Proc. 11th European Symposium on Artificial Neural Networks*, Bruges, Belgium (pp. 99-106).
- Archambeau, C., Valle, M., Assenza, A., & Verleysen, M. (2006). Assessment of probability density estimation methods: Parzen window and finite Gaussian mixtures. In *Proc. IEEE International Symposium on Circuits and Systems*, Kos, Greece.
- Arimoto, S. (1972). An algorithm for computing the capacity of arbitrary discrete memoryless channels. *IEEE Transactions on Information Theory*, 18(1), 14–20. doi:10.1109/TIT.1972.1054753
- Arnold, M. (2000). Audio watermarking: features, applications and algorithms. In *Proceeding. of the IEEE International Conference on Multimedia and Expo*, (Vol. 2, pp. 1013-1016).
- Arnold, M., Schmucker, M., & Wolthusen, S. (2003). *Techniques and Applications of Digital Watermarking and Content Protection*. Boston: Artech House.
- Arseneau, S. (2008). *Junction-Analysis*. Nevada, USA: VDM Verlag.
- Artz, D. (2001). Digital steganography: Hiding data within data. *IEEE Internet Computing*, 5(3), 75–80. doi:10.1109/4236.935180
- Aslantas, V. (2009). An optimal robust digital image watermarking based on SVD using differential evolution algorithm. *Optics Communications*, 282(5), 769–777. doi:10.1016/j.optcom.2008.11.024
- Aslantas, V., Dogan, A. L., & Ozturk, S. (2008). DWT-SVD based image watermarking using Particle Swarm Optimizer. In *Proceedings of 2008 IEEE International Conference on Multimedia* (pp. 241-244).
- Aslatnas, V. (2009). SVD and DWT-SVD domain robust watermarking using differential evolution algorithm. In Ao, S. I. (Ed.), *Advances in Electrical Engineering and Computational Science* (Vol. 39, pp. 147–159).
- Atallah, M., Prabhakar, S., Frikken, K., & Sion, R. (2004). Digital rights protection. *A Quarterly Bulletin of the Computer Society of the IEEE Technical Committee on Data Engineering*, 27, 19–26.
- Babu, K. S., Raja, K. B., Uma, M. R. K., Rashmi, K. A., Venugopal, K. R., & Patnaik, L. M. (2007). Robust and high capacity image steganography using SVD. In *International Conference on Information and Communication Technology in Electrical Sciences* (pp. 718-723). Chennai, India: Dr. M.G.R. University Press.
- Bahandri, K., Mitra, S. K., & Jadhav, A. (2005). A Hybrid Approach to Digital Image Watermarking Using Singular Value Decomposition and Spread Spectrum. In Pal, S. K. (Eds.), *Information Assurance in Computer Networks* (Vol. 3776, pp. 447–452). Berlin: Springer-Verlag.

- Balado, F., Pérez-González, F., & Scalise, S. (2001). Turbo coding for sample-level watermarking in the DCT domain. In *Proceedings of IEEE Int. Conf. on Image Processing*, Thessaloniki, Greece (pp. 1003-1006).
- Bao, P., & Ma, X. (2005). Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition. *IEEE Transactions on Circuits and Systems for Video Technology*, 15(1), 96–102. doi:10.1109/TC-SVT.2004.836745
- Barkat, B., & Sattar, F. (2003). A new time-frequency based private fragile watermarking scheme for image authentication. *IEEE International Symposium on Signal Processing and Applications*, (vol. 2, pp. 363–366).
- Barni, M., & Bartolini, F. (2004). *Watermark System Engineering*. New York: Marcel Dekker.
- Barni, M., Bartolini, F., & Furon, T. (2003). A general framework for robust watermarking security. *Signal Processing*, 83(10), 2068–2084. doi:10.1016/S0165-1684(03)00168-3
- Barni, M., Bartolini, F., & Piva, A. (1998). Copyright protection of digital images by means of frequency domain watermarking. *Proceedings of the Society for Photo-Instrumentation Engineers*, 3456, 25–35.
- Barni, M., Bartolini, F., & Piva, A. (2002). Multichannel watermarking of color images. *Circuits and Systems for Video Technology. IEEE Transactions on*, 12(3), 142–156.
- Barni, M., Bartolini, F., Cappellini, V., & Piva, A. (1998). A DCT-domain system for robust image watermarking. *Signal Processing*, 66(3), 357–372. doi:10.1016/S0165-1684(98)00015-2
- Barni, M., Bartolini, F., Cappellini, V., Lippi, A., & Piva, A. (1999). DWT-based technique for spatio-frequency masking of digital signatures. In *Security and Watermarking of Multimedia Contents* (Vol. 3657, pp. 31–39). SPIE.
- Barni, M., Bartolini, F., De Rosa, A., & Piva, A. (2003). Optimum decoding and detection of multiplicative watermarks. *IEEE Transactions on Signal Processing*, 51(4), 1118–1123. doi:10.1109/TSP.2003.809371
- Barni, M., Bartolini, F., Rosa, A. D., & Piva, A. (2002). Color image watermarking in the Karhunen-Loeve transform domain. *Journal of Electronic Imaging*, 11(1), 87–95. doi:10.1117/1.1426383
- Barreto, P. S. L. M., Kim, H. Y., & Rijmen, V. (2002). Toward secure public-key block-wise fragile authentication watermarking. *IEE Proceedings. Vision Image and Signal Processing*, 148(2), 57–62. doi:10.1049/ip-vis:20020168
- Barron, R., Chen, B., & Wornell, G. (2003). The duality between information embedding and source coding with side information and some applications. *IEEE Transactions on Information Theory*, 49(5), 1159–1180. doi:10.1109/TIT.2003.810639
- Bas, P., Chassery, J., & Macq, B. (2002). Geometrically invariant watermarking using feature points. *IEEE Transactions on Image Processing*, 11(9). doi:10.1109/TIP.2002.801587
- Bassia, P., Pitas, I., & Nikolaidis, N. (2001). Robust Audio Watermarking in the Time-Domain. *IEEE Transactions on Multimedia*, 3(2), 232–242. doi:10.1109/6046.923822
- Bassia, P., Pitas, I., & Nikolaidis, N. (2003). A temporal-domain audio watermarking technique. *IEEE Transactions on Signal Processing*, 51(4), 1088–1097. doi:10.1109/TSP.2003.809372
- Basso, A., Bergadano, F., Cavagnino, D., Pomponiu, V., & Vernone, A. (2009). A Novel Block-based Watermarking Scheme Using the SVD Transform. *Algorithms*, 2(1), 46–75. doi:10.3390/a2010046
- Bastug, A., & Sankur, B. (2004). Improving the payload of watermarking channels via LDPC coding. *IEEE Signal Processing Letters*, 11(2), 90–92. doi:10.1109/LSP.2003.819350
- Baudry, S., Delaigle, J.-F., Sankur, B., Macq, B., & Maitre, H. (2001). Analyses of error correction strategies for typical communication channels in watermarking. *Signal Processing*, 81, 1239–1250. doi:10.1016/S0165-1684(01)00041-X

Compilation of References

- Beerends, J., & Stemerdink, J. (1992). A perceptual audio quality measurement based on a psychoacoustic sound representation. *Journal of the Audio Engineering Society. Audio Engineering Society*, 40(12), 963–972.
- Belkasim, S. O., Shridhar, M., & Ahmadi, M. (1991). Pattern recognition with moment invariants: A comparative study and new results. *Pattern Recognition*, 24(12), 1117–1138. doi:10.1016/0031-3203(91)90140-Z
- Bender, W., Butera, W., Gruhl, D., Hwang, R., Paiz, F. J., & Pogreb, S. (2000). Applications for data hiding. *IBM Systems Journal*, 39(3-4), 547–568. doi:10.1147/sj.393.0547
- Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, 35(3), 313–336. doi:10.1147/sj.353.0313
- Benedens, O. (1999). Geometry-based watermarking of 3D models. *IEEE Computer Graphics and Applications*, 19(1), 46–55. doi:10.1109/38.736468
- Berghel, H. (1998, July). Watermarking Cyberspace. *ACM Communication*, 41(7), 19–24.
- Berghel, H., & O’Gorman, L. (1996, July). Protecting ownership rights through digital watermarking. *IEEE Computer*, 29(7), 101–103.
- Bergman, C., & Davidson, J. (2005). Unitary embedding for data hiding with the SVD. In Delp, E. J. (Eds.), *Security, Steganography, and Watermarking of Multimedia Contents* (Vol. 5681, pp. 619–630). Bellingham, WA: SPIE.
- Bevilacqua, A., & Azzari, P. (2007). A High Performance Exact Histogram Specification Algorithm. In *Image Analysis and Processing, 2007, (ICIAP 2007), 14th International Conference on* (pp. 623–628).
- Bezdek, J. C., & Pal, S. K. (Eds.) (1992). Fuzzy models for pattern recognition: methods that search for structures in data. New York: IEEE CS Press.
- Bhatnagar, G., & Raman, B. (2008). Dual Watermarking Scheme via Sub-sampling in WPT-SVD domain. In *Proceedings of the First International Conference on Emerging Trends in Engineering and Technology* (pp. 850–855).
- Bhattacharjya, A. K., & Ancin, H. (1999). Data Embedding in text for a copier system. In *Proc of International Conference on Image Processing*, 2, 245–249.
- Bhattacharya, A. (2009). *On Optimization of M-band wavelets zero-rate spread spectrum watermarking using Genetic Algorithms*. Unpublished master’s thesis, Bengal Engineering and Science University, Shibpur, India.
- Bhattacharya, A., & Bhattachary, R. (2008). Nonparametric statistics on manifolds with applications to shape spaces pushing the limits of contemporary statistics: contributions in honor of J.K. Ghosh. *IMS Collections*, 3, 282–301. doi:10.1214/074921708000000200
- Biehl, I., & Meyer, B. (1997). Protocols for Collusion-Secure Asymmetric Fingerprinting. In *Proc. 14th Annual Symposium on Theoretical Aspect of Computer Science*, (LNCS Vol. 1200, pp. 399–412). Berlin: Springer-Verlag.
- Biggs, N. (1993). *Algebraic Graph Theory* (2nd ed.). Cambridge, UK: Cambridge University Press.
- Bilgin, A., & Marcellin, M. (2006). JPEG2000 for digital cinema. In *Proceedings of the IEEE International Symposium on Circuits and Systems*, (pp. 3881 - 3885).
- Blahut, R. (1972). Computation of channel capacity and rate-distortion functions. *IEEE Transactions on Information Theory*, 18(4), 460–473. doi:10.1109/TIT.1972.1054855
- Bloom, J. A., Cox, I. J., Kalker, T., Linnartz, J. M. G., Miller, M. L., Brendan, C., & Traw, S. (1999). Copy protection for DVD video. *Proceedings of the IEEE*, 87(7), 1267–1276. doi:10.1109/5.771077
- Bogomjakov, A., Gotsman, C., & Isenburg, M. (2008). Distortion-free steganography for polygonal meshes. *Computer Graphics Forum*, 27(2), 637–642. doi:10.1111/j.1467-8659.2008.01161.x
- Böhle, K., Rader, M., Weber, A., & Weber, D. (2008). *Looking Forward in the ICT & Media Industries*. European Technology Assessment Group.
- Boneh, D., & Shaw, J. (1995). Collusion-secure fingerprinting for digital data. *IEEE Transactions on Information Theory*, 44(5), 1897–1905. doi:10.1109/18.705568

- Bors, A. (2006). Watermarking Mesh-Based Representations of 3D Objects Using Local Moments. *Image Processing, IEEE Transactions on*, 15, 687–701.
- Botsch, M., Pauly, M., Kobbelt, L., Alliez, P., Lévy, B., Bischoff, S., & Rössl, C. (2007). Geometric modeling based on polygonal meshes. In *Proc. of the ACM SIGGRAPH Course Notes*.
- Bounkong, S., Toch, B., Saad, D., & Lowe, D. (2004). ICA for Watermarking. *Journal of Machine Learning Research*, 4(7-8), 1471–1498. doi:10.1162/jmlr.2003.4.7-8.1471
- Box, G. E. P. (1978). *Statistics for experimenters: An introduction to design, data analysis, and model building*. New York: John Wiley & Sons.
- Boyer, J.-P., Duhamel, P., & Blanc-Talon, J. (2006). Asymptotically optimal scalar quantizers for QIM watermark Detection. In *Proceedings of IEEE International Conference on Multimedia and Expo*.
- Braci, S., Boyer, R., & Delpha, C. (2008). On the trade-off between security and robustness of the trellis coded quantization scheme. In *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*.
- Braci, S., Boyer, R., & Delpha, C. (2009). Security evaluation of informed watermarking schemes. *IEEE International Conference on Image Processing (ICIP)* (Accepted).
- Braci, S., Delpha, C., & Boyer, R. (2009). How quantization based schemes can be used in steganographic context. In *IEEE Int. Workshop on MultiMedia Signal Processing (MMSP)*, Rio de Janeiro, Brazil.
- Braci, S., Delpha, C., Boyer, R., & Guelvouit, G. L. (2008). Informed stego-systems in active warden context: statistical undetectability and capacity. In *Proceedings of IEEE International Workshop on MultiMedia Signal Processing (MMSP)*, Cairns, Queensland, Australia.
- Brandenburg, K., & Sporer, T. (1992). NMR and masking flag: Evaluation of quality using perceptual criteria. In *Proceedings of the International Audio Engineering Society Conference on Audio Test and Measurement*, (pp. 169–179).
- Brands, S. (1993). Untraceable off-line cash in wallet with observers. Advances in Cryptology - Crypto'93. (LNCS Vol. 773, pp. 302-318). Berlin: Springer-Verlag.
- Brassard, G., Chaum, D., & Crèau, C. (1988). Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37, 156–189. doi:10.1016/0022-0000(88)90005-0
- Brassil, J. T., Low, S. H., Maxemchuk, N. F., & O’Gorman, L. (1995 April), Document Marking and Identification using both Line and Word Shifting. In *Proceedings of IEEE INFOCOM ’95. Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, 2, 853-860.
- Brassil, J.T, Low, S.H, Maxechuk, N.F & O’Gorman, L. (1994). Electronic Marking and Identification Techniques to Discourage Document Copying. *IEEE Infocom ’94*, 3, 1278-1287.
- Braudaway, G. W., Magerlein, K. A., & Mintzer, F. (1996). Protecting publicly available images with a visible image watermark. In *The SPIE Conference on Optical Security and Counterfeit Deterrence Technique*, SPIE-2659, (pp. 126 – 132).
- Bro, R., Acar, E., & Kolda, T. G. (2008). Resolving the sign ambiguity in the singular value decomposition. *Journal of Chemometrics*, 22(1-2), 135–140. doi:10.1002/cem.1122
- Brunton, A., & Zhao, J. (2005). Real-time video watermarking on programmable graphics hardware. In *Canadian Conference on Electrical and Computer Engineering*, (pp. 1312 - 1315).
- Burdescu, D. D., & Stanescu, L. (2006). An Algorithm for Authentication of Digital Images. In *International Conference on Security and Cryptography*, Setubal, Portugal, (pp. 303-311).

Compilation of References

- Burdescu, D. D., Stanescu, L., Ion, A., & Tanasie, R. (2008). A New 3D Watermarking Algorithm. In *3DTV Conference: The True Vision - Capture, Transmission and Display of 3D Video*, Istanbul, Tukey, (pp. 381–384).
- Burdescu, D.D. & Stanescu, L. (2004). A Spatial Watermarking Algorithm for Digital Images. *Control Engineering and Applied Informatics Journal*, 6(3), 57–63.
- Burrus, C. S., Gopinath, R. A., & Guo, H. (1997). *Introduction to Wavelets and Wavelet Transforms, A Primer*. Upper Saddle River, NJ: Prentice Hall.
- Byun, S.-C., Lee, S.-K., Tewfik, A. H., & Ahn, B.-H. (2003). A SVD-Based Fragile Watermarking Scheme for Image Authentication. In Petitcolas, F. A. P. (Eds.), *Digital Watermarking* (Vol. 2613, pp. 375–391). Berlin: Springer-Verlag. doi:10.1007/3-540-36617-2_14
- Cachin, C. (1998). An information theoretic model for steganography. In D. Aucsmith (Eds.), *Proceedings of 2nd Workshop on Information Hiding* (LNCS vol.1525, pp. 306–318). Berlin: Springer.
- Calagna, M., Guo, H., Mancini, L. V., & Jajodia, S. (2006). Robust Watermarking System based on SVD Compression. In *Proceedings of the ACM Symposium on Applied Computing* (pp. 1341-1347). New York: ACM Press.
- Campisi, P., Kundur, D., Hatzinakos, D., & Neri, A. (2002). Compressive data hiding: an unconventional approach for improved color image coding. *EURASIP Journal on Applied Signal Processing*, (1): 152–163. doi:10.1155/S1110865702000550
- Castleman, K. (1996). *Digital Image Processing*. Upper Saddle River, NJ: Prentice-Hall.
- Cayre, F., & Macq, B. (2003). Data hiding on 3-D triangle meshes. *IEEE Transactions on Signal Processing*, 51(4), 939–949. doi:10.1109/TSP.2003.809380
- Cayre, F., Rondao-Alface, P., Schmitt, F., Macq, B., & Maître, H. (2003). Application of spectral decomposition to compression and watermarking of 3D triangle mesh geometry. *Signal Processing Image Communication*, 18(4), 309–319. doi:10.1016/S0923-5965(02)00147-9
- Chae, J., Mukherjee, D., & Manjunath, B. (1998). Color image embedding using multidimensional lattice structures. In *International Conference on Image Processing* (Vol. 1, pp. 460-464).
- Chakrabarti, C., Vishwanath, M., & Owen, R. M. (1995). A survey of architectures for the discrete and continuous wavelet transforms. *International Conference on Acoustics, Speech, and Signal Processing*, 5, (pp. 2849 - 2852).
- Chan, C. K., & Cheng, L. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, 37, 469–474. doi:10.1016/j.patcog.2003.08.007
- Chan, C. K., & Cheng, L. M. (2001). Improved hiding data in images by optimal moderately significant-bit replacement. *IEE Electronics Letter*, 37(16), 1017–1018. doi:10.1049/el:20010714
- Chan, P., & Lyu, M. (2003). A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code. In *Proceedings of the 5th International Conference on Information and Communications Security*, (pp. 202-213).
- Chandra, D. V. S. (2002). Digital image watermarking using singular value decomposition. In *Proceedings of IEEE 45th Midwest Symposium on Circuits and Systems: Vol. 3* (pp. 264-267).
- Chandramouli, R., & Memon, N. (2001). Analysis of LSB based image steganography techniques. In *Proceedings of IEEE International Conference on Image Processing*, (pp. 1019–1022).
- Chandramouli, R., Kharrazi, M., & Memon, N. (2004). Image Steganography. Concepts and Practice. *Lecture Notes in Computer Science*, 2939, 35–49.
- Chang, C., & Davisson, L. D. (2004). On calculating the capacity of an infinite-input finite (infinet)-output channel. *IEEE Transactions on Information Theory*, 50, 1004–1010. doi:10.1109/18.21223
- Chang, C., Tsai, P., & Lin, C. (2005). SVD-based digital image watermarking scheme. *Pattern Recognition Letters*, 26(10), 1577–1586. doi:10.1016/j.patrec.2005.01.004

- Chang, C.-C., Hu, Y.-S., & Lin, C.-C. (2007). A Digital watermarking scheme based on singular value decomposition. In Chen, B. (Eds.), *Combinatory, Algorithms, Probabilistic and Experimental Methodologies* (Vol. 4614, pp. 82–93). Berlin: Springer-Verlag. doi:10.1007/978-3-540-74450-4_8
- Chang, C.-C., Lin, C.-C., & Hu, Y.-S. (2007). An SVD oriented watermark embedding scheme with high qualities for the restored images. *International Journal of Innovative Computing. Information and Control*, 3(3), 609–620.
- Chang, C.-C., Tsai, P., & Lin, C.-C. (2005). SVD-based Digital Image Watermarking scheme. *Pattern Recognition Letters*, 26(10), 1577–1586. doi:10.1016/j.patrec.2005.01.004
- Chang, J., & Chang, L. (2004). A new image copyright protection algorithm using digital signature of trading message and bar code watermark. In *Image and Vision Computing New Zealand 2003*. Palmerston North, New Zealand: Massey University.
- Chao, S., Huang, H., & Chen, C. (2006). Digital watermarking of color image. In *Color imaging XI: (processing, hardcopy, and applications)* (Vol. 6058, p. 605815). SPIE.
- Chareyron, G., Coltuc, D., & Trémeau, A. (2006). Watermarking and Authentication of Color Images Based on Segmentation of the xyZ Color Space. *Journal of Imaging Science and Technology*, 50(5), 411–423. doi:10.2352/J.ImagingSci.Technol.(2006)50:5(411)
- Charoensak, C., & Sattar, F. (2005). Design of low-cost FPGA hardware for real-time ICA-based blind source separation algorithm. *EURASIP Journal on Applied Signal Processing*, 18, 3076–3086. doi:10.1155/ASP.2005.3076
- Chaum, D., & Pedersen, T. P. (1992). Wallet databases with observers. Advances in Cryptology - Crypto'92. (LNCS Vol. 740, pp. 89-105). Berlin: Springer-Verlag.
- Chaum, D., Damgaard, I., & Van de Graff, J. (1987). Multiparty computations ensuring privacy of each party's input and correctness of the result. In Advances in Cryptology - Crypto'87, (LNCS Vol. 293 pp. 87-119). Berlin: Springer-Verlag.
- Chen, B., & Wornell, B. (1999). Dither modulation: A new approach to digital watermarking and information embedding. In *Proceedings of SPIE: Security and Watermarking of Multimedia Contents*, (pp. 342–353).
- Chen, B., & Wornell, G. (2001). Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, 47(4), 1423–1443. doi:10.1109/18.923725
- Chen, X., Zhu, D., & Liu, J. (2007). *A practical digital watermarking protocol based on PKI-CA*. Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, SNPD 2007 (Vol. 1, pp. 483–488). Washington, DC: IEEE Computer Soc.
- Chen, Y.-W., Pan, H.-K., & Tseng, Y.-C. (2000). A Secure data hiding Scheme for two color images. In *Proceedings of 5th IEEE symposium on Computer and Communication*, (pp. 750-755).
- Cheng, Q., & Huang, T. (2001). *An Image Watermarking Technique Using Pyramid Transform*. Proc. Of the ACM Multimedia.
- Cheng, S., Yu, H., & Xiong, Z. (2002). Enhanced spread spectrum watermarking of MPEG-2 AAC. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 3728–3731).
- Cheng, Y.-M., & Wang, C.-M. (2006). A high-capacity steganographic approach for 3D polygonal meshes. *The Visual Computer*, 22(9-11), 845–855. doi:10.1007/s00371-006-0069-4
- Cheng, Y.-M., & Wang, C.-M. (2007). An adaptive steganographic algorithm for 3D polygonal meshes. *The Visual Computer*, 23(9), 721–732. doi:10.1007/s00371-007-0147-2
- Cheung, S. C., & Chiu, D. K. W. (2003). A watermarking infrastructure for enterprise document management. In *Proceedings of 36th annual Hawaii international conference on system sciences* (pp. 105–114).

Compilation of References

- Cheung, S. C., & Curreem, H. (2002). Buyer-Reseller Watermarking Protocol for MP3 Music. In *26th Annual International Computer and Applications Conference (COMPSAC 2002)*, (pp. 105-110).
- Cheung, S., Leung, H., & Wang, C. (2004). A Commutative Encrypted Protocol for the Privacy Protection of Watermarks in Digital Contents. In *37th Annual Hawaii International Conference on System Sciences (HICSS'04)*. Washington, DC: IEEE Computer Society.
- Cho, J.-W., Prost, R., & Jung, H.-Y. (2007). An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms. *IEEE Transactions on Signal Processing*, 55(1), 142–155. doi:10.1109/TSP.2006.882111
- Cho, W.-H., Lee, M.-E., Lim, H., & Park, S.-Y. (2005). Watermarking technique for authentication of 3-D polygonal meshes. In *Proc. of the International Workshop on Digital Watermarking* (pp. 259-270).
- Choi, J. G., Sakurai, K., & Park, J. H. (2003). Does it Need Trusted Third Party? Design of Buyer Seller Watermarking Protocol without Trusted Third Party. In Applied Cryptography and Network Security ACNS'03. (LNCS Vol. 2846, pp. 265-279). Berlin: Springer-Verlag.
- Chotikamthron, N. (1999). Document Image Data Hiding Technique Using Character Spacing Width Sequence Coding. In *Proceedings of IEEE International Conference on Image Processing*, 2, 250–254.
- Chou, C. M., & Tseng, D. C. (2006). A public fragile watermarking scheme for 3D model authentication. *Computer Aided Design*, 38(11), 1154–1165. doi:10.1016/j.cad.2006.06.009
- Chou, C., & Liu, K. (2006). Performance Analysis of Color Image Watermarking Schemes Using Perceptually Redundant Signal Spaces. In *International Conference on Intelligent Information Hiding and Multimedia*, (pp. 651-654).
- Chou, C., & Wu, T. (2003). Embedding color watermarks in color images. *EURASIP Journal on Applied Signal Processing*, 2003, 32–40. doi:10.1155/S1110865703211227
- Chou, J., Pradhan, S. S., & Ramchandran, K. (1999). On the duality between the distributed source coding and data hiding. In 33rd Asilomar conference on Signals, Systems and Computers, 2, 1503-1507.
- Chou, J., Ramchandran, K., & Ortega, A. (2001). High capacity audio data hiding for noisy channels. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, (pp. 108–111).
- Choudhury, A. K., Kristol, D. M., Lapone, A., Brassil, J. T., Low, S. H., Maxemchuk, N. F., & O’Gorman, L. (1996, May). SEPTEMBER—Secure Electronic Publishing Trial. *IEEE Communications Magazine*, 34(5), 48–55. doi:10.1109/35.492972
- Chrysochos, E., Fotopoulos, V., Skodras, A., & Xenos, M. (2007). *Reversible Image Watermarking Based on Histogram Modification* (pp. 93–104). PCI.
- Chu, W. (2003). DCT-Based Image Watermarking Using Subsampling. *IEEE Transactions on Multimedia*, 5(1), 34–38. doi:10.1109/TMM.2003.808816
- Chung, K.-L., Shen, C.-H., & Chang, L.-C. (2001). A novel SVD- and VQ-based image hiding scheme. *Pattern Recognition Letters*, 22(9), 1051–1058. doi:10.1016/S0167-8655(01)00044-7
- Chung, K.-L., Yang, W.-N., Huang, Y.-H., Wu, S.-T., & Hsu, Y.-C. (2007). On SVD-based watermarking algorithm. *Applied Mathematics and Computation*, 188(1), 54–57. doi:10.1016/j.amc.2006.09.117
- Cignoni, P., Rocchini, C., & Scopigno, R. (1998). Metro: Measuring error on simplified surfaces. *Computer Graphics Forum*, 17(2), 167–174. doi:10.1111/1467-8659.00236
- Ciloglu, T., & Karaaslan, S. (2000). An improved all-pass watermarking scheme for speech and audio. In *Proceedings of the IEEE International Conference on Multimedia and Expo*, (pp. 1017–1020).
- Clarke, R. J. (1985). *Transform Coding of Images*. New York: Academic Press.
- Coltuc, D., & Bolon, P. (2000). Color image watermarking in HSI space. In *International Conference on Image Processing* (Vol. 3, pp. 698-701).

- Corvi, M., & Nicchiotti, G. (1997). Wavelet-based image watermarking for copyright protection. In *Proceedings of the Scandinavian Conference on Image Analysis*, (pp. 157 – 163).
- Costa, M. (1983). Writing on dirty paper. *IEEE Transactions on Information Theory*, *IT-29*, 439–441. doi:10.1109/TIT.1983.1056659
- Cover, T. M. (1972). Broadcast Channels. *IEEE Transactions on Information Theory*, *18*, 2–14. doi:10.1109/TIT.1972.1054727
- Cover, T. M., & Thomas, J. A. (1991). *Elements of Information Theory*. Mahwah, NJ: John Wiley & Sons, Inc. doi:10.1002/0471200611
- Cox, I. J., & Linnartz, J. P. M. G. (1997). *Public watermarks and resistance to tampering*. Paper presented at the IEEE International Conference on Image Processing, Washington, DC.
- Cox, I. J., & Miller, M. (1997). A review of watermarking and importance of perceptual modeling. *Proceedings of SPIE Human Vision and Imaging*, *3016*, 92–99.
- Cox, I. J., & Miller, M. L. (2002). Electronic watermarking: The first 50 years. *EURASIP Journal on Applied Signal Processing*, *2*, 126–132. doi:10.1155/S1110865702000525
- Cox, I. J., Kilian, J. F., Leighton, T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, *6*(12), 1673–1687. doi:10.1109/83.650120
- Cox, I. J., Miller, M., & Bloom, J. (2000). Watermarking Applications and Their Properties. In *Proc. of Int. Conf. Information Technology: Coding and Computing*, (pp. 6-10).
- Cox, I. J., Miller, M., Bloom, J., Friedrich, J., & Kalker, T. (2007). *Digital Watermarking and Steganography*. San Francisco: Morgan Kaufmann.
- Cox, I., & Miller, M. (2001). Electronic watermarking: The first 50 years. In *Proceedings of the IEEE Workshop on Multimedia Signal Processing*, (pp. 225–230).
- Cox, I., Kilian, J., Leighton, F. T., & Shamoon, T. (1996). Secure Spread Spectrum Watermarking for Images, Audio and Video. In *Proceedings of the International Conference on Image Processing*, *3*, 243–246.
- Cox, I., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, *6*(12), 1673–1687. doi:10.1109/83.650120
- Cox, I., Miller, M., & Bloom, J. (2001). *Digital Watermarking: Principles & Practice*. San Francisco: The Morgan Kaufmann Series in Multimedia and Information Systems.
- Cox, I., Miller, M., & McKellips, A. (1999). Watermarking as communication with side information. *IEEE Int. Conference on Multimedia Computing and Systems*, (pp. 1127-1141).
- Craver, S., & Katzenbeisser, S. (2001). Copyright Protection Protocols Based on Asymmetric Watermarking. In *Fifth Conference on Communication and Multimedia Security (CMS'01)*, (pp. 159-170). Boston: Kluwer Academic Publishers.
- Craver, S., Memon, N., Yeo, B. L. & Yeung, M. M. (1998). Can invisible watermark resolve rightful ownerships? *IEEE Journal on Selected Areas in Communications. Special issue on copyright & privacy protection*, *16*(4), 573-586.
- Craver, S., Memon, N., Yeo, B. L., & Yeung, M. M. (1998). Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications. *IEEE J. Selec. Areas Comm.* *16*, (4 May), 573–586.
- Craver, S., Yeo, B., & Yeung, M. (1998, July). Technical Trial and Legal Tribulations. *ACM Communication*, *41*(7), 45–54. doi:10.1145/278476.278486
- Curran, K., & Bailey, K. (2003). An evaluation of image based steganography methods. *International Journal of Digital Evidence*, *2*(2), 1–40.

Compilation of References

- Cvejic, N., & Seppänen, T. (2002). Increasing the capacity of LSB-based audio steganography. In *Proceedings of the IEEE International Workshop on Multimedia Signal Processing*, (pp. 336–338).
- Cvejic, N., Keskinarkaus, A., & Seppänen, T. (2001). Audio watermarking using m-sequences and temporal masking. In *Proceedings of the IEEE Workshop on Applications of Signal Processing to Audio and Acoustics*, (pp. 227–230).
- Das, T. S., Mankar, V. H., & Sarkar, S. K. (2007). Performance evaluation of spread spectrum watermarking using error control coding [Dr. M G R University, Chennai, Tamilnadu, India.]. *IET-UK ITCES, 2007*, 708–710.
- Dauwels, J. (2005). Numerical computation of the capacity of continuous memoryless channels. In *26th Symposium on Information Theory*. Benelux.
- Dauwels, J. (2006). *On graphical models for communications and machine learning: algorithms, bounds and analog implementation*. Unpublished Ph.D. thesis, ETH Zürich.
- Davey, M. C., & Mackay, D. J. C. (2001). Reliable communication over channels with insertions, deletions, and substitutions. *IEEE Transactions on Information Theory*, 47(2), 687–698. doi:10.1109/18.910582
- Davoine, F. (2000). *Triangular meshes: A solution to resist to geometric distortions based watermark-removal softwares*. Paper presented at the European Signal Processing Conference, Tampere, Finland.
- Davoine, F., & Pateux, S. (Eds.). (2004). *Tatouage de documents audiovisuels numériques*. Lavoisier.
- Deng, M., & Preneel, B. (2008). On Secure and Anonymous Buyer-Seller Watermarking Protocol. Internet and Web Applications and Services - ICIW '08, (pp. 524-529).
- Depovere, G., Kalker, T., & Linnartz, J. P. (1998). Improved watermark detection reliability using filtering before correlation. In *Proc. of IEEE International Conference on Image Processing (ICIP)*: (Vol. 1, pp. 430–434).
- Deskshare. (2005, October). *Vcd, svcd and dvd quality, capacity and media types*. Retrieved from http://www.deskshare.com/Resources/articles/dmc_VcdQuality.aspx
- Dittman, J., & Steinmetz, A. (1999). Content-based digital signatures for motion pictures authentication and content-fragile watermarking. In *Proceedings of the IEEE ICMCS*, Florence, (pp. 574–579).
- Dodgson, N. A., Floater, M. S., & Sabin, M. A. (Eds.). (2004). *Advances in Multiresolution for Geometric Modelling*. Berlin: Springer-Verlag.
- Doerr, G., & Dugelay, J. (2003). A Guided Tour to Video Watermarking. *Signal Processing Image Communication*, 18, 263–282. doi:10.1016/S0923-5965(02)00144-3
- Dong, P., & Galatsanos, N. P. (2002, September). *Affine transformation resistant watermarking based on image normalization*. Paper presented at the IEEE International Conference on Image Processing, Rochester, NY.
- Dong, P., Brankov, J. G., Galatsanos, N. P., & Yang, Y. (2002, September). *Geometric robust watermarking through mesh model based correction*. Paper presented at the IEEE International Conference on Image Processing, Rochester, NY.
- Dong, P., Brankov, J. G., Galatsanos, N. P., Yang, Y., & Davoine, F. (2005). Digital watermarking robust to geometric distortions. *IEEE Transactions on Image Processing*, 14(12), 2140–2150. doi:10.1109/TIP.2005.857263
- Doulaverakis, C., Vagionitis, S., Zervakis, M., & Petrakis, E. (2004). Adaptive methods for motion characterization and segmentation of MPEG compressed frame sequence. In *1st Intern. Conference on Image Analysis and Recognition (ICIAR'2004), Proc. Part I*. Porto, Portugal. (LNCS 3211, pp. 310-317). Berlin: Springer Verlag.
- Dudani, S. A., Breeding, K. J., & McGhee, R. B. (1977). Aircraft identification by moment invariants. *IEEE Transactions on Computers*, C-26(1), 39–46. doi:10.1109/TC.1977.5009272

- Dugelay, J. L., & Petitolas, F. A. P. (2000). Possible counter-attacks against random geometric distortions. In P. W. Wong and E. J. Delp (Ed.), *Electronic imaging: Vol. 3971. Security and Watermarking of Multimedia Contents II* (pp. 338–345). San Jose, California: The Society for imaging science and technology (IS&T) and the international Society for optical engineering (SPIE.).
- Dugelay, J. L., & Roche, S. (2000). A survey of current watermarking techniques. In Katzenbeisser, S., & Petitolas, F. A. (Eds.), *Information hiding techniques for steganography and digital watermarking* (pp. 121–148). Norwood, MA: Artech House.
- Dumitrescu, S., Wu, W., & Wang, Z. (2003). Detection of LSB steganography via sample pair analysis. *IEEE Transactions on Signal Processing*, 51(7), 1995–2007. doi:10.1109/TSP.2003.812753
- Dumitru, O., Mitrea, M., & Prêteux, F. (2007). Accurate watermarking capacity evaluation. In *Proc. SPIE* (Vol. 6763, pp. 676303:1-12).
- Dupuis, F., Yu, W., & Willems, F. (2004). Blahut-Arimoto algorithms for computing channel capacity and rate-distortion with side information. In *Proc. IEEE International Symposium on Information Theory*, (pp. 181).
- Duta, S. (2009). *Robust video watermarking as an information theory application*. Unpublished PhD thesis, Université Paris V, France.
- Duta, S., Mitrea, M., & Prêteux, F. (2008). Capacity evaluation for MPEG-4 AVC watermarking. In *Proc. SPIE*, (Vol. 7000, pp. 70000V:1-10).
- Duta, S., Mitrea, M., Prêteux, F., & Belhaj, M. (2008). MPEG-4 AVC domain watermarking transparency. In *Proc. SPIE*, (Vol. 6982, pp. 69820F:1-10).
- DWA. (2008). Retrieved from <http://www.digitalwatermarkingalliance.org/default.asp>
- Ebner, M., Tischler, G., & Albert, J. (2007). Integrating Color Constancy Into JPEG2000. *Image Processing. IEEE Transactions on*, 16(11), 2697–2706.
- Echizen, I., Yamada, T., Fujii, Y., Tezuka, S., & Yoshiura, H. (2005). Real-time video watermark embedding system using software on personal computer. In *Proceedings of the IEEE International Conference on System, Man and Cybernetics*, (pp. 3369 - 3373).
- Eggers, J. J., Bauml, R., Tzhoppe, R., & Girod, B. (2003). Scalar Costa scheme for information embedding. *IEEE Transactions on Signal Processing*, 51(4), 1003–1019. doi:10.1109/TSP.2003.809366
- Eggers, J., & Girod, B. (2002). *Informed Watermarking*. Amsterdam: Kluwer Academic Publishers.
- Ejima, M., & Myazaki, A. (2001). On the evaluation of performance of digital watermarking in the frequency domain. In *Proceedings of the IEEE International Conference on Image Processing*, Thessaloniki, Greece.
- El Areef, T., Heniedy, H. S., & Ouda, O. M. (2006). Performance evaluation of image watermarking techniques. In *Proceedings of the 4th International Conference on Information & Communications Technology*, (pp. 1-1).
- El Zouka, H. (2008). FPGA based implementation of robust watermarking system. In *Fifth International Conference on Information Technology*, (pp. 1274- 1278).
- Elad, A., & Kimmel, R. (2003). On bending invariant signatures for surfaces. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(10), 1285–1295. doi:10.1109/TPAMI.2003.1233902
- Elbasi, E., & Eskicioglu, A. (2006). A Semi-Blind Watermarking Scheme for Color Images Using a Tree Structure. In *Western New York Image Processing Workshop* (pp. 1-8).
- EMC. (2009). *The digital universe*. EMC Corporation. Retrieved June 1, 2009, from <http://www.emc.com/> / digital_universe
- Engedy, M., Parasad, M. V. N. K., & Saxena, A. (2006). Singular Value Decomposition (SVD) Based Attack on Different Watermarking Schemes. *Computing Letters*, 2(3), 149–154. doi:10.1163/157404006778330843

Compilation of References

- Erelebi, E., & Bataki, L. (2009). Audio watermarking scheme based on embedding strategy in low frequency components with a binary image. *Digital Signal Processing*, 19(2), 265–277. doi:10.1016/j.dsp.2008.11.007
- Ericsson. (2009). Retrieved from <http://www.ericsson.com/ericsson/successtories/>
- Esen, E., & Alatan, A. A. (2004). *Data Hiding using Trellis Coded Quantization*. ICIP.
- Esen, E., Alatan, A. A., & Askar, M. (2003). *Trellis coded quantization for data hiding*. Ljubljana, Slovenia: EUROCON.
- Eskicioglu, A. M., & Delp, E. J. (2001). An overview of multimedia content protection in consumer electronics devices. *Signal Processing Image Communication*, 16, 681–699. doi:10.1016/S0923-5965(00)00050-3
- Eyadat, M., & El-Ddin, I. (2005). Compression Standards Roles in Image processing: Case Study. In *ITCC'05 (Vol. II)*, pp. 135–140). Washington, DC: IEEE.
- Fairchild, M. D., & Johnson, G. M. (2004). iCAM framework for image appearance, differences, and quality. *Journal of Electronic Imaging*, 13(1), 126–138. doi:10.1117/1.1635368
- Fan, M.-Q., Wan, H.-X., & Li, S.-K. (2008). Restudy on SVD-based watermarking scheme. *Applied Mathematics and Computation*, 203(2), 926–930. doi:10.1016/j.amc.2008.05.003
- Fan, Y. C., Van, L. D., Huang, C. M., & Tsao, H. W. (2005) Hardware-efficient architecture design of wavelet-based adaptive visible watermarking. In *Proceedings of the 9th IEEE international symposium on consumer electronics*, (pp. 399–403).
- Fan, Y.-C., & Tsao, H.-W. (2005). A dual pyramid watermarking for JPEG-2000. In *The First International Workshop on Information Networking and Applications*.
- Fei, C., Kundur, D., & Kwong, R. (2004). Analysis and Design of Watermarking Algorithms for Improved Resistance to Compression. *IEEE Transactions on Image Processing*, 13(2), 126–144. doi:10.1109/TIP.2004.823830
- Feng, G. R., Jiang, L. G., He, C., & Xue, Y. (2006). Chaotic spread spectrum watermark of optimal space-filling curves. *Chaos, Solitons, and Fractals*, 2, 580–587. doi:10.1016/j.chaos.2005.04.051
- Ferrer, J. D. (1999). Anonymous fingerprinting based on committed oblivious transfer. *Public Key Cryptography*, (LNCS Vol. 1560, pp. 43-52). Berlin: Springer-Verlag.
- Ferrer, J. D., & Herrera-Joancomartí, J. (1998). *A privacy homomorphism allowing field operations on encrypted data*. *Jornades de Matemàtica Discreta i Algorísmica*. Spain: University Rovira i Virgili.
- Ferrer, J. D., & Herrera-Joancomartí, J. (2000). Efficient smart-card based anonymous fingerprinting. *Smart Card Research and Applications*. (LNCS Vol. 1820, pp. 231-238). Berlin: Springer-Verlag.
- Ferrer, J. D., & Sebe, F. (2002). Enhancing watermark robustness through mixture of watermarked digital objects. *International Conference on Information Technology: Coding and Computing - ITCC'2002*. (pp. 85-89). Washington, DC: IEEE Computer Society.
- Fetscherin, M., & Schmid, M. (2003) Comparing the usage of Digital Rights Management Systems in Music, Film, and Print Industry. In *Proceedings of the 5th international conference on Electronic commerce*, 50, (pp. 316-325).
- Fischer, R. F. H., (2005). The Modulo-Lattice Channel: The key Feature in Precoding Schemes. *International Journal of Electronics and Communications*, 244-253.
- Fleet, D., & Heeger, D. (1997). Embedding invisible information in color images. In *1997 Proceedings International Conference on Image Processing*, (Vol. 1, pp. 532-535).
- Flusser, J., & Suk, T. (1993). Pattern Recognition by affine moment invariants. *Pattern Recognition*, 26, 167–174. doi:10.1016/0031-3203(93)90098-H
- Foo, S. W., Yeo, T. H., & Huang, D. Y. (2001). An adaptive audio watermarking system. In *Proceedings of the IEEE Region 10 International Conference on Electrical and Electronic Technology*, (pp. 509–513).

- Forney, G. D. Jr. (1973). The Viterbi algorithm. *Proceedings of the IEEE*, 61, 268–278. doi:10.1109/PROC.1973.9030
- Forssen, P.-E., Granlund, G., & Wikiund, J. (2002). *Channel representation of colour images*. (Tech. Rep. LiTH-ISYR-2418), Computer Vision Laboratory, Department of Electrical Engineering [Linkoping, Sweden]. *Linkoping University, SE-581, 83.*
- Fox, D., O’Gorman, L., & Story, G. A. (1992, September). The RightPages Image-Based Electronic Library for Altering and Browsing. *IEEE Computer*, 25(9), 17–26.
- Fre. (2009). Retrieved from <http://www.freshpatents.com/System-and-method-for-enriched-multimedia-conference-IBM>.
- Freeman, W. T., Anderson, D. B., Beardsley, P. A., Dodge, C. N., Roth, M., Weissman, C. D., et al. (1998). Computer Vision for Interactive Computer Graphics. In *Proceedings, IEEE Computer Graphics and Applications: Special issue on Computer Graphics I/O Devices*, 18(3), 42-53. Los Alamitos, CA: IEEE Computer Society Press.
- Fretland, T., Fritsch, L., & Grove, A. K. (2008). *State of the art in Digital Rights Management*. MARIAGE.
- Fridrich, J. (1999). Methods for tamper detection in digital images. In *Proc. of ACM Workshop on Multimedia and Security* (pp. 19-23). Orlando, FL: ACM
- Fridrich, J., Goljan, M., & Baldoza, A. C. (2000). New fragile authentication watermark for images. In *Proceedings of the IEEE international conference of image processing (ICIP)*, (pp. 446–449).
- Fridrich, J., Goljan, M., & Du, R. (2001). Distortion-free data embedding. *Lecture Notes in Computer Science*, 2137, 27–41. doi:10.1007/3-540-45496-9_3
- Fridrich, J., Goljan, M., & Du, R. (2002). Lossless data embedding—New paradigm in digital watermarking. *Applied Signal Processing*, (2): 185–196.
- Furht, B., & Kirovski, D. (2006). *Multimedia Watermarking Techniques and Applications*. Boca Raton, FL: CRC Press.
- Furon, T., & Duhamel, P. (2003). An asymmetric watermarking method. *IEEE Transactions on Signal Processing*, 51(4), 981–995. doi:10.1109/TSP.2003.809376
- Gang, L., Akansu, A., & Ramkumar, M. (2001). MP3 resistant oblivious steganography. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, (pp. 1365–1368).
- Ganic, E., & Eskicioglu, A. M. (2004). Robust DWT-SVD domain image watermarking: embedding data in all frequencies. In *Proceedings of the 2004 workshop on Multimedia and security* (pp. 166-174). New York: ACM Press.
- Ganic, E., Zubair, N., & Eskicioglu, A. M. (2003). An Optimal Watermarking Scheme Based on Singular Value Decomposition. In *Proceedings of the International Conference on Communication, Network, and Information Security* (pp. 85-90).
- Gantz, J. F., Chute, C., Manfrediz, A., Minton, S., Reinsel, D., Schlichting, W., & Toncheva, A. (2008). *The diverse and exploding digital universe*. An IDC White Paper, (pp. 1-16). Framingham, MA: IDC.
- Gantz, J., & Reinsel, D. (2009). *As the economy contracts, the digital universe expands*. IDC – Multimedia white paper, 1-10.
- Gao, K.-L., Dong, M., & Zhou, F.-Q. (2006). An image hiding algorithm using Arnold transform and technique of singular value. In Yunlong, S. (Eds.), *Optical Information Processing* (Vol. 6027, pp. 361–368). Bellingham, WA: SPIE Press.
- Gao, X., & Tang, X. (2002). Unsupervised Video-Shot Segmentation and Model-Free Anchorperson Detection for News Video Story Parsing. *IEEE Trans. Circuits and Systems for Video Technology*, 12(9), 765–776. doi:10.1109/TCSVT.2002.800510
- Garimella, A., Satyanarayana, M., Kumar, R., Murugesh, P., & Nirajan, U. (2003). VLSI implementation of online digital watermarking technique with difference encoding for 8-bit gray scale images. In *Proceedings of the 16th International Conference on VLSIDesign*, (pp. 283-288).

Compilation of References

- Garimella, A., Satyanarayana, M., Murugesh, P., & Niranjan, U. (2004). ASIC for digital color image watermarking. In IEEE 11th Digital Signal Processing Workshop & IEEE Signal Processing Education Workshop, (pp. 292 - 296).
- Gel'fand, S. I., & Pinsker, M. S. (1980). Coding for channel with random parameters. *Problems of Control and Information Theory*, 9(1), 19–31.
- Ghazy, R., El-Fishawy, N., Hadhoud, M., Dessouky, M., & El-Samie, F. (2007). An efficient block-by block SVD-based image watermarking scheme. *Ubiquitous Computing and Communication*, 2(5), 1–9.
- Ghosh, A., & Pal, S. K. (Eds.). (2002). *Soft computing approaches to pattern recognition and Image processing*. Singapore: World Scientific Press.
- Ghosh, S., Roy, P., Maity, S. P., & Rahaman, H. (2009). Spread Spectrum Image watermarking with Digital Design. In *Proceedings of IEEE International Advanced Computing conference (IACC 2009)*, Patiala, India, (pp. 868-873).
- Goi, B., Chung-Wei, R., Yang, Y., Bao, F., Deng, R. H., & Siddiqi, M. U. (2004). Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity. *Applied Cryptography and Network Security - ACNS 2004*. (LNCS Vol. 3089, pp. 369-382). Berlin: Springer-Verlag.
- Golub, G. H., & Loan, C. F. V. (1996). *Matrix Computations*, (3rd). Baltimore, MD: The Johns Hopkins University Press.
- Goodall, C., & Mardia, K. (1999). Projective shape analysis. *Journal of Computational and Graphical Statistics*, 8(2), 143–168. doi:10.2307/1390631
- Gorodetski, V. I., & Samoilov, V. (2003). Simulation-Based Exploration of SVD-Based Technique for Hidden Communication by Image Steganography Channel. In Gorodetski, V. I. (Eds.), *Computer Network Security* (Vol. 2776, pp. 349–359). Berlin: Springer-Verlag.
- Gorodetski, V. I., Popyack, L. J., Samoilov, V., & Skormin, V. (2001). SVD-Based Approach to Transparent Embedding Data into Digital Images. In Gorodetski, V. I. (Eds.), *Information Assurance in Computer Networks* (Vol. 2052, pp. 263–274). Berlin: Springer-Verlag. doi:10.1007/3-540-45116-1_26
- Gorodetski, V., Skormin, V., & Popyack, L. (2000). SVD approach to Digital Image Lossy Compression. In *Proceedings of the 4th Conference on Systems, Cybernetics and Informatics*.
- Grody, J., & Brutun, L. (2000). Performance Evaluation of Digital Audio Watermarking algorithms. In *Proceedings of the 43rd IEEE Midwest Symposium on Circuits and Systems*, (pp. 456-459).
- Guerchi, D., & Rabie, T. (2007). Narrowband CELP Hiding by Wideband Speech. *The Ninth IASTED International Conference on Signal and Image Processing (SIP 2007)*, Honolulu, Hawaii, USA.
- Guerchi, D., Harmain, H., Rabie, T., & Mohamed, E. (2008). Speech Secrecy: An FFT-based Approach. *International Journal of Mathematics and Computer Science*, 3(2), 1–19.
- Guillon, P., Furion, T., & Duhamel, P. (2002). Applied public-key steganography. In *Proceedings of SPIE*, San Jose, CA.
- Guitart, O., Kim, H. C., & Delp, E. J. (2006). Watermark evaluation test-bed. *J. Electr. Imag.*, 15(4).
- Guo, H., & Georganas, N. (2002). Multi-resolution Image Watermarking Scheme in the Spectrum Domain. In *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering*, Canada.
- Gutub, A. A., & Fattani, M. (2007, May). A Novel Arabic Text Steganography Method Using Letter Points and Extensions. In *WAST International Conference on Computer, Information and Systems Sciences and Engineering*, Vienna, Austria, (pp. 28-31).

- Guzman, V., Miyatake, M., & Meana, H. (2004). Analysis of Wavelet –Based Watermarking Algorithm. In *Proceedings of the 14th International IEEE Conference on Electronics, Communications and Computers*, Veracruz, Mexico.
- Haghghi, M. S., & Ghaemmaghami, S. (2005). An Optimal SVD-based Watermarking Framework through Linear Programming. In Hamza, M. H. (Ed.), *European Internet and Multimedia Systems and Applications* (pp. 271–274).
- Hanzo, L., Cherriaman, P. J., & Streit, J. (2001). Wireless video communication: second to third generation systems and beyond. In *IEEE series on digital and mobile communication*. New York: IEEE.
- Haouzia, A., & Noumeir, R. (2008). Methods for image authentication: a survey. *Multimedia Tools and Applications*, 39(1), 1–46. doi:10.1007/s11042-007-0154-3
- Harris, C., & Stephens, M. (1988). A combined corner and edge detector. In *Proceedings Fourth Alvey Vision Conference*, (pp. 147-151).
- Harte, T., & Bors, A. (2002). Watermarking 3D models. In *Proceedings 2002 International Conference on Image Processing*, (Vol. 3, pp. 661 – 664).
- Hartung, F., & Kutter, M. (1999). Multimedia watermarking techniques. *Proceedings of the IEEE*, 87(7), 1079–1107. doi:10.1109/5.771066
- Hartung, H., & Girod, B. (1998). Watermarking of Compressed and Un-Compressed Video. *Signal Processing*, 66(3), 283–301. doi:10.1016/S0165-1684(98)00011-5
- Hassanien, A. E., Abraham, A. & Grosan, C. (2009). Spiking neural network and wavelets for hiding iris data in digital images. *Bio-inspired information hiding: A fusion of foundations, methodologies and applications*, 13(4), 401-416.
- He, X. & Scordilis, M. S. (2008). Efficiently synchronized spread-spectrum audio watermarking with improved psychoacoustic model. *Research letters in Signal Processing*, 2008 (1), 1-5.
- Heileman, G. L., Pizano, C. E., & Abdallah, C. T. (1999). Performance measures for image watermarking schemes. In *Proceedings of the 5th Baiona Workshop on Emerging Technologies in Telecommunications*, (pp. 149–152).
- Hernandez, J. R., & Perez Gonzalez, F. (1999). Statistical analysis of watermarking schemes for copyright protection of images. *Proceedings of the IEEE*, 87(7), 1142–1146. doi:10.1109/5.771069
- Hernandez, J. R., Amado, M., & Perez Gonzalez, F. (2000). DCT domain watermarking techniques for still images: Detector performance analysis and a new structure. *IEEE Transactions on Image Processing*, 9(1), 55–68. doi:10.1109/83.817598
- Hernández, J. R., Delaigle, J.-F., & Macq, B. (2000). *Improving data hiding by using convolutional codes and soft-decision decoding*. SPIE (pp. 24–48). San Jose, CA: Security and Watermarking of Multimedia Contents II.
- Higuero, M. V. (2005). *Modelo de distribución de contenidos digitales marcados en Internet, con protección de derechos de copyright. Evaluación y optimización de la seguridad del protocolo mediante metodologías de análisis de riesgos*. Unpublished doctoral dissertation, University of the Basque Country, Spain.
- Ho, A. T. S., Shen, J., Chow, A. K. K., & Woon, J. (2003). Robust digital image-in-image watermarking using the fast Hadamard transform. In *Proceedings of the international symposium on circuits and systems (ISCAS 2003)*, (pp. 826–829).
- Holliman, M., & Memon, N. (2000). Counterfeiting attack on oblivious block wise independent invisible watermarking schemes. *IEEE Transactions on Image Processing*, 9, 432–441. doi:10.1109/83.826780
- Honsinger, C. (2000). *Data embedding using phase dispersion*. IEE Seminar on Secure Images and Image Authentication (Ref. No. 2000/039), (pp. 5/1–5/7). Rochester, NY: Eastman Kodak Co.
- Hou, Z. (2003). Adaptive singular value decomposition in wavelet domain for image denoising. *Pattern Recognition*, 36(8), 1747–1763. doi:10.1016/S0031-3203(02)00323-0

Compilation of References

- Hsiao, S.-F., Tai, Y.-C., & Chang, K.-H. (2000). VLSI design of an efficient embedded zerotree wavelet coder with function of digital watermarking. *IEEE Transactions on Consumer Electronics*, 46(3), 628–636. doi:10.1109/30.883423
- Hsieh, M., Tseng, D., & Huang, Y. (2001). Hiding Digital Watermarks Using Multiresolution Wavelet Transform. *IEEE Transactions on Industrial Electronics*, 48(5), 875–882. doi:10.1109/41.954550
- Hsieh, M.-S., & Tseng, D.-C. (2006). Wavelet-based Color Image Watermarking using Adaptive Entropy Casting. In *Multimedia and Expo, 2006 IEEE International Conference on* (pp. 1593–1596).
- Hsu, C., & Wu, J. (1998). Multiresolution Watermarking for Digital Images. *IEEE Transactions on IEEE Transactions on Circuits and Systems II*, 45(8), 1097–1101. doi:10.1109/82.718818
- Hu, M. K. (1961). Pattern recognition by moment invariants. In *Proceedings of IRE (Correspondence)*, 49, 1428–1961.
- Hu, M. K. (1962). Visual pattern recognition by moment invariants. *I.R.E. Transactions on Information Theory*, 8, 179–187. doi:10.1109/TIT.1962.1057692
- Hu, Y., & Kwong, S. (2001, September). Wavelet domain adaptive visible watermarking. *Electronics Letters*, 37(20), 1219–1220. doi:10.1049/el:20010838
- Hua, X. S., Feng, J. F., & Shi, Q. Y. (2001). Public multiple watermarking resistant to cropping. In *Proceedings of the 6th International Conference on Pattern Recognition and Information Processing*, (pp. 263–268).
- Huang, D. & Yan, H. (2001, December). Interword Distance Changes Represented by Sine Waves for Watermarking Text Images. *IEEE Transaction on Circuits and Systems for video technology*, 11(12), 1237-1245.
- Huang, D. Y., & Yeo, Y. H. (2002). Robust and inaudible multi-echo audio watermarking. In *Proceedings of the IEEE Pacific-Rim Conference on Multimedia*, (pp. 615–622).
- Huang, F. J., & Guan, Z. H. (2004). A hybrid SVD-DCT watermarking method based on LPSNR. *Pattern Recognition Letters*, 25(15), 1769–1775. doi:10.1016/j.patrec.2004.07.003
- Huang, H., Chu, C., & Pan, J. (2008). The optimized copyright protection system with genetic watermarking. *Soft Computing*, 13(4), 333–343. doi:10.1007/s00500-008-0333-9
- Huang, J., & Yang, C. (2004). Image Digital Watermarking Algorithm Using Multiresolution Wavelet Transform. In *Proceedings of the International IEEE Conference on Systems, Man, and Cybernetics*, the Hague, the Netherlands.
- Huang, P. S., & Chiang, C. (2005). Novel and robust saturation watermarking in wavelet domains for color images. *Optical Engineering (Redondo Beach, Calif.)*, 44(11), 117002. doi:10.1117/1.2128416
- Huang, T., Burnett, J., & Deczky, A. (1975). The importance of phase in image processing filters. *IEEE Trans. on ASSP*, 23(6), 529–542. doi:10.1109/TASSP.1975.1162738
- Hurtung, F., & Kutter, M. (1999, July). Multimedia Watermarking Techniques. *Proceedings of the IEEE*, 87(7), 1079–1107. doi:10.1109/5.771066
- Hwang, M. S., Chang, C. C., & Hwang, K. F. (2000). Digital watermarking of images using neural networks. *Journal of Electronic Imaging*, 9, 548–555. doi:10.1117/1.1289357
- Hyvärinen, A., & Oja, E. (1997). A fast fixed-point algorithm for independent component analysis. *Neural Computation*, 9(7), 1484–1492. doi:10.1162/neco.1997.9.7.1483
- Hyvärinen, A., & Oja, E. (1999). *Independent component analysis: A tutorial*. Notes for International Joint Conference on Neural Networks, Washington, DC.
- Hyvärinen, A., Karhunen, J., & Oja, E. (2001). *Independent Component Analysis*. New York: Wiley-Interscience. doi:10.1002/0471221317

- Iannella, R. (2001). Digital rights management (DRM) architectures. *D-Lib Magazine*, 7(6). Retrieved May 15, 2009, from <http://www.dlib.org/dlib/june01/iannella/06iannella.html>
- IBM. (2001). *Watermark standarization for DVD copy protection*. Retrieved May, 15, 2009, from http://www.trl.ibm.com/projects/RightsManagement/datahiding/dhvgx_e.htm
- Ikeda, M., Takeda, K., & Itakura, F. (1999). Audio data hiding use of bandlimited random sequences. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 2315–2318).
- Irisa. (2009). Retrieved from <http://www.irisa.fr/temics/research/>
- ISO. (2005). ISO/IEC 14496-10 (2005).
- Jain, A., Uludag, U., & Hsu, R. (2002). Hiding a face in a fingerprint image. In *Proc. International Conference on Pattern Recognition (ICPR)*, Quebec City, Canada.
- Jain, C., Arora, S., & Prasanta, P. K. (2008Submitted to). *A reliable SVD based watermarking scheme*. Elsevier.
- Jain, V., & Zhang, H. (2007). A spectral approach to shape-based retrieval of articulated 3D models. *Computer Aided Design*, 39(5), 398–407. doi:10.1016/j.cad.2007.02.009
- Jeong, Y.-J., Moon, K.-S., & Kim, J.-N. (2007). FPGA based implementation of real-time video watermarking chip. *LNCS*, 4523, 133–141.
- Johnson, N. F., & Katzenbeisser, S. (2000). A survey of steganographic techniques. In Katzenbeisser, S., & Petitcolas, F. A. P. (Eds.), *Information Hiding techniques for steganography and digital watermarking*. Boston: Artech House.
- Johnson, N., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, 31(2), 26–34. doi:10.1109/MC.1998.4655281
- Johnston, J. (1988). Estimation of perceptual entropy using noise masking criteria. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 2524–2527).
- Ju, H. S., Kim, H. J., Lee, D. H., & Lim, J. I. (2002). An anonymous buyer-seller watermarking protocol with anonymity control. In *Information Security and Cryptology-ICISC 2002*, (LNCS Vol. 2587, pp. 421-432). Berlin: Springer-Verlag.
- Jung, H., Cho, S., & Shik, S. Koh, Chung, Y., Lee, K., Lee, S. & Kim, C. (2003). Image Watermarking Based on Wavelet Transform Using Threshold Selection. In *Proceedings of the International IEEE SICE Conference*.
- Jung, H.-S., Lee, Y.-Y., & Lee, S. (2004). Scene-based RST-resilient videowatermarking technique. *EURASIP Journal on Applied Signal Processing*, 14, 2113–2131. doi:10.1155/S1110865704405046
- Kabal, P. (2002). *An Examination and Interpretation of ITU-R BS. 1387: perceptual evaluation of audio quality*. Technical report, Department of Electrical and Computer Engineering, Mc Gill University. Retrieved from <http://www.tsp.ece.mcgill.ca>
- Kalker, T., Depovere, G., Haitsma, J., & Maes, M. (1999). A video watermarking system for broadcast monitoring. In *Proceedings of the SPIE: Security and Watermarking of Multimedia Contents*, 3657, 103–112.
- Kanai, S., Date, H., & Kishinami, T. (1998). Digital watermarking for 3D polygons using multiresolution wavelet decomposition. In *Proc. of the International Workshop on Geometric Modeling: Fundamentals and Applications*, (pp. 296–307).
- Kang, H. I., & Delp, E. J. (2004). *An image normalization based watermarking scheme robust to general affine transformation*. Paper presented at the IEEE International Conference on Image Processing, Singapore.
- Kardamis, J. (2007). *Audio Watermarking Techniques using Singular Value Decomposition*. Unpublished master dissertation, Rochester Institute of Technology, Rochester, NY.
- Karmani, S., Djemal, R., & Tourki, R. (2007). A blind watermarking algorithm implementation for digital images and video. *International Journal of Soft Computing*, 2(2), 292–301.

Compilation of References

- Karmani, S., Djemal, R., & Tourki, R. (2009). 2D-scan-based wavelet watermarking for image and video. In *Computer Standards & Interfaces* (pp. 801–811). Efficient Hardware Architecture of.
- Karni, Z., & Gotsman, C. (2000). Spectral compression of mesh geometry. In *Proc. of the ACM Siggraph* (pp. 279-286).
- Katzenbeisser, S., & Petitcolas, F. (2000). *Information Hiding: Techniques for Steganography and digital watermarking*. Boston: Artech House.
- Kaufman, J., & Celenk, M. (2006). Digital Video Watermarking using Singular Value Decomposition and 2D Principal Component Analysis. In *Proceedings of the 2006 IEEE International Conference on Image Processing* (pp. 2561-2564).
- Kejariwal, A., Gupta, S., & Nicolau, A. (2006). Energy efficient watermarking on mobile devices using proxy-based partitioning. *IEEE Transactions on Very Large Scale Integration Systems*, 14(6), 625–636. doi:10.1109/TVLSI.2006.878218
- Kendall, D., Barden, D., Carne, T., & Le, H. (1999). *Shape and Shape Theory*. New York: Wiley.
- Khan, A., & Mirza, A. (2007). Genetic perceptual shaping: utilizing cover image and conceivable attack information using genetic programming. *Information Fusion*, 8(4), 354–365. doi:10.1016/j.inffus.2005.09.007
- Khisti, A., Erez, U., Lapidoth, A., & Wornell, G. (2007). Carbon Copying Onto Dirty Paper. *IEEE Transactions on Information Theory*, 53, 1814–1827. doi:10.1109/TIT.2007.894693
- Kim, H. C., Ogunleye, H., Guitart, O., & Delp, E. J. (2004). The watermark evaluation testbed (WET). In *Proceedings of SPIE Electronic Imaging*, 5306, 236–247.
- Kim, H. S., & Lee, H. K. (2003). Invariant image watermark using Zernike moments. *IEEE Transactions on Circuits System and Video Technology*, 13, 766–775. doi:10.1109/TCSVT.2003.815955
- Kim, H., & Choi, Y. (2003). A Novel Echo-hiding Scheme with backward and Forward Kernels. *IEEE Transactions on Circuits and Systems for Video Technology*, 13(8), 885–889. doi:10.1109/TCSVT.2003.815950
- Kim, K.-S., Lee, H.-Y., IM, D.-H., & Lee, H.-K. (2008). Practical, real-time, and robust watermarking on the spatial domain for high-definition video contents. *IEICE Transactions on Informations and Systems*, (5), 1359 - 1368.
- Kim, K.-S., Lee, M.-J., & Lee, H.-K. (2007). Blind Image Watermarking Scheme in DWT-SVD Domain. In *Proceedings of the 3rd IEEE International Conference on Intelligent Information Hiding and Multimedia Digital Processing* (pp. 477-480).
- Kim, Y., Moon, K., & Oh, I.-S. (2003). A Text Watermarking Algorithm based on Classification and Inter-word Space Statistics. In *Proc of 7th International Conference on Document Analysis and Recognition '03 (ICDAR '03)*, (pp. 775-779).
- Kim, Y.-K., Sutivong, A., & Sigurjonsson, S. (2004). Multiple User Writing on Dirty Paper. *IEEE Int. Symp. Information Theory*, 534.
- Kirovski, D., & Malvar, H. (2001). Robust covert communication over a public audio channel using spread spectrum. In *Proceedings of the Information Hiding Workshop*, (pp. 256–269).
- Kirovski, D., & Malvar, H. (2003). Spread Spectrum watermarking of Audio Signals. *IEEE Transactions on Signal Processing*, 51(4), 1020–1033. doi:10.1109/TSP.2003.809384
- Kitchen, L., & Rosenfeld, A. (1982). Gray-level corner detection. *Pattern Recognition Letters*, 1(2), 95–102. doi:10.1016/0167-8655(82)90020-4
- Ko, B. S., Nishimura, R., & Suzuki, Y. (2002). Time-spread echo method for digital audio watermarking using PN sequences. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 2001–2004).

- Ko, B. S., Nishimura, R., & Suzuki, Y. (2005). Time-spread echo method for digital audio watermarking. *IEEE Transactions on Multimedia*, 7(2), 212–221. doi:10.1109/TMM.2005.843366
- Koch, E., & Zhao, J. (1995). Towards robust and hidden image copyright labeling. In *Proceedings of the International Workshop on Nonlinear Signal Image Processing*, (pp. 452 – 455).
- Koepf, W. (1998). *Hypergeometric Summation - An Algorithmic Approach to Summation and Special Function Identities*. Germany: Vieweg.
- Kong, W., Yang, B., Wu, D., & Niu, X. (2006). SVD Based Blind Video Watermarking Algorithm. In *Proceeding of the First International Conference on Innovative Computing, Information and Control*, 1, 265–168.
- Kougianos, E., Mohanty, S. P., & Mahapatra, R. N. (2009, March). Hardware assisted watermarking for multimedia. *International Journal on Computers and Electrical Engineering*, 35(2), 339–358. doi:10.1016/j.compeleceng.2008.06.002
- Krawtchouk, M. (1929). Sur une généralisation des polynomes d'Hermite. *C. R. Acad. Sci.*, 189(17), 620–622.
- Kumar, K. S., & Sreenivas, T. (2007). Increased watermark-to-host correlation of uniform random phase watermarks in audio signals. *Signal Processing*, 87, 61–67. doi:10.1016/j.sigpro.2006.04.005
- Kumsawat, P., & Attakitmongcol, K. (2005). A new approach for optimization in image watermarking by using genetic algorithms. *IEEE Transactions on Signal Processing*, 53(12), 4707–4719. doi:10.1109/TSP.2005.859323
- Kundur, D., & Hatzinakos, D. (1997). A robust digital image watermarking method using wavelet-based fusion. In *International Conference on Image Processing* (Vol. 1, pp. 544-547).
- Kundur, D., & Hatzinakos, D. (2001). Diversity and attack characterization for improved robust watermarking. *IEEE Transactions on Signal Processing*, 49(10), 2383–2396. doi:10.1109/78.950793
- Kundur, D., & Hatzinakos, D. (2004). Toward robust logo watermarking using multiresolution image fusion principles. *Multimedia. IEEE Transactions on*, 6(1), 185–198.
- Kundur, D., Su, K., & Hatzinakos, D. (2004). Digital Video Watermarking: Techniques, Technology, and Trends. In Pan, P., Huang, H., & Jain, L. (Eds.), *Intelligent Watermarking Techniques* (pp. 265–314). Singapore: World Scientific Computing.
- Kuo, S. S., Johnston, J., Turin, W., & Quackenbush, S. (2002). Covert audio watermarking using perceptually tuned signal independent multiband phase modulation. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 1753–1756).
- Kuribayashi, M., & Morii, M. (2008). On the implementation of asymmetric fingerprinting protocol. In *16th European Signal Processing Conference (EUSIPCO-2008)*. European Association for Signal Processing.
- Kuribayashi, M., & Tanaka, H. (2001). A new anonymous fingerprinting scheme with high enciphering rate. In *Progress in Cryptology - INDOCRYPT 2001*. (LNCS Vol. 2247, pp. 30-39). Berlin: Springer-Verlag.
- Kuribayashi, M., & Tanaka, H. (2004). *A watermarking scheme applicable for fingerprinting protocol. Digital Watermarking* (Vol. 2939, pp. 532–543). Berlin: Springer-Verlag.
- Kutter, M. (1999). Performance improvement of spread spectrum based image watermarking schemes through M-ary modulation. In A. Pfitzmann (Ed.), *Third International Workshop on Information Hiding, Steganography: Paradigms and Examples* (LNCS Vol. 1728, pp. 238–250). Berlin: Springer.
- Kutter, M., & Petitcolas, F. A. P. (1999). A fair benchmark for image watermarking systems. In *Proc. of the SPIE Electronic Imaging*, (vol. 3657, pp. 226–239).
- Kutter, M., & Winkler, S. (2002). A vision-based masking model for spread-spectrum image watermarking. *IEEE Transactions on Image Processing*, 11, 16–25. doi:10.1109/83.977879

Compilation of References

- Kutter, M., Jordan, F., & Bossen, F. (1997). Digital signature of color images using amplitude modulation. In *Storage and retrieval for image and video databases* (Vol. 3022, pp. 518–526). SPIE.
- Kutter, M., Jordon, F., & Bossen, F. (1998). Digital watermarking of color images using amplitude modulation. *Journal of Electronic Imaging*, 7(2), 326–332. doi:10.1117/1.482648
- Lai, C.-C., Huang, H.-C., & Tsai, C.-C. (2008). Image Watermarking Scheme Using Singular Value Decomposition and Micro-genetic Algorithm. In *Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 469–472).
- Lamarche, L., Liu, Y., & Zhao, J. (2006). Flaw in SVD-based Watermarking. In *Proceedings of the Canadian Conference on Electrical and Computer Engineering* (pp. 2082–2085).
- Lancini, R., Mapelli, F., & Tubaro, S. (2002). Embedding indexing information in audio signal using watermarking technique. *Proceedings of EURASIP-IEEE Region 8 International Symposium on Video/Image Processing and Multimedia Communications*, (pp. 257–261).
- Langelaar, G., Setyawan, I., & Lagendijk, R. (2000). Watermarking Digital Image and Video Data: A State-of-Art Overview. *IEEE Signal Processing Magazine*, 17(5), 20–46. doi:10.1109/79.879337
- Lavoué, G., Denis, F., & Dupont, F. (2007). Subdivision surface watermarking. *Computers & Graphics*, 31(3), 480–492. doi:10.1016/j.cag.2007.01.022
- Le Leguelvouit, G. (2005). *Trellis coded quantization for Public key steganography*. Philadelphia, USA: ICASSP.
- Lee, C.-H., & Lee, H.-K. (2005). Geometric attack resistant watermarking in wavelet transform domain. *Optics Express*, 13, 1307–1321. doi:10.1364/OPEX.13.001307
- Lee, H.-Y., Kim, H. & Lee, H.-K. (2006). Robust image watermarking using local invariant features. *Optical Engineering*, 45(3), 037002(1-11).
- Lee, I., & Tsai, W. (2009). Data hiding in grayscale images by dynamic programming based on a human visual model. *Pattern Recognition*, 42(7), 1604–1611. doi:10.1016/j.patcog.2009.01.014
- Lee, J., & Won, C. S. (2000). A watermarking sequence using parities of error control coding for image authentication and correction. *IEEE Transactions on Consumer Electronics*, 46(2), 313–317. doi:10.1109/30.846663
- Lee, S. K., & Ho, Y. S. (2000). Digital audio watermarking in the cepstrum domain. *IEEE Transactions on Consumer Electronics*, 46(3), 744–750. doi:10.1109/30.883441
- Lee, S., Jang, D., & Yoo, C. D. (2005). An SVD-Based Watermarking Method for Image Content Authentication with Improved Security. In. *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2, 525–528.
- Lee, S.-H., & Kwon, K.-R. (2007). A watermarking for 3D mesh using the patch CEGIs. *Digital Signal Processing*, 17(2), 396–413. doi:10.1016/j.dsp.2005.04.014
- Lee, Y. K., & Chen, L. H. (2000). High capacity image steganographic model. *IEEE Proceedings on Vision. Image and Signal Processing*, 147(3), 288–294. doi:10.1049/ip-vis:20000341
- Lefebvre, F., Gueluy, D., Delannay, D., & Macq, B. (2001). *A Print and Scan Optimized Watermarking Scheme* (pp. 511–516). Cannes, France: MMSP.
- Lei, C. L., Yu, P. L., Tsai, P. L., & Chan, M. H. (2004). An efficient and anonymous buyer-seller watermarking protocol. *IEEE Transactions on Image Processing*, 13(12), 1618–1626. doi:10.1109/TIP.2004.837553
- Lewicki, M., & Sejnowski, T. J. (2000). Learning overcomplete representations. *Neural Computation*, 12, 337–365. doi:10.1162/089976600300015826
- Li, B. C. (1990). *Applications of moment invariants to neurocomputing for pattern recognition*. PhD dissertation, The Pennsylvania State University, Pennsylvania.

- Li, F. Y., Stol, N., Pham, T. T., & Andresen, S. (2001). A priority-oriented QoS management framework for multimedia services in UMTS. In *Proceedings of the fourth international IEEE symposium wireless personal multimedia communications*.
- Li, H., Wang, S., Song, W., & Wen, Q. (2005). A Novel Watermarking Scheme Based on Independent Component Analysis. In Wang, L. (Eds.), *Advances in Natural Computation* (Vol. 5326, pp. 448–453). Berlin: Springer-Verlag.
- Li, J., Su, B., Li, S., Wang, S., & Yao, D. (2008). A Semi-fragile Watermark Scheme Based on the Logistic Chaos Sequence and Singular Value Decomposition. In Fyfe, C. (Eds.), *Intelligent Data Engineering and Automated Learning* (Vol. 5326, pp. 57–64). Berlin: Springer-Verlag. doi:10.1007/978-3-540-88906-9_8
- Li, Q., & Dong, Z. (2008). Novel Text Watermarking Algorithm Based on Chinese Characters Structure. *IEEE Symposium on Computer Science and Computational Technology*, 2, 348-351.
- Li, Q., Yuan, C., & Zhong, Y. Z. (2007). Adaptive DWT-SVD domain image watermarking using human visual model. In *Proceedings of the 9th International Conference on Advanced Communication Technology: Vol. 3* (pp. 1947-1951).
- Li, X., & Xue, X. (2004). Improved robust watermarking in DCT domain for color images. In *Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on* (Vol. 1, pp. 53-58).
- Li, X., & Yu, H. (2000). Transparent and robust audio data hiding in sub-band domain. In *Proceedings of the International Conference on Information Technology: Coding and Computing*. (pp. 74–79).
- Li, X., Tao, D., Gao, X., & Lu, W. (2009). A natural image quality evaluation metric. *Signal Processing*, 89(4), 548–555. doi:10.1016/j.sigpro.2008.10.007
- Liao, S. X., & Pawlak, M. (1996). On image analysis by moments. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18, 254–266. doi:10.1109/34.485554
- Lie, W., & Chang, L. (2006). Robust and high-quality time-domain audio watermarking based on low-frequency amplitude modification. *IEEE Transactions on Multimedia*, 8(1), 46–59. doi:10.1109/TMM.2005.861292
- Lim, H., Park, S.-Y., Kang, S.-J., & Cho, W.-H. (2003). FPGA Implementation of Image Watermarking Algorithm for a Digital Camera. *IEEE Pacific Rim Conference on Communications, Computers and signal Processing*, 2, (pp. 1000 - 1003).
- Lin, C. Y., Wu, M., Bloom, J. A., Cox, I. J., Miller, M., & Lui, Y. M. (2001). Rotation, scale, and translation resilient public watermarking for images. *IEEE Transactions on Image Processing*, 10(5), 767–782. doi:10.1109/83.918569
- Lin, C. Y., Wu, M., Lui, Y. M., Bloom, J. A., Miller, M. L., & Cox, I. J. (1999). Rotation, Scale and Translation Resilient Public Watermarking for Images. *IEEE Transactions on Image Processing*, 10(5), 767–782. doi:10.1109/83.918569
- Lin, C., Chan, D., Su, H., & Hsieh, W. (2006). Histogram-oriented watermarking algorithm: colour image watermarking scheme robust against geometric attacks and signal processing. *Vision. Image and Signal Processing*, 153(4), 483–492. doi:10.1049/ip-vis:20050107
- Lin, C.-H., Liu, J.-C., & Han, P.-C. (2008). On the Security of the Full-Band Image Watermark for Copyright Protection. In *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing* (pp. 74-80).
- Lin, C.-Y., & Chang, S.-F. (2000). Semi-fragile watermarking for authenticating JPEG visual content. *SPIE Security and Watermarking of Multimedia Contents II*, 3971, 140–151.
- Lin, H. S., Liao, H. M., Lu, C., & Lin, J. (2005). Fragile watermarking for authenticating 3-D polygonal meshes. *IEEE Transactions on Multimedia*, 7(6), 997–1006. doi:10.1109/TMM.2005.858412

Compilation of References

- Lin, Y., & Abdulla, W. H. (2008). Perceptual Evaluation of Audio Watermarking Using Objective Quality Measures. In *Proceedings of the IEEE International Conference on Acoustic, Speech, and Signal Processing*, Las Vegas, NV, (pp. 1745 - 1748).
- Ling, H.-C., Phan, R. C.-W., & Heng, S.-H. (2008). Attacks on SVD-Based Watermarking Schemes. In Yang, C. C. (Eds.), *Intelligence and Security Informatics* (Vol. 5075, pp. 83–91). Berlin: Springer-Verlag. doi:10.1007/978-3-540-69304-8_10
- Liu, F., & Liu, Y. (2008). A Watermarking Algorithm for Digital Image Based on DCT and SVD. In *Proceedings of the 2008 Congress on Image and Signal Processing: Vol. 1* (pp. 380-383).
- Liu, J., Niu, X., & Kong, W. (2006). Image watermarking scheme based on singular value decomposition. In *Proceedings of the IEEE International Conference on Intelligent Information Hiding and Multimedia* (pp. 457-460).
- Liu, J.-C., Lin, C.-H., Kuo, L.-C., & Chang, J.-C. (2007). Robust Multi-scale Full-Band Image Watermarking for Copyright Protection. In Okuno, H. G., & Ali, M. (Eds.), *New Trends in Applied Artificial Intelligence* (Vol. 4570, pp. 176–184). doi:10.1007/978-3-540-73325-6_18
- Liu, R., & Tan, T. (2002). A SVD-Based Watermarking Scheme for Protecting Rightful Ownership. *IEEE Transactions on Multimedia*, 4(1), 121–128. doi:10.1109/6046.985560
- Liu, R., Zhang, H., Shamir, A., & Cohen-Or, D. (2009). A part-aware surface metric for shape analysis. *Computer Graphics Forum*, 28(2), 397–406. doi:10.1111/j.1467-8659.2009.01379.x
- Liu, T., & Zheng-ding Qiu. (2002). A DWT-based color image steganography scheme. In *Signal Processing, 2002 6th International Conference on* (Vol. 2, pp. 1568-1571).
- Liu, Y., Prabhakaran, B., & Guo, X. (2008). A robust spectral approach for blind watermarking of manifold surfaces. In *Proc. of the ACM Workshop on Multimedia and Security*, (pp. 43-52).
- Liu, Y.-W., & Smith, J. O. (2004). Multiple Watermarking: is power sharing better than time sharing? In *IEEE Int. Conf. on Multimedia and Expo, ICME*, (pp. 1939-1942).
- Loo, P., & Kingsbury, N. (2003). Watermark detection based on the properties of error control codes. *IEE Proceedings. Vision Image and Signal Processing*, 150(2), 115–121. doi:10.1049/ip-vis:20030167
- Lounsbury, M., DeRose, T. D., & Warren, J. (1997). Multiresolution analysis for surfaces of arbitrary topological type. *ACM Transactions on Graphics*, 16(1), 34–73. doi:10.1145/237748.237750
- Louvre. (2009). Retrieved from <http://www.bestofmicro.com/actualite/24309-louvre-guide-multimedia.html>
- Lo-Varco, G., Puech, W., & Dumas, W. (2005). Content Based Watermarking for Securing Color Images. *The Journal of imaging science and technology*, 49(5), 464-473.
- Low, S. H., Maxemchuk, N. F., & Lapone, A. M. (1995). Document Identification to Discourage Illicit Copying, *IEEE Global Telecommunications Conference, GLOBECOM '95*, 2, 1203-1208.
- Lowe, D. G. (1999). Object recognition from local scale-invariant features. In *Proceedings, the IEEE International Conference on Computer Vision*, (Vol. 2, pp. 1150–1157). Kerkyra, Greece: IEEE Computer Society Press.
- Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, 60(2), 91–110. doi:10.1023/B:VISI.0000029664.99615.94
- Lu, C. S., Huang, S. K., Sze, C. J., & Liao, H. Y. M. (2000). Cocktail Watermarking for Digital Image Protection. *IEEE Trans. On Multimedia*, 2(4), 209–224. doi:10.1109/6046.890056
- Lu, T.-C., Chang, C.-C., & Liu, X.-Y. (2006). A content-based image authentication scheme based on singular value decomposition. *Pattern Recognition and Image Analysis*, 16(3), 506–522. doi:10.1134/S1054661806030187
- Lukac, R., & Plataniotis, K. (2007). *Color Image Processing* (p. 580). Boca Raton, FL: CRC Press.

- Lukac, R., & Plataniotis, K. N. (2006). Secure single-sensor digital camera. *IEE Electronics Letters*, 42(11), 627–629. doi:10.1049/el:20060604
- Luo, L. M., Hamitouche, C., Dilenseger, J. L., & Coatrieux, J. L. (1993). A moment-based three-dimensional edge operator. *IEEE Transactions on Bio-Medical Engineering*, 40, 693–703. doi:10.1109/10.237699
- Luo, L. M., Xie, X. H., & Bao, X. D. (1994). A modified moment-based edge operator for rectangular pixel image. *IEEE Transactions on Circuits and Systems for Video Technology*, 4, 552–554. doi:10.1109/76.340199
- Luo, M., & Bors, A. G. (2008). Principal component analysis of spectral coefficients for mesh watermarking. In *Proc. of the IEEE International Conference on Image Processing* (pp. 441-444).
- Luo, M., Wang, K., Bors, A. G., & Lavoué, G. (2009). Local patch blind spectral watermarking method for 3D graphics. In *Proc. of the International Workshop on Digital Watermarking*. (pp. 211-226).
- Lyu, S., & Farid, H. (2004). Steganalysis using color wavelet statistics and one-class support vector machines. In *Security, stenography, and watermarking of multimedia contents* (Vol. 5306, pp. 35–45). SPIE.
- Macadam, D. (1942). Visual Sensitivities to Color Differences in Daylight. *Journal of the Optical Society of America*, 32(5), 247–273. doi:10.1364/JOSA.32.000247
- Macq, B., Dittmann, J., & Delp, E. (2004). Benchmarking of image watermarking algorithms for digital rights management. *Proceedings of the IEEE*, 92(6), 971–984. doi:10.1109/JPROC.2004.827361
- Maes, M., Kalker, T., Linnartz, J.-P., Talstra, J., Depover, G., & Haitsma, J. (2000, September). Digital watermarking for DVD video copy protection. *IEEE Signal Processing Magazine*, 47–57. doi:10.1109/79.879338
- Maillet, C., Martínez-Ballesté, A., Sebé, F., & Ferrer, J. D. (2003). *Prototipos del proyecto STREAMOBILE. (STREAMOBILE TIC-2001-0633-C03)*, University Rovira i Virgili, Spain. Retrieved May, 15, 2009, from <http://crises-deim.urv.cat/projects/spanish/streamobile/demo1/report.streamobile.pdf>
- Maity, S. P. & Kundu, M. K. (2009). Genetic algorithms for optimality of data hiding in digital images. *Bio-inspired information hiding: A fusion of foundations, methodologies and applications*, 13(4), 361-373.
- Maity, S. P. & Kundu, M. K. (2009). Distortion free image-in-image communication with implementation in FPGA. *International Journal of Electronics and Communication*.
- Maity, S. P. & Kundu, M. K. (2009). DHT domain digital watermarking with low loss in image information. *International Journal of Electronics and Communication Engg.*, 1-15.
- Maity, S. P. (2008). *Studies on data hiding in digital media for secured communication, authentication and content integrity*. Unpublished doctoral dissertation, Bengal Engineering and Science University, Shibpur, India.
- Maity, S. P., & Kundu, M. K. (2009). DHT domain digital watermarking with low loss in image informations. *AEU - International Journal of Electronics and Communications*.
- Maity, S. P., & Maity, S. (2008). Wavelet based Hilbert transform with digital design and application to QCM-SS watermarking. *Radioengineering. Proceedings of Czech and Slovak Technical Universities*, 17(1), 64–72.
- Maity, S. P., & Maity, S. (2009). Multistage spread spectrum watermark detection technique using fuzzy logic. *IEEE Signal Processing Letters*, 16(4), 245–248. doi:10.1109/LSP.2009.2014097
- Maity, S. P., Banerjee, A., & Kundu, M. K. (2004). An image-in-image communication scheme and VLSI implementation using FPGA. In *Proceedings of IEEE Indian annual conference (INDICON 2004)*, (pp. 6–11).

Compilation of References

- Maity, S. P., Banerjee, A., Abhijit, A., & Kundu, M. K. (2007). VLSI design of spread spectrum watermarking. In *Proceedings of 13th National conference on communication*, IIT Kanpur, India, (pp. 251–257).
- Maity, S. P., Kundu, M. K., & Das, T. S. (2007). Robust SS Watermarking with improved capacity. *Pattern Recognition Letters*, 28, 350–357. doi:10.1016/j.patrec.2006.04.004
- Maity, S. P., Kundu, M. K., & Maity, S. (2006). Capacity improvement in digital watermarking using QCM scheme. In *Proceedings of 12th National Conference on Communications (NCC 2006)*, IIT Delhi, India, (pp. 511-515).
- Maity, S. P., Kundu, M. K., & Maity, S. (2009). Dual purpose FWT domain spread spectrum. Image watermarking in real-time. *Computers & Electrical Engineering*, 35(2), 415–433. doi:10.1016/j.compeleceng.2008.06.003
- Maity, S. P., Kundu, M. K., & Mandal, M. K. (2006). Performance improvement in spread spectrum watermarking via M-band Wavelets and N-ary modulation. In *Proceedings of 3rd IET International Conference on Visual Information Engineering*, (pp. 35-40).
- Maity, S. P., Maity, S., & Sil, J. (2009). Diversity Assisted GCIC for Spread Spectrum Watermark Detection using Genetic Algorithms. *IEEE Conference on Image Processing*, (pp.3649-3652). Washington, DC: IEEE CS Press.
- Maity, S. P., Maity, S., & Sil, J. (2009). Estimation of fading attack on high payload spread spectrum watermarking with variable embedding rate using genetic algorithms. *Third International Conference on Imaging for Crime Detection and Prevention (ICDP-09)*, (Accepted).
- Maity, S. P., Nandi, P. K., Kundu, M. K., & Banerjee, A. (2005). Low cost data authentication scheme and hardware realization. In *Proceedings of 11th National Conference on Communication (NCC-2005)*, (pp. 574-577).
- Maity, S., Maity, S. P., & Sil, J. (2009). Spread spectrum watermark embedder optimization using Genetic Algorithms. In 7th International Conferences on Advances in Pattern Recognition, (pp.29-32). Washington, DC: IEEE CS Press.
- Malik, H., Ansari, R., & Khokhar, A. (2008). Robust audio watermarking using frequency-selective spread spectrum. *IET Information Security*, 2(4), 129–150. doi:10.1049/iet-ifis:20070145
- Mallat, S. (1989). A theory for multi-resolution signal decomposition: The wavelet Representation. *IEEE Trans. on Pat. Anal. Mach. Inte.*, 11(7), 674-693.
- Malver, H., & Florencio, A. F. (2003). Improved spread spectrum: A new modulation technique for robust watermarking. *IEEE Transactions on Signal Processing*, 51(4), 898–905. doi:10.1109/TSP.2003.809385
- Mansouri, A., Aznaveh, A. M., & Azar, F. T. (2008). Secure Digital Image Watermarking Based on SVD-DCT. In Sarbazi-Azad, H. (Eds.), *Advances in Computer Science and Engineering* (Vol. 6, pp. 645–652). Berlin: Springer-Verlag. doi:10.1007/978-3-540-89985-3_79
- Marcellin, M. W., & Fisher, T. R. (1990). Trellis coded quantization of memoryless and Gauss-Markov sources. *IEEE Transactions on Communications*, 38, 83–93. doi:10.1109/26.46532
- Margulis, D. (2006). *Photoshop Lab Color: The Canyon Conundrum and Other Adventures in the Most Powerful Colorspace*. Berkeley, CA: Pearson Education.
- Martin, J. R. H., & Kutter, M. (2001, August). Information Retrieval in Digital Watermarking. *IEEE Communications Magazine*, 39(8), 110–116. doi:10.1109/35.940051
- Martínez-Ballesté, A., Sebé, F., & Ferrer, J. D. (2003). Aspectos prácticos de la protección de la propiedad intelectual en contenidos multimedia. *II Simposio Español de Comercio Electrónico (SCE'03)*, (Vol. II, pp. 219-228), Universitat Politècnica de Catalunya, Spain.
- Marvel, L. M., Charles, G., Boncelet, J., & Retter, C. T. (1999). Spread spectrum image steganography. *IEEE Transactions on Image Processing*, 8(8), 1075–1083. doi:10.1109/83.777088
- Matam, B. R., & Lowe, D. (2006). Steganography, BioPatterns and Independent Components. In *Proc. 7th Int. Conf. Mathematics in Signal Processing*, (pp. 206-209).

- Matam, B. R., & Lowe, D. (2009). Exploiting sensitivity of nonorthogonal joint diagonalisation as a security mechanism in steganography. In *Proceedings of 16th International Conference on Digital Signal Processing*.
- Mathai, N. J., Kundur, D., & Sheikholesla, A. (2003, April). Hardware implementation perspectives of digital video watermarking algorithms. *IEEE Transactions on Signal Processing*, 51(4), 925–938. doi:10.1109/TSP.2003.809382
- Mathai, N. J., Sheikholeslami, A., & Kundur, D. (2003). VLSI Implementation of a Real-Time Video Watermark Embedder and Detector. In *Proceedings of the 2003 International Symposium on Circuits and Systems*, 2, (pp. II-772- II-775).
- Matz, G., & Duhamel, P. (2004). Information geometric formulation and interpretation of accelerated Blahut-Arimoto-type algorithms. In *Proc. 2004 IEEE Information Theory Workshop*, San Antonio, TX (pp. 66-70).
- Mayer, J., Silverio, A. V., & Bermudez, J. C. M. (2002). On the design of pattern sequences for spread spectrum image watermarking. In *International Telecommunications Symposium- ITS2002*, Natal, Brazil.
- Meerwald, P., & Uhl, A. (2001). A survey of wavelet domain watermarking. In *Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III*, (vol. 4314).
- Meerwald, P., & Uhl, A. (2008). Watermarking of Raw Digital Images in Camera Firmware: Embedding and Detection. In *Proceedings of the 3rd Pacific Rim Symposium on Advances in Image and Video Technology* (pp. 340-348). Tokyo, Japan: Springer-Verlag.
- Mehul, R., & Priti, R. (2003). Discrete Wavelet Transform Based Multiple Watermarking Scheme. In *Proc. IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific*, Bangalore, India.
- Mei, Q., Wong, E. K., & Memon, N. (2001). *Data Hiding in Binary Text Documents*. Retrieved on 19th Feb 2009 from http://mike.sfs.poly.edu/memon/publications/pdf/2001_Data_Hiding_in_Binary_Text_Documents.pdf
- Memon, N., & Wong, P. W. (1998). Protecting digital media content. *Communications of the ACM*, 41(7), 35–43. doi:10.1145/278476.278485
- Memon, N., & Wong, P. W. (2001). A buyer-seller watermarking protocol. *IEEE Transactions on Image Processing*, 10(4), 643–649. doi:10.1109/83.913598
- Meng, X., Cai, L., Yang, X., Xu, X., Dong, G., & Shen, X. (2007). Digital color image watermarking based on phase-shifting interferometry and neighboring pixel value subtraction algorithm in the discrete-cosine-transform domain. *Applied Optics*, 46(21), 4694–4701. doi:10.1364/AO.46.004694
- Micic, A., Radenkovic, D., & Nikolic, S. (2005, September). Autentification of Text Documents Using Digital Watermarking. In *Proc of 7th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services*, 2, 503-505.
- Miller, M. L., Doerr, G. J., & Cox, I. J. (2002). Dirty-paper trellis codes for watermarking. In *Proc. of IEEE Int. Conf. on Image Processing*, Rochester, New York, (vol. 2, pp. 129–132).
- Miller, M. L., Doerr, G. J., & Cox, I. J. (2004). Applying informed coding and embedding to design a robust high capacity watermark. *IEEE Transactions on Image Processing*, 13, 792–807. doi:10.1109/TIP.2003.821551
- Miller, M., Doerr, G., & Cox, I. (2004). Applying informed coding and embedding to design a robust high-capacity watermark. *IEEE Transactions on Image Processing*, 13(6), 792–807. doi:10.1109/TIP.2003.821551
- Mintzer, F. C., Boyle, L. E., Cazes, A. N., Christian, B. S., Cox, S. C., & Giordano, F. P. (1996). Towards online Worldwide Access to Vatican Library Materials. *IBM Journal of Research and Development*, 40(2), 139–162. doi:10.1147/rd.402.0139
- Mintzer, F., & Braudaway, G. W. (1999). If one watermark is good, are more better? In *IEEE Int. Conf. on Acoustics, Speech and Signal Processing, ICASSP*, (pp. 2067-2069).

Compilation of References

- Mintzer, F., Braudaway, G. W., & Bell, A. E. (1998). Opportunities for watermarking standards. *Communications of the ACM*, 41(7), 57–64. doi:10.1145/278476.278487
- Mintzer, F., Braudaway, G., & Yeung, M. (1997). Effective and ineffective digital watermarks. In *Proceedings of the IEEE International Conference on Image Processing*, 3, 9–12.
- Mishra, R. & Raghuvansh, S. (2009, March). Binary Image Mapping for Digital Rights Management. *CSI Communications*, 17-20.
- Mishra, R. (2007, November/December). *Sectional Fingerprinting for Binary Images*. Talk at 42nd Annual Convention of Computer Society of India, “Generation Next”, Bangalore, India.
- Mitra, S. (1998). *Digital Signal Processing*. Columbus, OH: McGraw –Hill.
- Mitrea, M., & Prêteux, F. (2009). From watermarking to in-band enrichment: future trends. invited paper to SPIE Electronic Imaging. In *Proc. SPIE*, (Vol. 7248, pp. 7248OI:1-10).
- Mitrea, M., Dumitru, O., Duta, S., Prêteux, F., & Vlad, A. (2008). A comprataive study on video watermarking capacity. In *Proc. of the IEEE 7th Intl. Conf. Communications 2008*, Bucharest, Romania (pp. 335-339).
- Mitrea, M., Dumitru, O., Prêteux, F., & Vlad, A. (2007). Zero-memory information sources approximating to video watermarking attacks. *Lecture Notes in Computer Science* 4707, (Vol. 3, pp. 445-459).
- Mitrea, M., Duta, S., Preda, M., & Prêteux, F. (2006). In-band enriched video for interactive applications. *WSEAS Trans. on Communications*, 5(8), 1528–1534.
- Mitrea, M., Duta, S., Prêteux, F., & Vlad, A. (2006). Data payload optimality: A Key Issue for Video Watermarking Applications. In *Proc. SPIE*, (Vol. 6315, pp. 630509:1-11).
- Mitrea, M., Duta, S., Zaharia, T., & Prêteux, F. (2006). Ensuring multimedia content adaptability by means of data hiding techniques. In *Proc. SPIE*, (Vol. 6383, pp. 63830:1-8).
- Mitrea, M., Prêteux, F., Vlad, A., & Fetita, C. (2004). The 2D-DCT coefficient statistical behaviour: a comparative analysis on different types of image sequences. *JOAM*, 6(1), 95–102.
- Mitrea, M., Zaharia, T., Prêteux, F., & Vlad, A. (2004). Accurate Data Modelling for Watermarking Applications. In *Proc. of the IEE-IMA Intl. Conf. Mathematics in Signal Processing VI*, Cirencester – UK (pp. 167-170).
- Mobasseri, B. (1998). Direct sequence watermarking of digital video using mframes. In *Proceedings of the International Conference on Image Processing*, (pp. 399–403).
- Mohamed, F. K., & Abbes, R. (2007). RST robust watermarking schema based on image normalization and DCT decomposition. *Malaysian Journal of Computer Science*, 20(1), 77–90.
- Mohammad, A., Al-Haj, A., & Shaltaf, S. (2008). An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Processing Journal*, 88(9), 2158–2180. doi:10.1016/j.sigpro.2008.02.015
- Mohan, B. C., & Kumar, S. A. (2008). A Robust Digital Image Watermarking Scheme using Singular Value Decomposition. *Journal of Multimedia*, 3(1), 7–15. doi:10.4304/jmm.3.1.7-15
- Mohan, B. C., Srinivaskumar, S., & Chatterji, B. N. (2008). A Robust Digital Image Watermarking Scheme using Singular Value Decomposition (SVD), Dither Quantization and Edge Detection. *International Journal on Graphics. Vision and Image Processing*, 8(1), 17–23.
- Mohanty, P., Guturu, P., Kougnos, E., & Pati, N. (2006). A Novel Invisible Color Image Watermarking Scheme Using Image Adaptive Watermark Creation and Robust Insertion-Extraction. In *Multimedia, 2006. ISM'06. Eighth IEEE International Symposium on* (pp. 153-160).
- Mohanty, S. P. (1999). *Digital Watermarking: A Tutorial Review*. Bangalore, India: Department of Electrical Engineering, Indian Institute of Science.

- Mohanty, S. P., & Bhargava, B. K. (2008). Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks. *ACM Trans. Multimedia Comput. Commun. Appl.*, 5(2), 12. doi:10.1145/1413862.1413865
- Mohanty, S. P., & Bhargava, B. K. (2008). Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks. *CM Transactions on Multimedia Computing, Communications, and Applications*, 5(2), 12:1-12:22.
- Mohanty, S. P., Adamo, O. B., & Kougianos, E. (2007). VLSI Architecture of an Invisible Watermarking Unit for a Biometric-Based Security System in a Digital Camera. In *The 25th IEEE International Conference on Consumer Electronics*, (pp. 485-486).
- Mohanty, S. P., Guturu, P., Kougianos, E., & Pati, N. (2006). A novel invisible color image watermarking scheme using image adaptive watermark creation and robust insertion-extraction. In *Proceedings of the 8th IEEE International Symposium on Multimedia (ISM)*, (pp. 153–160).
- Mohanty, S. P., Kougianos, E., Cai, W., & Ratnani, M. (2009). VLSI Architectures of Perceptual Based Video Watermarking for Real-Time Copyright Protection. In *The 10th IEEE International Symposium on Quality Electronic Design*, (pp. 527-534).
- Mohanty, S. P., Kumara, R. C., & Nayak, S. (2004). FPGA Based Implementation of an Invisible-Robust ImageWatermarking Encoder. *LNCS*, 344-353.
- Mohanty, S. P., Ramakrishnan, K. R., & Kankanhalli, M. S. (2000). A DCT Domain Visible Watermarking Technique for Images. In *Proceedings of the IEEE International Conference on Multimedia*, (pp. 1029 – 1032).
- Mohanty, S. P., Ranganathan, N., & Balakrishnan, K. (2005). Design of a Low Power Image Watermarking Encoder using Dual Voltage and Frequency. In *Proceedings of 18th IEEE International Conference on VLSI Design*, (pp.153–158).
- Mohanty, S. P., Ranganathan, N., & Balakrishnan, K. (2006). A dual voltage-frequency VLSI chip for image watermarking in DCT domain. *IEEE Transactions on Circuits and Systems II*, 53(5), 394–398. doi:10.1109/TCSII.2006.870216
- Mohanty, S. P., Ranganathan, N., & Namballa, R. K. (2003). VLSI implementation of invisible digital watermarking algorithms towards the development of a secure JPEG encoder. In *Proceedings of the IEEE workshop on signal processing systems*, (pp. 183–188).
- Mohanty, S. P., Ranganathan, N., & Namballa, R. K. (2005). A VLSI architecture for visible watermarking in a secure still digital camera (S2DC) design. *IEEE Transactions on Very Large Scale Integration Systems*, 13(8), 1002–1012. doi:10.1109/TVLSI.2005.857991
- Mohanty, S., Kougianos, E., & Ranganathan, N. (2007). VLSI architecture and chip for combined invisible robust and fragile watermarking. *IET Computers & Digital Techniques*, 1(5), 600–611. doi:10.1049/iet-cdt:20070057
- Mohanty, S., Pati, N., & Kougianos, E. (2007). A Watermarking Co-Processor for New Generation Graphics Processing Units. *International Conference on Consumer Electronics*, (pp. 1 - 2).
- Morris, H., & Muhi El-Ddin, I. (2007). Feature frame watermarking. In *Proceedings of the 41 st Annual Asilomar Conference on Signals, Systems, and Computers*, (pp. 565-569).
- Morris, H., & Muhi El-dDin, I. (2008). A new image transform. In *Proceedings of IPV08*.
- Moulin, P., & Ivanovic, A. (2003). The zero-rate spread spectrum watermarking game. *IEEE Signal Processing*, 51(4), 1098–1117. doi:10.1109/TSP.2003.809370
- Moulin, P., & O’Sullivan, J. A. (2003). Information-theoretic analysis of information hiding. *IEEE Transactions on Information Theory*, 49, 563–593. doi:10.1109/TIT.2002.808134

Compilation of References

- Muhi El-Ddin, I., Morris, H., & Eyadat, M. (2008). Watermarking: A new approach. In *Proceedings of the Fifth International Conference on Information Technology: New Generations*, (pp. 795–800).
- Mukherjee, D. P., Maitra, S., & Acton, S. T. (2004). Spatial domain digital watermarking of multimedia objects for buyer authentication. *IEEE Transactions on Multimedia*, 6(1), 1–15. doi:10.1109/TMM.2003.819759
- Mukundan, R. (2004). Some computational aspects of discrete orthonormal moments. *IEEE Transactions on Image Processing*, 13, 1055–1059. doi:10.1109/TIP.2004.828430
- Mukundan, R., & Ramakrishnan, K. R. (1998). *Moment functions in image analysis - Theory and applications*. Singapore: World Scientific.
- Mukundan, R., Ong, S. H., & Lee, P. A. (2001). Image analysis by Tschebycheff moments. *IEEE Transactions on Image Processing*, 10, 1357–1364. doi:10.1109/83.941859
- Murillo-Fuentes, J. J. (2007). Independent component analysis in the blind watermarking of digital images. *Neurocomputing*, 70(16–18), 2881–2890. doi:10.1016/j.neucom.2006.06.011
- Nahrstedt, K., & Qiao, L. (1998). *Non-Invertible Watermarking Methods for MPEG Video and Audio*. Paper presented at the ACM Multimedia Security Workshop, England.
- Navasd, K. A., & Sasikumar, M. (2007). Survey of Medical Image Watermarking Algorithms. In *The 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications*, Tunisia.
- Nelson, G. R., Jullien, G. A., & Pecht, O. Y. (2005). CMOS image sensor with watermarking capabilities. In *Proceedings of the IEEE International Conference on Circuits and Systems (ISCAS)*, (pp. 5326–5329).
- Neubauer, C., & Herre, J. (2000). Audio watermarking of MPEG-2 AAC bit streams. In *Proceedings of the Audio Engineering Society Convention*.
- Neubauer, C., Herre, J., & Brandenburg, K. (1998). Continuous steganographic data transmission using uncompressed audio. In *Proceedings of the Information Hiding Workshop*, (pp. 208–217).
- Niu, X., Lu, Z., & Sun, S. (2000). Digital Image Watermarking Based on Multi-resolution Decomposition. *IEEE Electronics Letters*, 36(13), 1108–1110. doi:10.1049/el:20000819
- Noll, P. (1993). Wideband speech and audio coding. *IEEE Communications Magazine*, 31(11), 34–44. doi:10.1109/35.256878
- Nozaki, K., Niimi, M., Eason, R. O., & Kawaguchi, E. (1998). A large capacity steganography using colour bmp images. In *ACCV '98: Proceedings of the Third Asian Conference on Computer Vision*, (Vol. I, pp.112–119). London: Springer-Verlag.
- O’Ruanaidh, J., Dowling, W., & Boland, F. (1996, September 16–19). Phase watermarking of digital images. In *Proc. IEEE International Conference on Image Processing (ICIP)*, Lausanne, Switzerland, (Vol. 3, pp. 239–242).
- Oh, H. O., Seok, J. W., Hong, J. W., & Youn, D. H. (2001). New echo embedding technique for robust and imperceptible audio watermarking. In *Proceedings of the IEEE International Conference on Acoustic, Speech and Signal Processing*, (pp. 1341–1344).
- Oh, I.-S., & Kim, Y.-W. (2004, May). Watermarking text Document images using edge direction histograms. *Pattern Recognition Letters*, 25, 1243–1251. doi:10.1016/j.patrec.2004.04.002
- Ohbuchi, R., & Mukaiyama, A. (2004). Watermarking a 3D Shape Model Defined as a Point Set. In *Proceeding of CW* (pp. 392–399). Takahashi.
- Ohbuchi, R., Masuda, H., & Aono, M. (1997). Watermarking three-dimensional polygonal models. In *Proc. of the ACM Multimedia* (pp. 261–272).
- Ohbuchi, R., Mukaiyama, A., & Takahashi, S. (2002). A frequency-domain approach to watermarking 3D shapes. *Computer Graphics Forum*, 21(3), 373–382. doi:10.1111/1467-8659.t01-1-00597

- Okttavia, V., & Lee, W.-H. (2004). A Fragile Watermarking Technique for Image Authentication Using Singular Value Decomposition. In Aizawa, K. (Eds.), *Advances in Multimedia Information Processing* (Vol. 3332, pp. 42–49). Berlin: Springer-Verlag.
- Oppenheim, A., & Lim, J. (1981). The importance of phase in signals. *Proceedings of the IEEE*, 69(5), 529–541. doi:10.1109/PROC.1981.12022
- Oppenheim, A., Lim, J., & Curtis, S. (1983). Signal synthesis and reconstruction from partial Fourier-domain information. *Journal of the Optical Society of America*, 73(11), 1413–1420. doi:10.1364/JOSA.73.001413
- Ozer, H., Sankur, B., & Memon, N. (2005). An SVD-based audio watermarking technique. In *Proceedings of the Multimedia and Security Workshop*, (pp. 51-56).
- Painter, T., & Spanias, A. (2000). Perceptual Coding of Digital Audio. *Proceedings of the IEEE*, 88(4). doi:10.1109/5.842996
- Pal, S. K., & Mitra, S. (1999). *Neuro-fuzzy pattern recognition methods in soft computing*. New York: John Wiley.
- Pal, S. K., & Wang, P. P. (1996). *Genetic algorithms for pattern recognition*. Boca Raton, FL: CRC Press.
- Pal, S. K., Ghosh, A., & Kundu, M. K. (Eds.). (2000). *Soft Computing for Image Processing*. Heidelberg, Germany: Physica Verlag.
- Pan, H.-K., & Tseng, Y.-C. (2001). Secure and Invisible Data Hiding in 2-Color Images. *Proceedings - IEEE INFOCOM*, 2, 887–895.
- Pan, J. S., & Abraham, A. (Eds.). (2009). Bio-inspired information hiding: A fusion of foundations, methodologies and applications. Springer, 13(4).
- Pan, J. S., Huang, H. C., & Jain, L. C. (Eds.). (2004). *Intelligent Watermarking Techniques*. Singapore: World Scientific.
- Pan, J. S., Huang, H. C., & Wang, F. H. (2001). Genetic watermarking techniques. In *Proceedings of the fifth International Conference on Information Engineering Systems & Allied Technologies*, (pp. 1032-1036).
- Panda, M. (2009). *On Optimization of M-band wavelets and N-ary modulation for high payload spread spectrum watermarking using Genetic Algorithms*. Unpublished master's thesis, Bengal Engineering and Science University, Shibpur, India.
- Papademetriou, R. C. (1992, August/September). Reconstructing with moments. In *Proceedings of 11th International Conference on Pattern Recognition* (Vol. 3. Image, Speech and Signal Analysis, pp 476-480). Los Alamitos, CA: IEEE Computer Society Press.
- Papoulis, A. (1992). *Probability, random variables, and stochastic processes*. New York: McGraw-Hill.
- Patra, J. C., Soh, W., Ang, E. L., & Meher, P. K. (2006). An Improved SVD-Based Watermarking Technique for Image and Document Authentication. In *Proceedings of the IEEE Conference on Circuits and Systems* (pp. 1984-1987).
- Paul, R. (2008). Amount of digital info – Global storage capacity. *Ars Technica*. Retrieved June 1, 2009 from <http://arstechnica.com/old/content/2008/03/study-amount-of-digital-info-global-storage-capacity.ars>
- Pawlak, M. (1992). On the reconstruction aspects of moment descriptors. *IEEE Transactions on Information Theory*, 38(6), 1698–1708. doi:10.1109/18.165444
- Pay. (2009). Retrieved from <http://www.paypernews.nl/home/products/digi-magazine>
- Pei, S., & Chen, J. (2006). Color Image Watermarking by Fibonacci Lattice Index Modulation. In *Colour in Graphics* (pp. 211–215). Imaging, and Vision.
- Pei, S., & Cheng, C. (2000). *Palette-based color image watermarking using neural network training and repeated LSB insertion*. In *13th*(Vol. 1, pp. 1–8). IPPR Conf. on Computer Vision, Graphics and Image Processing.
- Peng, Z., & Liu, W. (2006). Color image authentication based on spatiotemporal chaos and SVD. *Chaos, Solitons, and Fractals*, 36(4), 946–952. doi:10.1016/j.chaos.2006.07.015

Compilation of References

- Pereira, S., & Pun, T. (2000). Robust template matching for affine resistant image watermarks. *IEEE Transactions on Image Processing*, 9(6), 1123–1129. doi:10.1109/83.846253
- Perez-Gonzalez, F., & Hernandez, J. R. (1999). A Tutorial on Digital Watermarking. In *Proceeding of IEEE 33rd Annual International Carnahan Conference on Security Technology*, 286-292.
- Petitcolas, F. A. P. (2000). Introduction to information hiding. In Katzenbeisser, S., & Petitcolas, F. A. P. (Eds.), *Information Hiding techniques for steganography and digital watermarking*.
- Petitcolas, F. A. P. (2002). *StirMark 4.0*. Retrieved from <http://www.petitcolas.net/fabien/watermarking/-stirmark/index.html>
- Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1998). Attacks on copyright marking systems. In D. Aucsmith (Ed.), Second workshop on information hiding (LNCS Vol. 1525). Portland, OR: Springer.
- Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1998). Attacks on copyright marking systems. Information Hiding: Second International Workshop, (LNCS Vol. 1525, pp. 218-238). Berlin: Springer-Verlag.
- Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—A Survey. In *Proc. IEEE* 87(7, July), 1062–1078.
- Petitjean, G., Dugelay, J. L., Gabriele, S., Rey, C., & Nicolai, J. (2002). Towards Real-time Video Watermarking for Systems- On-Chip. In *Proceedings of the IEEE International Conference on Multimedia and Expo* (Vol. 1), (pp. 597–600).
- Pfitzmann, B., & Sadeghi, A. R. (1999). Coin-based anonymous fingerprinting. Advances In Cryptology-Eurocrypt'99, (LNCS Vol. 1592, pp. 150-164). Berlin: Springer-Verlag.
- Pfitzmann, B., & Schunter, M. (1996). Asymmetric fingerprinting. Advances in Cryptology -Eurocrypt'96. (LNCS Vol. 1070, pp. 84-95). Berlin: Springer-Verlag.
- Pfitzmann, B., & Waidner, M. (1997). Anonymous fingerprinting. Advances In Cryptology - Eurocrypt'97. (LNCS Vol. 1233, pp. 88–102). Berlin: Springer-Verlag.
- Phadikar, A., Maity, S. P., & Kundu, M. K. (2009). An Optimized Image Database Watermarking Scheme using Genetic Algorithms and Lifting. In *Proceedings of IEEE International Advanced Computing*, (pp. 2151-2155).
- Pirsch, P., Demassieux, N., & Gehrke, W. (1995). VLSI architectures for video compression: a survey. *Proceedings of the IEEE*, 83(2), 220–246. doi:10.1109/5.364465
- Piva, A., Barni, M., & Bartolini, F. (2002). Managing copyright in open networks. *IEEE Internet Computing*, 6(3), 18–26. doi:10.1109/MIC.2002.1003126
- Piva, A., Barni, M., Bartolini, F., & Cappellini, V. (1997). DCT-Based watermark recovering without restoring to the uncorrupted original image. *International Conference on Image Processing*, III, (pp. 520 - 523).
- Piva, A., Bartolinin, F., Cappellini, V., & Barni, M. (1999). Exploiting the cross-correlation of RGB-channels for robust watermarking of color images. In *International Conference on Image Processing* (Vol. 1, pp. 306-310).
- Potdar, V. M., Han, S., & Chang, E. (2005). A Survey of Digital Image Watermarking Techniques. *Proceedings of the 3rd International Conference on Industrial Informatics*, (pp. 709 - 716).
- Prasad, M., & Koliwad, S. (2009). A comprehensive survey of contemporary researches in watermarking for copyright protection of digital images. *International Journal of Computer Science and Network Security*, 9(4), 91–107.
- Praun, E., Hoppe, H., & Finkelstein, A. (1999). Robust mesh watermarking. In *Proceedings of SIGGRAPH*, 99, 49–56.
- Prokop, R.J., & Reeves, A.P. (1992). A survey of moment-based techniques for unoccluded object representation and recognition. In *Proceedings, CVGIP: Vol. 54. Graphical models and Image Processing* (pp. 438-460). Orlando, FL: Academic Press, Inc.

- Provost, N., & Honeyman, P. (2003). Hide and seek: an introduction to steganography. *IEEE Security and Privacy Magazine, IEEE. Computers & Society*, 32–44.
- Puate, J., & Jordan, F. (1996). Using Fractal Compression Scheme to Embed a digital Signature into an Image. In *Proc. of SPIE Photonics East Symposium*.
- Qi, X., Bialkowski, S., & Brimley, G. (2008). An adaptive QIM- and SVD-based digital image watermarking scheme in the wavelet domain. In *Proceedings of the 15th IEEE International Conference on Image Processing* (pp. 421-424).
- Qiao, L., & Nahrstedt, K. (1998). Watermarking schemes and protocols for protecting rightful ownership. *Journal of Visual Communication and Image Representation*, 9(3), 194–210. doi:10.1006/jvci.1998.0391
- Qiu, G. (2004). Embedded colour image coding for content-based retrieval. *Journal of Visual Communication and Image Representation*, 15(4), 507–521. doi:10.1016/j.jvcir.2003.11.002
- Quadir, A., & Ahmad, I. (2005, October). Digital Text Watermarking: Secure Content Delivery and Data Hiding in Digital Documents. In *Proceeding of 39th Annual International Carnahan Conference on Security Technology* (CCST'05), (pp. 101- 104).
- Quan, L., & Qingsong, A. (2004). A combination of DCT-based and SVD-based watermarking scheme. In *Proceedings of the 7th international Conference on Signal Processing: Vol. 3* (pp. 873-876).
- Quan, L., & Xiaomei, Z. (2006). A SVD Based Digital Watermarking Algorithm for 3D Models. In *Proceedings of the 8th International Conference on Signal Processing: Vol. 4*.
- Rabie, T. (2004). Adaptive hybrid mean and median filtering of high-ISO long-exposure sensor noise for digital photography. *SPIE Journal of Electronic Imaging*, 13(2), 264–277. doi:10.1117/1.1668279
- Rabie, T. (2006, November 19-21). A Novel Compression Technique for Super Resolution Color Photography. In *Proceedings of the IEEE International Conference on Innovations in Information Technology (IIT2006)*, (pp. 1-5), Jumeirah Beach Hotel, Dubai, UAE.
- Rabie, T. (2007). Frequency-domain data hiding based on the Matryoshka principle. *Int. J. Advanced Media and Communication*, 1(3), 298–312. doi:10.1504/IJAMC.2007.013952
- Rabie, T., & Guerchi, D. (2007, November 24-27). Magnitude Spectrum Speech Hiding. In *IEEE International Conference on Signal Processing and Communication (ICSPC07)*, Dubai, UAE.
- Ramkumar, M., & Akansu, A. (2004). A Robust Protocol for Proving Ownership of Multimedia Content. *IEEE Transactions on Multimedia*, 6(3), 496–478. doi:10.1109/TMM.2004.827494
- Ramkumar, M., Akansu, A., & Alatan, A. (1999). A robust data hiding scheme for images using DFT. In *Proc. IEEE International Conference on Image Processing (ICIP)*, (pp.1-5).
- Reddy, A., & Chatterji, B. (2005). A New Wavelet Based Logo-watermarking Scheme. *Pattern Recognition Letters*, 26(7), 1019–1027. doi:10.1016/j.patrec.2004.09.047
- Rey, C., & Dugelay, J.-L. (2002). A survey of watermarking algorithms for image authentication. *EURASIP Journal on Applied Signal Processing*, (1): 613–621. doi:10.1155/S1110865702204047
- Rezazadeh, S., & Yazdi, M. (2006). A Nonoblivious Image Watermarking System Based on Singular Value Decomposition and Texture Segmentation. *Proceedings of the World Academy of Science, Engineering and Technology*, 13, 255-259.
- Rivest, R., Adleman, L., & Dertouzos, M. (1978). *On data banks and privacy homomorphisms. Foundations of Secure Computation* (pp. 169–179). New York: Academic Press.

Compilation of References

- Rodríguez, M. A., & González, F. P. (2002). Analysis of pilot-based synchronization algorithms for watermarking of still images. *Signal Processing Image Communication*, 17(8), 661–633.
- Rondao-Alface, P., & Macq, B. (2005). Blind watermarking of 3D meshes using robust feature points detection. In *Proc. of the IEEE International Conference on Image Processing*, (vol. 1, pp. 693–696).
- Rondao-Alface, P., & Macq, B. (2007). From 3D mesh data hiding to 3D shape blind and robust watermarking: A survey. *LNCS Transactions on Data Hiding and Multimedia Security*, 2, 99–115.
- Rothe, I., Susse, H., & Voss, K. (1996). The method of normalization to determine Invariants. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18(4), 366–376. doi:10.1109/34.491618
- Rouvroy, G., Lefebvre, F., Standaert, F.-X., Macq, B., Quisquater, J.-J., & Legat, J.-D. (2004). Hardware Implementation of a Fingerprinting Algorithm Suited for Digital Cinema. *European Signal Processing Conference*, (pp. XXXV-2310).
- Rouvroy, G., Standaert, F.-X., Lefebvre, F., Quisquater, J.-J., Macq, B., & Legat, J.-D. (2004). Reconfigurable Hardware Solutions for the Digital Rights Management of Digital Cinema. In *Proceedings of the 4th ACM Workshop on Digital Rights Management* (pp. 40 - 53). Washington, DC: ACM.
- Roy, S., & Chang, E. (2004). Watermarking color histograms. In *International Conference on Image Processing* (Vol. 4, pp. 2191-2194).
- Ruanaidh, J. J. K. O., & Pun, T. (1998). Rotation, scale, and translation invariant spread spectrum digital image watermarking. *Signal Processing*, 66, 303–317. doi:10.1016/S0165-1684(98)00012-7
- Ruiz, F., & Deller, J. (2000). Digital watermarking of speech signals for the national gallery of the spoken word. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (pp. 1499–1502).
- Rustamov, R. M. (2007). Laplace-Beltrami eigenfunctions for deformation invariant shape representation. In *Proc. of the Symposium on Geometry processing* (pp. 225-233).
- Rykaczewski, R. (2007). Comments on „An SVD-Based Watermarking Scheme for Protecting Rightful Ownership. *IEEE Transactions on Multimedia*, 9(2), 421–423. doi:10.1109/TMM.2006.886297
- Sadeghi, A.-R. (2008). The Marriage of Cryptography and Watermarking -- Beneficial and Challenging for Secure Watermarking and Detection. In *Proceedings of the 6th International Workshop on Digital Watermarking*, (pp. 2 - 18).
- Safabakhsh, R., Zaboli, S., & Tabibazar, A. (2004). Digital Watermarking on Still Images Using Wavelet Transform. In *Proceedings of the International IEEE Conference on Information Technology: Coding and Computing*, Las Vegas, Nevada.
- Schaefer, G., & Stich, M. (2004). UCID-An Uncompressed Color Image Database. In *Proceedings of Society of Photo-Optical Instrumentation Engineers, Storage and Retrieval Methods and Applications for Multimedia*: Vol. 5307 (pp. 472-480). Bellingham, WA: SPIE Press.
- Schanda, J. (2007). *Colorimetry* (p. 61). New York: Wiley-Interscience. doi:10.1002/9780470175637
- Schneier, B. (2000). *Secrets and lies. digital security in a networked world*. Chichester, UK: John Wiley and Sons, Inc.
- Schulzrinne, G., Paul, S., Maxemchuk, N. F., & Choudhury, A. K. (1995, May/June). Copyright Protection for Electronic Publishing Over Computer Networks. *IEEE Network*, 9(3), 12–20. doi:10.1109/65.386048
- Schyndel, R. G., Tirkel, A. Z., & Osborne, C. F. (1994). A digital watermark. *Proceedings of the IEEE International Conference on Image Processing*, 2, 86–90.
- Sebe, F., & Ferrer, J. D. (2002). Oblivious image watermarking robust against scaling and geometric distortions. In *4th International Conference on Information Security*. (LNCS Vol. 2200, pp. 420-432). Berlin: Springer-Verlag.

- Sebe, F., Domingo-Ferrer, J., & Herrera, J. (2000). Spatial Domain Image Watermarking Robust Against Compression, Filtering, Cropping, and Scaling. In *Proceedings of the 3rd Int. Workshop on Info. Security*, Australia.
- Sehirli, M., Gurgen, F., & Ikizoglu, S. (2004). Performance evaluation of digital audio watermarking techniques designed in time, frequency and cepstrum domains. In *Proceedings of the International Conference on Advances in Information Systems*, (pp. 430–440).
- Sencar, H. T., & Memon, N. (2005, November). Watermarking and Ownership Problem – A Revisit. In *Proceedings of the 5th ACM workshop on Digital rights management*, (pp. 93–101).
- Seo, Y. H., & Kim, D. W. (2003). Real-Time Blind Watermarking Algorithm and its Hardware Implementation for Motion JPEG2000 Image Codec. In *Proceedings of the 1st Workshop on Embedded Systems for Real-Time Multimedia*, (pp. 88–93).
- Seok, J. W., & Hong, J. W. (2001). Audio watermarking for copyright protection of digital audio data. *Electronics Letters*, 37(1), 60–61. doi:10.1049/el:20010029
- Sequeira, A., & Kundur, D. (2001). Communications and information theory in watermarking: A survey. In *Proceedings of SPIE Multimedia Systems and Application IV*, 4518, 216–227.
- Servette, S. D., Podilchuk, C., & Ramchandran, K. (1998). Capacity issues in digital watermarking. In *Proceedings of the IEEE International Conference on Image Processing, ICIP-98*, (Vol. 1, pp. 445–449).
- Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, 27, 379–423.
- Shannon, C. E. (1958). Channels with side information at the transmitter. *IBM Journal*, 289–293.
- Shao, M.-H. (2007). A privacy-preserving buyer-seller watermarking protocol with semi-trust third party. Trust, Privacy and Security in Digital Business, (LNCS Vol. 4657, pp. 44–53). Berlin: Springer-Verlag.
- Shapira, L., Shamir, A., & Cohen-Or, D. (2008). Consistent mesh partitioning and skeletonization using the shape diameter function. *The Visual Computer*, 24(4), 249–259. doi:10.1007/s00371-007-0197-5
- Sharma, G. (2002). *Digital Color Imaging Handbook*. Boca Raton, FL: CRC Press, Inc.
- Shen, D., & Ip, H. S. (1997). Generalized affine invariant image normalization. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(5), 431–440. doi:10.1109/34.589203
- Shen, D., & Ip, H. S. (1998). Discriminative wavelet shape descriptors for recognition of 2-d patterns. *Pattern Recognition*, 32(2), 151–165. doi:10.1016/S0031-3203(98)00137-X
- Shen, D., Ip, H. S., Cheung, K. K. T., & Teoh, E. K. (1999). Symmetry detection by generalized complex (GC) moments: A close-form solution. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 21(5), 466–476. doi:10.1109/34.765657
- Shen, Y.-Z., Zhang, M.-J., & Liu, F. (2006). A new algorithm of gray watermark Embedding. In Pan, Z. (Eds.), *Advances in Artificial Reality and Tele-Existence* (Vol. 4282, pp. 769–801). Berlin: Springer-Verlag. doi:10.1007/11941354_82
- Sheppard, N. P., Safavi-Naini, R., & Liu, Q. (2003). Digital Rights Management for Content Distribution. In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*, 21, 49–58.
- Shi, J., & Tomasi, C. (1994). Good features to track. In *Proceedings of the IEEE Conference of Computer Vision and Pattern Recognition (CVPR'94)*.
- Shieh, C. S., Huang, H.-C., Wang, F. H., & Pan, J. S. (2004). Genetic watermarking based on transform domain techniques. *Pattern Recognition*, 37(3), 555–565. doi:10.1016/j.patcog.2003.07.003
- Shieh, J.-M., Lou, D.-C., & Chang, M.-C. (2006). A semi-blind digital watermarking scheme based on singular value decomposition. *Computer Standards & Interfaces*, 28(4), 428–440. doi:10.1016/j.csi.2005.03.006

Compilation of References

- Shih, F. Y., & Edupuganti, V. G. (2009). A differential evolution based algorithm for breaking the visual steganographic system, *Bio-inspired information hiding: A fusion of foundations, methodologies and applications*, 13(4), 345-353.
- Shih, F. Y. (2004). *Digital watermarking and steganography- fundamental and techniques*. Boca Raton, FL: CRC Press.
- Shih, F. Y., & Wu, Y. T. (2005). Robust watermarking and compression for medical images based on genetic algorithms. *Information Sciences*, 176, 200–216. doi:10.1016/j.ins.2005.01.013
- Shnayderman, A., Gusev, A., & Eskicioglu, A. (2004). A Multidimensional Image Quality Measure Using Singular Value Decomposition. In Y. Miyake et al. (Eds.), *Image Quality and System Performance Conference: vol. 5294* (pp. 82–92). Bellingham WA: SPIE Press.
- Shukran, M., Chung, Y., & Chen, X. (2007). Implementation of a New H.264 Video Watermarking Algorithm with Usability Test. In *Human-Computer Interaction. HCI Intelligent Multimodal Interaction Environments*.
- Shutler, J. (2002). Statistical moments. In CVonline: On-line compendium of computer vision. R. Fisher (ed.) Available: <http://homepages.inf.ed.ac.uk/rbf/CVonline/>.
- Simone, F. D., Ticca, D., Dufaux, F., Ansorge, M., & Ebrahimi, T. (2008). A comparative study of color image compression standards using perceptually driven quality metrics. In *Applications of Digital Image Processing XXXI* (Vol. 7073, pp. 70730Z-70730Z-11). SPIE.
- Sinha, N. K. (1991). *Linear Systems*. New York: Wiley.
- Sion, R., & Atallah, M. (2004). *Fellow, Rights Protection for Relational Data (Vol. 16)*. IEEE Transactions on Knowledge and Data Engineering.
- Smith, J. R., & Comiskey, B. O. (1996). Modulation and Information Hiding in Images. In *Proceedings of the First Information Hiding Workshop*, (pp. 207 - 226).
- Solanki, K., Jacobsen, N., Madhow, U., Manjunath, B. S., & Chandrasekaran, S. (2004). Robust image-adaptive data hiding using erasure and error correction. *IEEE Transactions on Image Processing*, 13(12), 1627–1639. doi:10.1109/TIP.2004.837557
- Solanki, K., Sarkar, A. & Manjunath, B. S. (2007). YASS: yet another steganographic scheme that resists blind steganalysis. In *9th International Workshop on Information Hiding*, Saint Malo, Brittany, France.
- Sorkine, O., Cohen-Or, D., & Toledo, S. (2003). High-pass quantization for mesh encoding. In *Proc. of the Symposium on Geometry Processing* (pp. 42-51).
- Sparr, G. (1996). *Proceedings of the 13th International Conference on Pattern Recognition (Vienna)*, (pp. 328-333). Washington, DC: IEEE Compute. Soc. Press.
- Stallings, W. (2003). *Cryptography and Network Security Principles and Practice*. Upper Saddle River, NJ: Pearson Education International.
- Steinebach, M., Petitcolas, F., Raynal, F., Dittmann, J., Fontaine, C., Seibel, S., et al. (2001). Stirmark benchmark: Audio watermarking attacks. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, (pp. 49–54).
- Strang, G., & Nguyen, T. (1996). *Wavelets and Filter Banks*. New York: Wellesley-Cambridge Press.
- Strycker, L. D., Termont, P., Vandewege, J., Haitsma, J., Kalker, A., & Maes, M. (2000). Implementation of a realtime digital watermarking process for broadcast monitoring on Trimedia VLIW processor. *IEE Proceedings. Vision Image and Signal Processing*, 147(4), 371–376. doi:10.1049/ip-vis:20000580
- Strycker, L. D., Termont, P., Vandewege, J., Haitsma, J., Kalker, A., Maes, M., & Depovere, G. (2000). Implementation of a real-time digital watermarking process for broadcast monitoring on trimedia VLIW processor. *IEE Proceedings. Vision Image and Signal Processing*, 147, 371–376. doi:10.1049/ip-vis:20000580

- Su, J. K., Eggers, J. J., & Girod, B. (2000) Optimum attack on digital watermarks and its defense. In *Proceedings of 34th Asilomar Conference on Signals, Systems and Computers*, Asilomar, CA, USA.
- Su, J. K., Eggers, J. J., & Girod, B. (2001). Analysis of digital watermarks subjected to optimum linear filtering and additive noise. *Signal Processing*, 81, 1141–1175. doi:10.1016/S0165-1684(01)00038-X
- Sugihara, R. (2001). Practical capacity of digital watermark as constrained by reliability. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, (pp. 85–89).
- Sun, R., Sun, H., & Yao, T. (2002). A SVD and quantization based semi-fragile watermarking technique for image authentication. In *Proceedings of the 6th International Conference on Signal Processing: Vol. 2*(pp. 1592-1595).
- Sun, X., Luo, G., & Huang, H. (2004, November). Component-Based Digital Watermarking of Chinese Texts. In *Proceedings of the 3rd international conference on Information security*, 81, 76-81.
- Sverdlov, A., Dexter, S., & Eskicioglu, A. M. (2005). Robust dct-svd domain image watermarking for copyright protection: embedding data in all frequencies. In J. Dittmann (Ed.), *Proceedings of the 2004 Workshop on Multimedia and Security* (pp. 168-174). New York: ACM Press.
- Swanson, M. D., Kobayashi, M., & Tewfik, A. H. (1998). Multimedia data-embedding and watermarking technologies. In *IEEE International Conference on Communications*, 2, 823-827.
- Swanson, M., Zhu, B., & Tewfik, A. (1999). Current state-of-the-art, challenges and future directions for audio watermarking. In *Proceedings of the IEEE International Conference on Multimedia Computing and Systems*, (pp. 19–24).
- Swanson, M., Zhu, B., Tewfik, A., & Boney, L. (1998). Robust audio watermarking using perceptual masking. *Signal Processing*, 66(3), 337–355. doi:10.1016/S0165-1684(98)00014-0
- Tachibana, R., Shimizu, S., Kobayashi, S., & Nakamura, T. (2002). An audio watermarking method using a two-dimensional pseudo-random array. *Signal Processing*, 82(10), 1455–1469. doi:10.1016/S0165-1684(02)00284-0
- Takamatsu, R., Sato, M., & Kawarada, H. (1997). Pointing device gazing at hand based on local moments. In *Proceedings, Real-Time Imaging II* (Vol. 3028, pp. 155-163). San Jose, CA: SPIE.
- Tan, C. (2002). *Image Camou-Flaging using Phase Randomization*. Retrieved from <http://pachome2.paci.c.net.sg/chewkeong/ImgCamou.pdf>
- Tang, X., Yang, L., Li, L., & Niu, Y. (2004). Study on a Multifunctional watermarking Algorithm. In. *Proceedings of the IEEE International Conference Signal Processing*, 1, 848–852.
- Teague, M. R. (1980). Image analysis via the general theory of moments. *Journal of the Optical Society of America*, 70, 920–930. doi:10.1364/JOSA.70.000920
- Tefas, A., & Pitas, I. (2001). Robust spatial image watermarking using progressive detection. In. *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, 3, 1973–1976.
- Tefas, A., Nikolaidis, A., Nikolaidis, N., Solachidis, V., Tsekeridou, S., & Pitas, I. (2003). Performance analysis of correlation-based watermarking schemes employing Markov chaotic sequences. *IEEE Transactions on Signal Processing*, 51(7), 1979–1994. doi:10.1109/TSP.2003.811245
- Teh, C. H., & Chin, R. T. (1988). On Image analysis by the method of moments. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 10, 485–513. doi:10.1109/34.3913
- Termont, P., De Strycker, L., Vandewege, J., Haitsma, J., Kalker, T., Maes, M., et al. (1999). Performance measurements of a real-time digital watermarking system for broadcast monitoring. In *Proc. IEEE International Conference on Multimedia Computing and Systems*, Florence, Italy, (pp. 220–224).

Compilation of References

- Termont, P., De Stycker, L., Vandewege, J., Op de Beeck, M., Haitsma, J., Kalker, T., et al. (2000). How to achieve robustness against scaling in a real-time digital watermarking system for broadcast monitoring. In *Proc. IEEE International Conference on Image Processing*, Vancouver, Canada, (pp. 407–410).
- Theimert, S., Steinebach, M., & Wolf, P. (2006, September). A Digital Watermarking for Vector-Based Fonts. In *Proceedings of the 8th workshop on Multimedia and security*, (pp. 120-123).
- Thomas, J., Chareyron, G., & Treméau, A. (2007). Image watermarking based on a color quantization process. In A. Hanjalic (Ed.), *Multimedia Content Access: Algorithms and Systems* (Vol. 6506, pp. 650603-650603-12). SPIE.
- Thomson. (2009). Retrieved from <http://www.thomson.net/GlobalEnglish/Corporate/News/PressReleases/Pages/thomson-showcases-powerful-broadband-home-networking-ecosystem-at-cebit-2008-with-several-new-products.aspx>
- Tilki, J., & Beex, A. (1997). Encoding a hidden auxiliary channel onto a digital audio signal using psychoacoustic masking. In *Proceedings of the IEEE South East Conference*, (pp. 331–333).
- Ting, G. C.-W. (2006). Ambiguity Attacks on the Ganic-Eskicioglu Robust DWT-SVD Image Watermarking Scheme. In Won, D. (Eds.), *Information Security and Cryptology-ICISC 2005* (Vol. 3935, pp. 378–389). Berlin: Springer-Verlag. doi:10.1007/11734727_30
- Ting, G. C.-W., Goi, B.-M., & Heng, S.-H. (2007). A fragile watermarking scheme protecting originator's rights for multimedia service. In Gervasi, O. (Eds.), *Computational Science and Its Applications* (Vol. 4705, pp. 644–654). Berlin: Springer-Verlag.
- Ting, G. C.-W., Goi, B.-M., & Heng, S.-H. (2009). Attack on a semi-blind watermarking scheme based on singular value decomposition. *Computer Standards & Interfaces*, 31(2), 523–525. doi:10.1016/j.csi.2008.02.007
- Toch, B., & Lowe, D. (2005). Watermarking of medical signals. In *Proc. 2nd Int. Conf. on Computational Intelligence in Medicine and Healthcare*, Lisbon, Portugal, (pp. 231- 236).
- Toch, B., Lowe, D., & Saad, D. (2003). Watermarking of audio signals using Independent Component Analysis. In *3rd International Conference on WEB Delivering of Music (WEDELMUSIC'03)*, (pp. 71-74).
- Topkara, M., Kamara, A., Atallah, M., & Nita-Rotaru, C. (2005). ViWiD: Visible watermark based defense against phishing. [LNCS]. *Lecture Notes in Computer Science*, 470–484. doi:10.1007/11551492_36
- Toutant, J., Puech, W., & Fiorio, C. (2006). Minimizing Data-Hiding Noise in Color JPEG Images by Adapting the Quantization. In *Conference on Colour in Graphics Imaging and Vision* (pp. 387-391).
- Tovée, M. J. (2008). *An Introduction to the Visual System Edition: 2*. Cambridge, UK: Cambridge University Press.
- Trappe, W., Wu, M., Wang, Z., & Liu, K. (2003). Anti-collusion fingerprinting for multimedia. *IEEE Transactions on Signal Processing*, 51(4), 1069–1087. doi:10.1109/TSP.2003.809378
- Trefethen, L. N., & David, B. (1997). The Singular Value Decomposition. In *Numerical Linear Algebra* (pp. 25–31). Philadelphia, PA: Society for Industrial and Applied Mathematics.
- Tréneau, A., Tominaga, S., & Plataniotis, K. (2008). *Color in Image and Video Processing: Most Recent Trends and Future Research Directions*. EURASIP Journal on Image and Video Processing.
- Tsai, C.-F., & Yang, W.-Y. (2007). Real-time color image watermarking based on D-SVD scheme. In Mery, D., & Rueda, L. (Eds.), *Advances in Image and Video Technology* (Vol. 4872, pp. 289–297). Berlin: Springer-Verlag. doi:10.1007/978-3-540-77129-6_27
- Tsai, H., & Sun, D. (2007). Color image watermark extraction based on support vector machines. *Information Sciences*, 177(2), 550–569. doi:10.1016/j.ins.2006.05.002

- Tsai, P., Hu, Y., & Chang, C. (2004). A color image watermarking scheme based on color quantization. *Signal Processing*, 84(1), 95–106. doi:10.1016/j.sigpro.2003.07.012
- Tsai, T. H., & Lu, C. Y. (2001). A systems level design for embedded watermark technique using DSC systems. In *Proceedings of the IEEE International Workshop on Intelligent Signal Processing and Communication Systems*.
- Tsai, T. H., & Wu, C. Y. (2003). An Implementation of Configurable Digital Watermarking Systems in MPEG Video Encoder. In *Proceedings of the IEEE International Conference on Consumer Electronics*, (pp. 216–217).
- Tsui, T. K., Zhang, X.-P., & Androutsos, D. (2006). Color Image Watermarking Using the Spatio-Chromatic Fourier Transform. In *Acoustics, Speech and Signal Processing, 2006. ICASSP 2006 Proceedings. 2006 IEEE International Conference on* (Vol. 2, pp. II-II).
- Tuceryan, M. (1994). Moment-based texture segmentation. *Pattern Recognition Letters*, 15, 115–123. doi:10.1016/0167-8655(94)90069-8
- Uccheddu, F., Corsini, M., & Barni, M. (2004). Wavelet-based blind watermarking of 3D models. In *Proc. of the ACM Workshop on Multimedia and Security* (pp. 143-154).
- Ungerboeck, G. (1987). Trellis-coded modulation with redundant signal sets, parts i and ii. *IEEE Communications Magazine*, 25, 5–21. doi:10.1109/MCOM.1987.1093542
- Vallet, B., & Lévy, B. (2007). *Manifold harmonics*. Technical Report of INRIA - ALICE Project Team.
- Vallet, B., & Lévy, B. (2008). Spectral geometry processing with manifold harmonics. *Computer Graphics Forum*, 27(2), 251–260. doi:10.1111/j.1467-8659.2008.01122.x
- Van Leest, A., Haitsma, J., & Kalker, T. (2003). On digital cinema and watermarking. *SPIE Proceedings Security and Watermarking of Multimedia Contents V*, 5020, 526–535.
- van Schyndel, R., Tirkel, A., & Osborne, C. (1994). A digital watermark. In *International Conference on Image Processing* (Vol. 2, pp. 86-90).
- Vidal, J., Madueno, M., & Sayrol, E. (2002). Color image watermarking using channel-state knowledge. In *Security and watermarking of multimedia contents IV* (Vol. 4675, pp. 214-221).
- Viterbi, A. (1967). Error bounds for convolution codes and an asymptotically optimum decoding algorithm. *IEEE Transactions on Information Theory*, 13, 260–269. doi:10.1109/TIT.1967.1054010
- Voloshynovskiy, S., Pereira, S., Herrigel, A., Baumgartner, N., & Pun, T. (2000). Generalized watermark attack based on watermark estimation and perceptual remodulation. In P. W. Wong, E. J. Delp III (Ed.), *Security and Watermarking of Multimedia Contents II*, (Vol. 3971, Attack, pp. 445-449). San Jose: SPIE.
- Voloshynovskiy, S., Deguillaume, F., & Pun, T. (2000). Content Adaptive Watermarking Based on a Stochastic Multi-resolution Image Modeling. In *Tenth European Signal Processing Conference*.
- Voloshynovskiy, S., Deguillaume, F., Koval, O., & Pun, T. (2003). Information-Theoretic Data-Hiding for Public Network Security, Services Control and Secure Communications. *IEEE Int. Conf. on Telecomm. in Modern Satellite, Cable and Broadcasting Service*, 1, 3-17.
- Voloshynovskiy, S., Pereira, S., Iquise, V., & Pun, T. (1988). Attack modeling: towards a second generation watermarking benchmark. *Signal Processing*, 81, 1177–1214. doi:10.1016/S0165-1684(01)00039-1
- Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J., & Su, J. (2001). Attacks on digital watermarks: Classification, estimation-based attacks and benchmarks. *IEEE Communications Magazine*, 39(9), 118–126. doi:10.1109/35.940053
- Vontobel, P. O., Kavcic, A., Arnold, D. M., & Loeliger, H.-A. (2008). A generalization of the Blahut–Arimoto algorithm to finite-state channels. *IEEE Transactions on Information Theory*, 54(5), 1887–1918. doi:10.1109/TIT.2008.920243
- Voyatzis, G., & Pitas, I. (1999). Protecting digital-image copyrights: a framework. *IEEE Computer Graphics and Applications*, 19, 18–24. doi:10.1109/38.736465

Compilation of References

- Wagner, N. R. (1983). Fingerprinting. In *IEEE Symposium on Security and Privacy 1983*, (pp. 18-22).
- Wang, C., Doherty, J., & Van Dyke, R. (2002). A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images. *IEEE Transactions on Image Processing*, 11(2), 77–78. doi:10.1109/83.982816
- Wang, C.-M., & Cheng, Y.-M. (2005). An efficient information hiding algorithm for polygon models. *Computer Graphics Forum*, 24(3), 591–600. doi:10.1111/j.1467-8659.2005.00884.x
- Wang, H.-X., Lu, Z.-M., & Sun, S.-H. (2008). A Blind Video Watermarking Algorithm Based on SVD in the DCT Domain. In *Proceeding of the International Electronic Conference on Computer Science: Vol. 1060* (pp. 360-364).
- Wang, J., Liu, J. C., & Masilela, M. (2009). A real-time video watermarking system with buffer sharing for video-on-demand service. *Computers & Electrical Engineering*, 35(2), 395–414. doi:10.1016/j.compeleceng.2008.06.011
- Wang, K., Lavoué, G., Denis, F., & Baskurt, A. (2008). A comprehensive survey on three-dimensional mesh watermarking. *IEEE Transactions on Multimedia*, 10(8), 1513–1527. doi:10.1109/TMM.2008.2007350
- Wang, K., Lavoué, G., Denis, F., & Baskurt, A. (2008). Hierarchical watermarking of semiregular meshes based on wavelet transform. *IEEE Transactions on Information Forensics and Security*, 3(4), 620–634. doi:10.1109/TIFS.2008.2007229
- Wang, K., Luo, M., Bors, A. G., & Denis, F. (2009). Blind and robust mesh watermarking using manifold harmonics. In *Proc. of the IEEE International Conference on Image Processing*.
- Wang, R. Z., Lin, C. F., & Lin, J. C. (2000). Hiding data in images by optimal moderately significant-bit replacement. *IEEE Electronics Letters*, 36(25), 2069–2070. doi:10.1049/el:20001429
- Wang, R. Z., Lin, C. F., & Lin, J. C. (2001). Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition Letters*, 34(3), 671–683.
- Wang, W.-B., Zheng, G.-Q., Yong, J.-H., & Gu, H.-J. (2008). A numerically stable fragile watermarking scheme for authenticating 3D models. *Computer Aided Design*, 40(5), 634–645. doi:10.1016/j.cad.2008.03.001
- Wang, X., & Zhao, H. (2006). A novel synchronization invariant audio watermarking scheme based on DWT and DCT. *IEEE Transactions on Signal Processing*, 54(12), 4835–4840. doi:10.1109/TSP.2006.881258
- Wang, X., Xu, Z., & Yang, H. (2009). A robust image watermarking algorithm using SVR detection. *Expert Systems with Applications*, 36(5), 9056–9064. doi:10.1016/j.eswa.2008.12.040
- Wang, Y. G., Lu, Z. M., Fan, L., & Zheng, Y. (2009). Robust dual watermarking algorithm for AVS video. *Signal Processing Image Communication*, 24, 333–344. doi:10.1016/j.image.2009.03.004
- Wang, Z., Bovik, A., Sheikh, H., & Simoncelli, E. (2004). Image quality assessment: from error visibility to structural similarity. *Image Processing. IEEE Transactions on*, 13(4), 600–612.
- Watson, A. (1990). Perceptual-components architecture for digital video. *Journal of the Optical Society of America. A, Optics and Image Science*, 7(10), 1943–1954. doi:10.1364/JOSAA.7.001943
- Watson, A. B. (Ed.). (1993). *Digital images and human vision* (p. 224). Cambridge, MA: MIT Press.
- Wei, L., & Xue, X. (2003). An audio watermarking technique that is robust against random cropping. *Computer Music Journal*, 27(4), 58–68. doi:10.1162/014892603322730505
- Wen, X. B., Zhang, H., Xu, X. Q. & Quan, J.J. (2009). A new watermarking approach based on probabilistic neural network in wavelet domain. *Bio-inspired information hiding: A fusion of foundations, methodologies and applications*, 13(4), 355-360.
- Westfeld, A., & Pfitzmann, A. (1999). Attacks on steganographic systems. In *Proc. 3rd Int'l Workshop on Information Hiding*, (pp.61–76). London: Springer Verlag.

- Wiegand, T., Sullivan, G. J., Bjontegaard, G., & Luthra, A. (2003). Overview of the H.264/AVC video coding standard. *IEEE Trans. on Circuits and Systems for Video Technology*, 13(7), 560–576. doi:10.1109/TCSVT.2003.815165
- Wilkinson, S. (2005). *Hide and seek: robust digital watermarking*. Technical Report, School of computing. Leeds, UK: University of Leeds.
- Wipo. (2009). Retrieved from <http://www.wipo.int/pctdb/en/wo.jsp?IA=WO2000067479&DISPLAY=STATUS&services-in-a-telecommunications-network-dt20061228ptan20060294186.php>
- Wolfgang, R., Podilchuk, C., & Delp, E. (1998). The effect of matching watermark and compression transforms in compressed color images. In *Image Processing, ICIP 98, Proceedings, 1998 International Conference on* (Vol. 1, pp. 440-444 vol.1).
- Wong, P. H. W., Au, O. C., & Yeung, Y. M. (2003). A novel blind multiple watermarking techniques for images. *IEEE Trans. on Circuits and Systems for Video Technology*, 13, 813–830. doi:10.1109/TCSVT.2003.815948
- Wong, P. W. (1998). A public key watermark for image verification and authentication. *Proceedings of the International Conference on Image Processing*, 1, 455–459.
- Wong, P. W., & Memon, N. (1998, July). Protecting Digital Media Content. *ACM Communication*, 41(7), 35–43. doi:10.1145/278476.278485
- Wong, P.-W., & Memon, N. (2000). Secret and public key authentication watermarking schemes that resist vector quantization attack. In Wong, P. W. (Eds.), *Security and Watermarking of Multimedia Contents* (pp. 417–427). Bellingham, WA: SPIE Press.
- Wood, J. (1996). Invariant pattern recognition: A review. *Pattern Recognition*, 29(1), 1–17. doi:10.1016/0031-3203(95)00069-0
- Woon, W. L., & Lowe, D. (2001). Nonlinear Signal Processing for Noise Reduction of Unaveraged Single Channel MEG Data. In *Proc. Int. Conf. Artificial Neural Networks*, (pp. 650 -657).
- Wu, C., Su, P., & Kuo, J. (2000). Robust and Efficient Digital Audio Watermarking Using Audio Content analysis. In *Proceedings of the SPIE 12th International Symposium on Electronic Imaging, CA* (Vol. 3971, pp. 382-392).
- Wu, D., Kong, W., Yang, B., & Niu, X. (2008). A fast SVD based video watermarking algorithm compatible with MPEG2. *Standard Soft Computing - A Fusion of Foundations. Methodologies and Applications*, 13(4), 375–382.
- Wu, H.-C., Yeh, C.-P., & Tsai, C.-S. (2006). A Semi-fragile Watermarking Scheme Based on SVD and VQ Techniques. In Gavrilova, M. (Eds.), *Computational Science and Its Applications* (Vol. 3982, pp. 406–415). Berlin: Springer-Verlag. doi:10.1007/11751595_44
- Wu, H.-T., & Cheung, Y.-M. (2006). A high-capacity data hiding method for polygonal meshes. In *Proc. of the International Workshop on Information Hiding* (pp. 188-200).
- Wu, M. Y., & Lee, J. H. (1998, December). A Novel Data Embedding Method for Two-Color Facsimile Images. In *Proc. International Symposium on Multimedia Information Processing*, Taiwan, R.O.C.
- Wu, M., & Liu, B. (2003). Data hiding in image and video: part I – fundamental issues and solutions. *IEEE Transactions on Image Processing*, 12(6), 685–695. doi:10.1109/TIP.2003.810588
- Wu, M., & Liu, B. (2003). *Multimedia Data Hiding*. New York: Springer-Verlag.
- Wu, M., & Liu, B. (2004, August). Data Hiding in Binary Image for Authentication and Annotation. *IEEE Transactions on Multimedia*, 6(4), 528–538. doi:10.1109/TMM.2004.830814
- Wu, M., Trappe, W., Wang, Z., & Liu, K. (2004). Collusion-resistant fingerprinting for multimedia. *IEEE Signal Processing Magazine*, 21(2), 15–27. doi:10.1109/MSP.2004.1276103

Compilation of References

- Wu, Y. (2005). On the Security of an SVD-Based Ownership Watermarking. *IEEE Transactions on Multimedia*, 7(4), 624–627. doi:10.1109/TMM.2005.846774
- Wu, Y., & Shimamoto, S. (2006). A Study on DWT-Based Digital Audio Watermarking for Mobile Ad Hoc Networks. In *Proceedings of the International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*.
- Wu, Y., Guan, X., Kankanhalli, M. S., & Huang, Z. (2001). Robust invisible watermarking of volume data using the 3D DCT. In *Proceedings of Computer Graphics International* (pp. 359–362). CGI.
- Xenos, M., Hantzara, K., Mitsou, E., & Kostopoulos, I. (2005). A model for the assessment of watermark quality with regard to fidelity. *Journal of Visual Communication and Image Representation*, 16(6), 621–642. doi:10.1016/j.jvcir.2005.03.006
- Xia, X.-G., Boncelet, C. G., & Arce, G. R. (1998). Wavelet transform based watermark for digital images. *Optics Express*, 3(12), 497–511. doi:10.1364/OE.3.000497
- Xiao, L., Wei, Z., & Ye, J. (2008). Comments on “Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition” and theoretical analysis. *Journal of Electronic Imaging*, 17(4), 1–3. doi:10.1117/1.3041170
- Xiao-Ping, Z., & Kan, L. (2005). Comments on „An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*, 7(2), 593–594. doi:10.1109/TMM.2005.843357
- Xie, R., Wu, K., Du, J., & Li, C. (2007). Survey of Public Key Digital Watermarking Systems. *Proceedings of the International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, (pp. 439 - 443).
- Xin, Y., Liao, S., & Pawlak, M. (2004). *A multibit geometrically robust image watermark based on Zernike moments*. Paper presented at the meeting of International Conference on Pattern Recognition, Cambridge, UK.
- Xin, Y., Liao, S., & Pawlak, M. (2004). *Geometrically robust image watermarking via pseudo-Zernike moments*. Paper presented at the IEEE Canadian Conference on Electrical and Computer Engineering, Ontario, Canada.
- Xing, Y., & Tan, J. (2007). A Color Watermarking Scheme Based on Block-SVD and Arnold Transformation. In *Proceedings of the Second Workshop on Digital Media and its Application in Museum and Heritage* (pp. 3–8).
- Xu, C., Wu, J., Sun, Q., & Xin, K. (1999). Applications of watermarking technology in audio signals. *Journal of the Audio Engineering Society. Audio Engineering Society*, 47(10).
- Yang, J.-F., & Lu, C.-H. (1995). Combined Techniques of Singular Value Decomposition and Vector Quantization for Image Coding. *IEEE Transactions on Image Processing*, 4(8), 1141–1146. doi:10.1109/83.403419
- Yap, P.-T., Paramesran, R., & Ong, S. H. (2003). Image Analysis by Krawtchouk Moments. *IEEE Transactions on Image Processing*, 12(11), 1367–1377. doi:10.1109/TIP.2003.818019
- Yap, P.-T., Paramesran, R., & Ong, S. H. (2007). Image Analysis Using Hahn Moments. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(11), 2057–2062. doi:10.1109/TPAMI.2007.70709
- Yaqin, Z., Zhilu, W., Guanghui, R., & Xuemai, G. (2002). A New Approach of 2D Discrete Cosine Transform with Möbius Inverse Formula. *Proceedings of the 6th International Conference on Signal Processing*, 1, 162 - 165.
- Yavuz, E., & Telatar, Z. (2006). SVD Adapted DCT Domain DC Sub-band Image Watermarking Against Watermark Ambiguity. In Gunsel, B. (Eds.), *Multi-media Content Representation, Classification and Security* (Vol. 4105, pp. 66–73). Berlin: Springer-Verlag. doi:10.1007/11848035_11
- Yavuz, E., & Telatar, Z. (2007). SVD Adapted DCT Domain DC Sub-band Image Watermarking Against Watermark Ambiguity. In Y. Cho et al. (Eds.), *Proceedings of the 2007 ACM symposium on Applied computing: Vol. 4105* (pp. 1051-1055). New York: ACM Press.

- Yeh, C. H., & Kuo, C. J. (1999). Digital watermarking through quasi m-arrays. In *Proceedings of the IEEE Workshop on Signal Processing Systems*, (pp. 456–461).
- Yeo, B., & Yeung, M. M. (1999). Watermarking 3D objects for verification. *IEEE Computer Graphics and Applications*, 19(1), 36–45. doi:10.1109/38.736467
- Yeo, I. K., & Kim, H. J. (2003). Modified patchwork algorithm: A novel audio watermarking scheme. *IEEE Transactions on Speech and Audio Processing*, 11(4), 381–386. doi:10.1109/TSA.2003.812145
- Yeo, I. K., & Kim, H. J. (2003). Modified patchwork algorithm: A novel audio watermarking scheme. *IEEE Transactions on Speech and Audio Processing*, 11(4), 381–386. doi:10.1109/TSA.2003.812145
- Yu, D., Sattar, F., & Ma, K. K. (2002). Watermark detection and extraction using independent component analysis method. *EURASIP Journal on Applied Signal Processing*, 1, 92–104. doi:10.1155/S111086570200046X
- Yu, P., Tsai, H., & Lin, J. (2001). Digital watermarking based on neural networks for color images. *Signal Processing*, 81(3), 663–671. doi:10.1016/S0165-1684(00)00239-5
- Yudell, L. L. (1975). *Mathematical functions and approximations*. New York: Academic Press Inc.
- Zafeiriou, S., Tefas, A., & Pitas, I. (2005). Blind robust watermarking schemes for copyright protection of 3D mesh objects. *Visualization and Computer Graphics. IEEE Transactions on*, 11(5), 596–607.
- Zaharia, T., & Prêteux, F. (2004). Descripteurs visuels dans le standard MPEG-7. In Mostefaoui, A., Prêteux, F., Lecuire, V., & Moureaux, J.-M. (Eds.), *Gestion des données multimédias* (pp. 225–282). Lavoisier.
- Zaharia, T., Preda, M., & Prêteux, F. (2006). Interactivity, reactivity and programmability: advanced MPEG-4 multimedia applications. *IEEE International Conference on Consumer Electronics*, Las Vegas, NV (pp. 441–442).
- Zaidi, A., & Vandendorpe, L. (2009). Coding schemes for relay-assisted information embedding. *IEEE Transactions on Information Security and Forensics*, 4(1), 70–85. doi:10.1109/TIFS.2008.2009588
- Zaidi, A., Piantanida, J. P., & Duhamel, P. (2007). Broadcast- and MAC-aware coding strategies for multiple user information embedding. *IEEE Transactions on Signal Processing*, 55, 2974–2992. doi:10.1109/TSP.2007.893973
- Zamir, R., Shamai (Shitz), S., & Erez, U. (2002). Nested linear/lattice codes for structured multi-terminal binning. *IEEE Transactions on Information Theory*, 48, 1250–1276. doi:10.1109/TIT.2002.1003821
- Zeng, W. (2006). *Multimedia security technologies for digital rights management*, Academic press. Elsevier.
- Zhang, F., Pan, Z., Cao, K., Zheng, F., & Wu, F. (2008). The upper and lower bounds of the information-hiding capacity of digital images. *Information Sciences*, 178, 2950–2959. doi:10.1016/j.ins.2008.03.011
- Zhang, H., van Kaick, O., & Dyer, R. (2007). Spectral Methods for Mesh Processing and Analysis. In Proc. of the Eurographics State-of-the-art Report (pp. 1-22).
- Zhang, J., Kou, W., & Fan, K. (2006). Secure buyer-seller watermarking protocol. *IEE Proceedings Information Security*, 153(1), 15–18. doi:10.1049/ip-ifs:20055069
- Zhang, R., Yu, X., Zhou, L., & Li, H. (2006). A new watermarking protocol of copyright protection. In Intelligent Information Hiding and Multimedia Signal Processing - IIH-MSP '06. (pp. 83-88). Washington, DC: IEEE Computer Soc.
- Zhang, W., Zeng, Z., Pu, G., & Zhu, H. (2006). Chinese Text Watermarking Based on Occlusive Components. In 2nd IEEE Information and Communication Technologies, ICTTA '06, 1, (pp. 1850-1854).
- Zhang, X., & Wandell, B. (1996). A spatial extension of cielab for digital color image reproduction. *Journal of the Society for Information Display*, 5(1), 61–63. doi:10.1889/1.1985127
- Zhang, X., & Wang, S. (2009). Fragile watermarking scheme using a hierarchical mechanism. *Signal Processing*, 89(4), 675–679. doi:10.1016/j.sigpro.2008.10.001

Compilation of References

- Zhang, X.-P., & Li, K. (2005). Comments on “An SVD-Based watermarking scheme for protecting rightful Ownership”. *IEEE Transactions on Multimedia*, 7(3), 593–594. doi:10.1109/TMM.2005.843357
- Zhang, F., Panb, Z., Caoa, K., Zhenga, F., & Wu, F. (2008). The upper and lower bounds of the information-hiding capacity of digital images. *Information Sciences*, 178(14), 2950–2959. doi:10.1016/j.ins.2008.03.011
- Zhao, B., Dang, L., Kou, W., Zhang, J., & Cao, X. (2007). Design of secure watermarking scheme for watermarking protocol. Advances in multimedia information processing - PCM 2007, (LNCS Vol. 4810, pp. 357-366). Berlin: Springer-Verlag.
- Zhao, J., Koch, E., & Luo, C. (1998, July). In business Today and Tomorrow. *ACM Communication*, 41(7), 66–72.
- Zhao, Y., Campisi, P., & Kundur, D. (2004). Dual domain watermarking for authentication and compression of cultural heritage images. *Image Processing. IEEE Transactions on*, 13(3), 430–448.
- Zheng, D., & Zhao, J. (2007). A rotation invariant feature and image normalization based image watermarking algorithm. Paper presented at the IEEE International Conference on Multimedia and Expo, Beijing, China.
- Zheng, D., Liu, Y., Zhao, J., & El-Saddik, A. (2007). A survey of RST invariant image watermarking algorithms. [CSUR]. *ACM Computing Surveys*, 39(2). doi:10.1145/1242471.1242473
- Zhou, B., & Chen, J. (2004). A geometric distortion resilient image watermarking algorithm based on SVD. *Chinese Journal of Image and Graphics*, 9(4), 506–512.
- Zhou, J., Shu, H., Zhu, H., Toumoulin, C., & Luo, L. (2005). Image analysis by discrete orthogonal Hahn moments. In M. Kamel & A. Campilho (Eds.), *Second International Conference on Image Analysis and Recognition, Toronto, Canada*, (Vol. 3656: Image Analysis and Recognition, pp. 524-531). Berlin: Springer.
- Zhu, H., Shu, H., Liang, J., Luo, L., & Coatrieux, J.-L. (2007). Image analysis by discrete orthogonal Racah moments. *Signal Processing*, 8, 687–708. doi:10.1016/j.sigpro.2006.07.007
- Zhu, S., & Liu, J. (2009). A Novel Adaptive Watermarking Scheme Based on Human Visual System and Particle Swarm Optimization. In Bao, F., Li, H., & Wang, G. (Eds.), *Information Security Practice and Experience* (Vol. 5451, pp. 136–146). Berlin: Springer-Verlag. doi:10.1007/978-3-642-00843-6_13
- Zhu, W., Xiong, Z., & Zhang, Y.-Q. (1999). Multiresolution watermarking for images and video. *IEEE Trans. Circuits and Systems for Video Technology*, 9(4), 545–550. doi:10.1109/76.767121
- Zude, Z., Qingsong, A., & Quan, L. (2006). A SVD-based Digital Watermarking Algorithm for 3D Mesh Models. In *Proceedings of the 8th International Conference on Signal Processing: Vol. 4* (pp. 16-18).
- Zwicker, E., & Fastl, H. (1999). *Psychoacoustics: Facts and models*. Berlin: Springer-Verlag.

About the Contributors

Ali Al-Haj received his first university degree in Electrical Engineering from Yarmouk University, Jordan, in 1985. He then pursued his higher studies in Japan, and received the M.Sc degree in Electronics Engineering from Tottori University in 1988 , and the Ph.D degree in Computer Engineering from Osaka University in 1993. He then worked as a research associate at ATR Advanced Telecommunications Research Laboratories in Kyoto, Japan, until 1995. He joined Princess Sumaya University, Jordan, in October 1995, where he is now an associate professor. Al-Haj has published numerous papers in areas such as parallel processing, dataflow computing, parallel information retrieval, VLSI digital signal processing, neural networks, and multimedia watermarking.

* * *

Marina Aguado received her B.Sc. degree as telecommunication engineer from ETSI Bilbao, Spain in 1992 and her M.Sc. from Cranfield University, England in 1993. In 1993, she worked as a trainee in the Ford Motor Company, United Kingdom. From 1994–2003, she worked at the traffic control center in several railway companies in Brazil, first as network support analyst, and finally as an R&D manager responsible for IT projects on railway operation. Nowadays she works as an assistant lecturer in the Faculty of Engineering of Bilbao, in the University of the Basque Country (UPV/EHU). She also works as a researcher in the I2T (Investigacion e Ingenieria Telematica: Research and Engineering in Telematics, <http://i2t.ehu.es>), a Group for Research in Telematics in the same University. Her current research interests are broadband wireless access technologies and handover, protocols and security related issues in communication networks.

Shiraz Ahmad's education includes M.Sc. Physics (1998) from Islamia University, Bahawalpur, Pakistan, M.Sc. Systems Engineering (2001) from Quaid-i-Azam University, Islamabad, Pakistan, and Ph.D. Information and Signal Processing from Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, P. R. China. From 1999 to 2001 he was a research fellow at Pakistan Institute of Engineering and Applied Sciences, Nilore, Pakistan. Since October 2001 he is with Pakistan Atomic Energy Commission (PAEC), Islamabad, Pakistan, and currently holds the position of Senior Scientist since December 2003. For his distinctive achievements, during the academic and professional careers, he has been the recipient of a Silver Medal, PAEC's Fellowship Award (1999-2001), the Youngest Excellent Professional Honour for four consecutive years (2001 to 2004), Fifty Excellent Talent Support award in Basics Sciences (2006-2010), and several other competitive certificates, grants and awards. His interest domains include multimedia analysis and processing and with specific research interests in data and information hiding/security, watermarking, biometrics, and image and video inpainting.

About the Contributors

Tahani Al-Khatib received her BSc and MSc degrees in Computer Science from the University of Jordan in 2002, and 2005, respectively. Ms. Al-Khatib has been an instructor at the department of Computer Information Systems, the University of Jordan, since 2006. Her research interests include image processing and information security.

Atilla Baskurt received the B.S. degree in 1984, the M.S. degree in 1985 and the Ph.D. degree in 1989, all in Electrical Engineering from INSA of Lyon, Lyon, France. From 1989 to 1998, he was “Maître de Conférences” at INSA of Lyon. Since 1998, he is Professor in Electrical and Computer Engineering, first at Université Claude Bernard Lyon 1, Lyon, France, and now at INSA of Lyon. Between 2003 and March 2008, he was Director of the Telecommunication Department of INSA of Lyon. During 2008, he was Deputy Director of the research center LIRIS. Between September 2006 and December 2008, he was “Chargé de Mission” on Information and Communication Technologies at the French Research Ministry. Currently, he is Director of LIRIS. Pr. A. Baskurt leads his research activities in two teams of LIRIS: the IMAGINE team and the M2DisCo team. These teams work on image and 3-D data analysis and segmentation for image compression, image retrieval, shape detection and identification. His technical research and experience include digital image processing, 2-D/3-D data analysis, compression, retrieval and watermarking, especially for multimedia applications.

Alessandro Basso is a postdoctoral researcher at the Computer Science Department, Università degli Studi di Torino, Italy, where he received his MSC and PhD in Computer Science. His research interests mainly focus in the Computer and Network security area, spanning between Digital Watermarking of multimedia content, Web application security and Mobile device security. Recently, he turned his attention towards the field of Distributed Applications for Complex Networks, being involved in the study of information processing and filtering, social networks and recommender systems.

Dumitru D. Burdescu graduated in Automatics and Computers specialty at Faculty of Electro-technics, University of Craiova in 1974 and Mathematics specialty at Faculty of Sciences, University of Craiova in 1980 and got his Ph.D. degree in 1990. He became a senior member of IEEE in 2007. He is currently professor at Software Engineering Department, Faculty of Automatics, Computers and Electronics, University of Craiova, Romania. Since 2000 he is director to Research Center “Multimedia Applications Development”. He is the author and coauthor of more than 120 scientific papers presented to conferences or published in different journals, 10 books in the computers area, chair or co-chair and member in the program committees of international conferences, member in the editorial board of international magazines. He was director of 11 research grants. His research activity was focused on areas like: algorithms theory, multimedia and visual information retrieval. More information may be found on personal web page at: <http://software.ucv.ro/~dburdescu/>

Davide Cavagnino is currently a researcher at the Università degli Studi di Torino, Italy. He received the laurea degree in Computer Science in 1992 and the Ph.D. in Computer Science in 1998. He worked in the fields of image processing and compression, pattern recognition, computer and network security, and is currently merging this knowledge in the field of digital image watermarking.

Gaël Chareyron was born in Valence, France. He received his Ph.D. degree in computer science and vision from University Jean Monnet in Saint-Etienne, France in 2005. Previously, he completed his

B.S and M.S degrees in computer science from University Louis Pasteur, Strasbourg, France in 1999 and from University Jean Monnet, Saint-Etienne, France in 2001, respectively. In 2003, he was with the University of Louvain La Neuve, Belgium as a research associate. From 2005 to 2006, he was with the University of Saint-Etienne as an assistant professor. Since 2006, he is a professor in computer science at the University Leonard de Vinci, Paris la défense, France. His research topics include multimedia and security, computer vision, color image and image quality evaluation.

Nedeljko Cvejic received the Dipl.-Ing. degree in electrical engineering from the University of Belgrade, Serbia, in 2000 and the Dr. Tech. degree from the University of Oulu, Finland, in 2004. From 2001 to 2004, he was a Research Scientist with MediaTeam Research Group, Department of Electrical and Information Engineering, University of Oulu, Finland. From 2005 until 2008 he was a Research Associate with the Department of Electrical and Electronic Engineering of the University of Bristol, United Kingdom. He is currently a Research Associate with the Department of Engineering, University of Cambridge.

Jérôme DaRugna was born in Lyon, France. He received his B.S and M.S degrees in computer science from Ecole Normale Supérieure, Lyon, France in 1997 and from University Jean Monnet, Saint-Etienne, France in 1999, respectively. He received his Ph.D. degree in computer science and vision from University Jean Monnet, Saint-Etienne, France in 2004. He was a Professor in the Department of Vision and Computer Engineering at the University Jean Monnet from 2005 to 2008 prior to joining the computer science department at the University Leonard de Vinci in Paris la défense, France. His research interests include image, video and graphics understanding, video enhancement, multimedia security, and computer vision.

Claude Delpha graduated in Electronics and Signal Processing Engineering. He obtained his PhD in Laboratory of Interfaces, Components and Microelectronics in the University of Metz in the field of Electronics, gas sensing signal processing and pattern recognition analysis (Electronic noses). Since 2001, he is a professor assistant in the Université Paris Sud 11 (IUT of Cachan). He also works in the Laboratory of Signals and Systems (L2S – CNRS- SUPELEC – Univ Paris-Sud 11) for research activities in the field of signal processing for multimedia applications and smart systems. His main areas of interests are Multimedia Data hiding, Digital Watermarking, Steganography and Multimedia Security Diffusion, Pattern Recognition, Multimedia.

Florence Denis received the B.S. degree in 1985, the M.S. degree in 1985, and the Ph.D. degree in 1990, all in Electrical Engineering from INSA of Lyon, Lyon, France. She is currently an Associate Professor at Université Claude Bernard Lyon 1, Lyon, France. She is also a member of the M2DisCo team of the LIRIS laboratory. Her research interests are in the fields of 2-D and 3-D image processing, segmentation, and watermarking.

Dejan Dražić was born in Belgrade, Yugoslavia in 1970. He received the B.Sc., M.Sc. and Ph.D. degrees from Faculty of Electrical Engineering, University of Belgrade, Belgrade, Serbia in 1995, 1999 and 2004. From 1995 to 1999 he worked as a Research Scientist at the Faculty of Electrical Engineering, Belgrade. In 2000, he joined the Centre for Wireless Communications, University of Oulu, Oulu, Finland where he worked as a Research Scientist on project concerning development of advanced receivers for

About the Contributors

WCDMA. In 2002, he joined Ericsson d.o.o., Belgrade, Serbia and Montenegro, where he is currently working as a Solution Manager for Core and IMS area. His main research interests include adaptive equalization, signal processing, audio watermarking, turbo coding and their implementation in future wireless communication systems design.

Samir Abou El-Seoud received the BSc degree in physics, electronics, and mathematics in 1967, his higher diploma in computing from the Technical University of Darmstadt (TUD), Germany, in 1975, and his doctor of science from TUD in 1979. El-Seoud held various academic positions at TUD Germany and abroad, the latest being full-professor in 1987. His main research is focused on numerical parallel algorithms, scientific computation, and computational fluid mechanics. Currently, he is interested in e-learning and computer aided learning. El-Seoud joined Princess Sumaya University, Jordan, in 2004.

Mohammad Eyadat is a Professor of Computer Information Systems at California State University, Dominguez Hills, California, USA. He received the Ph.D. in Computer Science/Engineering Mathematics from Claremont Graduate School in Claremont, Master of Science Degree in Computer Science from the University of Southern California, and Bachelor of Science Degree in Computer Science from Yarmouk University - Jordan. He has been serving as professor at different institutions international and domestic. The institutions where he has taught courses in Computer Science, Computer Information Systems, Information Technology, and Mathematics provide graduate and undergraduate degree. His working experience ranges from Software Designer and developer to Business Consultant. As a researcher, he has been a collaborator for organizing several research activities including professional research conferences. He is active member of the professional community, and a member of several professional organizations. His research interests include watermarking algorithms for images and video data, multimedia software security, software engineering, Education and Information Technology, and Web accessibility.

Mariví Higuero obtained her BS and MS degrees in Electrical Engineering, in the University of the Basque Country (Spain), and Ph.D. degree in the same University in 2005. She worked in Sarenet, an Internet Service Provider company, as a technical department member, acquiring experience with operation and management of telecommunication networks and services. Nowadays she works as assistant professor in the Department of Electronics and Telecommunications at Faculty of Engineering of Bilbao in the University of the Basque Country, teaching Telematics Laboratoy, Telematics Fundamentals, and Doctorate Courses on Advanced Networks and Services, and Security in Wireless Networks. She is also member of the I2T (Research and Engineering in Telematics, <http://i2t.ehu.es>) Research Group in the same University, doing research in Telematics issues such as Computer Networks, Protocols and Services, Mobility and Security.

Fayez M. Idris is an Assistant Professor of Computer Engineering and the Director of the Information Systems and Technology Center at the German-Jordanian University, Jordan. He receiveed his PhD and MSc in Electrical and Computer Engineering from the University of Ottawa, Canada in 2000 and 1993, respectively. From July 2000 to August 2006, he was an Assistant Professor of Computer Engineering at the Jordan University of Science and Technology (JUST). From September 2003 to August 2005 he was the Chair of the Department of Computer Engineering at JUST. Before joining JUST he was a Senior Research and Development Engineer at Callisto Media Systems, Hull, Quebec, Canada. Dr. Idris

participated in externally funded projects from King Abdullah II Fund for Development, TEMPUS, and EUMEDIS. His research interests include computer architecture, software/hardware co-design, e-learning, and image processing.

Guillaume Lavoué received the Engineer degree in Electronic, Telecommunications and Computer Science from CPE-Lyon, Lyon, France, in 2002, the M.S. degree in Image Processing from Université Jean Monnet de St. Etienne, St. Etienne, France, in 2002, and the Ph.D. degree in Computer Science from Université Claude Bernard Lyon 1, Lyon, France, in 2005. From February to April 2006, he was a Postdoctoral Fellow at the Signal Processing Institute, Lausanne, Switzerland. He is currently an Associate Professor of Computer Science at INSA of Lyon, Lyon, France. His research interests include 3-D mesh analysis, 3-D watermarking and compression, perception for computer graphics, and object recognition and detection.

David Lowe has a background and PhD in theoretical physics, and worked in the UK Defence sector before moving into academia, joining Aston University in 1993 to a Chair in Neural Networks. He has worked in problems of brain state characterisation from EEG and MEG signals, modelling visualisation of temporal sequences of DNA microarrays, financial data analysis, information hiding in digital media, and emergent behaviour in nonlinear coupled MEMS sensor arrays. He is currently investigating Complexity as a guiding principle in a new design philosophy of novel sensor arrays, especially in coupled nonlinear oscillators in microelectromechanical systems (MEMS). He is perhaps best known for being the co-inventor of the Radial Basis Function neural network - one of the most popular artificial neural network architectures in use worldwide, and co-inventor of the NeuroScale architecture for high dimensional topographic data visualisation. He has consulted for various large and small commercial companies in Defence, Finance, Automotive, Biomedical and Paper manufacturing industries. He has been an International Reviewer for the Australian DSTO programme in Data Fusion, and has served on several UK national panels on topics such as "The Future of Computing", "Data Fusion" and academic review panels and is on the Advisory Board of the Leverhulme Trust.. He has been a member of the committees of several international conferences at the interface of mathematics, computing, engineering and the medical life sciences.

Zhe-Ming Lu received the B.S., M.E. and Ph.D. degrees from the Harbin Institute of Technology, Harbin, P. R. China, in 1995, 1997 and 2001, respectively. Currently he is the Professor of the School of Aeronautics and Astronautics, Zhejiang University, Hangzhou, China. His current scientific interests cover digital watermarking, image and video compression, visual information retrieval, information security and image analysis. He has authored and co-authored over 190 articles in journals and conferences. Dr. Lu has served as the Editor-in-chief of the International Journal of Information Analysis and Processing, as the Executive Editor of the International Journal of Computer Sciences and Engineering Systems, and as an Associate Editor for the International Journal of Innovative Computing, Information and Control, and the Journal of Information Hiding and Multimedia Signal Processing.

Santi P. Maity received his B.E. in Electronics and Communication Engineering and M.Tech degree in Microwaves, both from the University of Burdwan, India in 1993 and 1997, respectively. He received his Ph.D. degree in Engineering (Computer Science and Technology) from Bengal Engineering and Science University, Shibpur, India in 2008. During January ,2009 to July, 2009 he did pos-doctoral work

About the Contributors

concerning watermarking in lured applications in the “Laboratoire des Signaux et Systems (CNRS-Supelec-Universite Paris-Sud 11)” in France. He is at present working as Assistant Professor at the Department of Information Technology, Bengal Engineering and Science University, Shibpur since September, 2006. He also worked as Lecturer in Electronics and Telecommunication Engineering department of the same university from 2000 to 2006. Prior to that, he worked as Lecturer in Electronics and Telecommunication Engineering Department of K.G. Engineering Institute, Bishnupur, Bankura, India and Haldia Institute of Technology, Haldia, India, from 1997 to 2000. His research areas include digital image watermarking, multiuser detection in CDMA, digital signal processing, digital wireless communication, VLSI watermarking. He delivers several lectures and invited talk on short term course/seminar/workshop/conference and acts as committee member for national and international conferences like ICVGIP-2004, IMSA 2008, IMSA2009 and IMSA 2010. He is an Associate Member of Institute of Engineer (India) and a Member of Institute of Electronics and Telecommunication Engineers (IETE), India. He is principal investigator of a project “High Power and Spectral Efficiency Multiuser System for Broadband Wireless Communication” sponsored by Department of Information Technology, Ministry of Communication and Information Technology, Govt. of India. He has contributed about 70 research papers in well-known and prestigious archival journals, international refereed conferences and as chapters in edited volumes.

Tuqa Manasrah received her first university degree in Computer Engineering from Yarmouk University, Jordan, in 2000, and the M.Sc degree in Computer Engineering from Jordan University for Science and Technology in 2005. She worked as a computer engineer and lab instructor at several IT enterprises and universities since Jordan. Ms. Manasrah has been a lecturer at the department of Computer Engineering, the University of Jordan, since 2006. Her research interests include medical imaging, information retrieval and digital multimedia watermarking.

B.R.Matam has received a M.Tech from Mangalore University, India in Digital Electronics and Advanced Communication in 1999. She has worked as a lecturer in one of the leading colleges in Karnataka, India before joining Aston University in 2005 to study towards a PhD. She has recently completed her PhD in Watermarking Biomedical Data under the supervision of Professor David Lowe.

Cristian M. Mihăescu is lecturer at the Software Engineering Department, Faculty of Automation, Computers and Electronics, University of Craiova, Romania. He graduated Computer Science English teaching, Faculty of Automatics, Computers and Electronics, University of Craiova, Romania and got his PhD degree in computer science from University of Craiova in 2007. He is the author or co-author of 1 book and more than 30 conference and journal papers. He also served as program committee member for some important conferences. Current research interests include e-Learning, machine learning, data mining, software engineering and multimedia. The research activity carried on 4 research grants. As a member of the Research Center “Multimedia Applications Development” he coordinates the “e-Learning Applications Development” research group, with a number of practical achievements regarding e-Learning enhancement. More information may be found on personal web page at: <http://software.ucv.ro/~cmihaescu/>

Ahmad Mohammad received his BSc in Electrical Engineering from Ein-Shams University in Egypt in 1986, and the MSc, and PhD degrees in Electrical Engineering, from Akron University, USA, in 1989, and 1992, respectively. Dr. Mohammad has been an assistant professor at the department of

Computer Engineering, Princess Sumaya University, Jordan, since 2000. His research interests include control systems, image processing, and information security.

Hedley Morris received his Sc.D. (1986), from Trinity College Dublin, Ireland, his Ph.D. in Theoretical Physics (1971) from the University of London, England and his B.Sc. in Mathematics (1968) from the University of London, England. An internationally known researcher in the area of nonlinear wave theory, Professor Morris is a member of IEEE, co-author of a major textbook and the editor of several other publications. He is currently Professor of Mathematics and Financial Engineering at Claremont Graduate University.

Imad Muhi received his Ph.D. in Engineering Mathematics from Claremont Graduate School in Claremont and Master of Science Degree in Mathematics from Germany. His main research interest watermarking algorithms for images and video data, He is active participant in professional activities. He is currently Professor of Mathematics in New York Institute of Technology, Amman, Jordan

Victor Pomponiu is a Ph.D. student and member of the Security and Network group at the Computer Science Department, Università degli Studi di Torino, Italy, since January 2009. He received his B.Sc. and M.Sc. in Computer Science from the Polytechnic University of Bucharest in 2006 and 2008 specializing in communication systems. His areas of research include digital image/signal processing and information security, in particular cryptography, steganography and watermarking.

Tamer Rabie is an Associate Professor at the College of Information Technology United Arab Emirates University, UAE. He received his PhD in Computer Science from the University of Toronto, Canada. His research interests include digital image processing, computer vision, virtual reality, and their application to the field of intelligent transportation systems. He is senior member in the IEEE and member of the Professional Engineers of Ontario (PEO) Association in Toronto, Canada.

Lama Rajab received her BSc and MSc degrees in Computer Science from the University of Jordan in 2002, and 2005, respectively. Ms. Rajab has been an instructor at the department of Computer Information Systems, the University of Jordan, since 2006. Her research interests include image processing and information security.

Mehul S Raval (Member, IEEE) received the Bachelor of Engineering degree in 1996, Master of Engineering in 2002 and PhD degree from University of Pune, India, in 2008. All the degrees were obtained in Electronics and Telecommunication Engineering. He joined Sarvajanik College of Engineering and Technology, Surat, India as Lecturer in 1997. Currently he is serving as Assistant Professor at Dhirubhai Ambani Institute of Information and Communication Technology. His research interests lie in the area of Digital data hiding, Steganography, and security aspects of digital data hiding. He is reviewer for many international and national journals and conferences. He has research publications in peer reviewed journals and conferences.

Puri Saiz obtained her BS and MS degrees in Telecommunication Engineering from the University of the Basque Country (UPV/EHU), Spain, in 1996; and her Ph.D. degree in 2007, from the same Uni-

About the Contributors

versity. After 6 years of professional experience in operation and engineering of GSM/GPRS/UMTS mobile networks, she works since 2002 as a lecturer in the Electronics and Telecommunications Department at the Faculty of Engineering of Bilbao, in the UPV/EHU. There she teaches Telecommunication Services and Networks, Mobile Services and Networks, and Switching Techniques. She also works as a researcher in the I2T (Investigación e Ingeniería Telemática), a Group for Research in Telematics in the same University. Her research interests include Security, Mobility, Wireless Networks and Computer Networks. In her PhD, she proposed a new security framework and protocol for the establishment of peer-to-peer secure sessions.

Liana Stănescu is professor at the Software Engineering Department, Faculty of Automation, Computers and Electronics, University of Craiova, Romania. She received a PhD in computer science from University of Craiova in 2002. She is the author or co-author of 10 books and more than 90 conference and journal papers. Her fields of scientific interest are: multimedia databases, content-based visual retrieval, multimedia e-learning and topic maps. She also served as program committee member and organizer for some important conferences. The research activity carried on more than 10 research grants was directly focused on image databases and content-based visual retrieval. As a member of the Research Center “Multimedia Applications Development” she coordinates the “Multimedia Applications in Medicine” research group, with a number of practical achievements in the medical e-learning and diagnostic aid. More information may be found on personal web page at: <http://software.ucv.ro/~lstanescu/>

Alain Tréneau is professor, in Color Imaging at the Université Jean Monnet, Saint-Etienne, France. Alain Tréneau is member of the Laboratoire Hubert Curien, UMR 5516, a research laboratory working in Photonics and Optics, and in Computer Vision and Color Imaging Science. He is currently mainly focused on mathematical imaging and color science with reference to human vision and perception. He works also in color metric with regard to color appearance and rendering measurements. He has written numerous papers or book chapters on Computational Colour Imaging and Processing. He is the coordinator of the ERASMUS MUNDUS master CIMET devoted to Color in Informatics and Media Technology.

Annamaria Verone is currently a technician at the Department of Genetics Biology and Biochemistry, Università degli Studi di Torino, Italy. She received the laurea degree in Computer Science in 1991. Her areas of research include signal processing, digital image and video watermarking and bioinformatics (protein analysis in biomedical field).

Kai Wang received the B.E. degree in Telecommunication Engineering and the M.E. degree in Pattern Recognition and Intelligent System, both from Xi'an Jiaotong University, Xi'an, China, in 2003 and 2006 respectively, and the Generalist Engineer degree from Ecole Centrale de Lyon, Lyon, France, in 2006. He is currently pursuing the Ph.D. degree at INSA of Lyon, Lyon, France, within the M2DisCo team of the LIRIS laboratory. His research interests include multimedia signal processing, digital watermarking and geometric modeling.

Index

A

Acrobat Reader 160, 171
adaptation 111
additive white Gaussian noise (AWGN) channel 327, 343
affine transformation 104, 107
agent-based restrictions 161
algorithms, anti-collusion properties of 129
ambiguity problem 288
analog to digital (A/D) conversions 147, 325
anonymity 348, 358
application specific integrated circuit (ASIC) 455, 457, 458, 480, 481, 482
appropriate watermarks, insertion of 349
artificial neural networks (ANN) 370, 383, 406
asymmetric fingerprinting 364, 366
asymmetric fingerprinting protocols 350
asymmetry 348
audio compression 131, 133, 147, 151
audio signal distortion 147
audio signals 147
audio signals, copyright protection of 144
audio watermarking 127, 128, 129, 130, 131, 132, 134, 136, 139, 140, 141, 142, 143, 147
audio watermarking algorithms 127, 128, 130, 131, 132, 134, 136, 143
audio watermarking algorithms, attacks against 132
audio watermarking, attacks against 127, 128, 129, 130, 132, 133, 134, 136, 137, 139, 142, 143
audio watermarking magic triangle 127, 130, 132

audio watermarking magic triangle, perceptual transparency 130
audio watermarking magic triangle, watermark bit rate 131
audio watermarking magic triangle, watermark robustness 130
audio watermarking systems 128
authentication 255, 260, 270, 271, 272, 279, 280, 281, 284, 285, 286, 407, 408, 415, 422, 423, 424, 425, 426, 427, 428, 437, 438, 448, 449, 451, 452, 453
authentication information 2

B

backward compatibility 111, 112
Binary Symmetric Channel (BSC) 410, 413
biorthogonal wavelet based Hilbert transform 455, 457, 462
bit commitment schemes 351
bit-error probability (BER) 131
bit error ratio (BER) 408, 410, 413, 414, 415, 416
bits per second (bps) 131, 132, 133, 136, 137, 139
Blahut-Arimoto algorithm 115, 126
Blahut-Arimoto algorithm, discrete 115
blind detection 128
blind mesh watermarking techniques 200, 203
blind source 62, 109
blind watermarking 326
blind watermarking algorithms 427
blind watermarking detection 410
blind watermarking schemes 203
Bose Chaudhuri and Hocquenghem (BCH) codes 410, 411, 412, 413, 414

bounding box scale-invariant feature transform 57
broadcast channels (BC) 329, 330, 331, 334, 335
broadcast monitoring 129, 131, 142, 255, 427, 428, 429, 449, 452
bus encryption 160
business models 366
business models, feasible 348

C

capacity 370, 377, 378, 381, 382, 387, 388, 390, 395, 396, 397, 398, 399, 400, 402, 403, 405, 427, 428, 429, 448, 453
carrier signal 325
CeBIT (Centre of Office and Information technology) expo 112
channel coding 408, 421
chaotic dynamic systems 370
chrominance (color) 22, 23, 24, 25, 26, 27, 28, 29, 31
CIE (International Commission on Illumination) 23, 24, 38, 40, 50, 53, 56
CIE L*a*b* color space 23, 25, 38, 39, 40, 43, 45, 46, 50, 56
color appearance model (CAM) 49, 56
color channels 36, 48
color channels, individual 36
color images 36, 37, 42, 44, 49, 51, 52, 53, 54, 55
color image watermarking 36, 37, 50, 53, 54, 55
color opponent process 56
color palette 43, 44, 55, 56
combined domain 288
complex distributed systems 347
compressed audio stream 131
computer games 111
connectivity attacks 226
content access control 37
content authentication 424
content customisation 111
content origin identification 37
content-preserving operations 226
content scrambling system (CSS) 159
copy control 145, 428

copy control systems 366
copy protection 37
copyright infringement 369, 426
copyright messages 145, 152, 153, 154, 155, 156
copyright protection 21, 144, 145, 146, 147, 155, 158, 254, 255, 267, 268, 280, 286, 289, 319, 325, 344, 345, 347, 348, 361, 362, 365, 367, 407, 408, 411, 415, 417, 422, 424, 425, 426, 427, 428, 437, 448, 449
copyright protection, unauthorized usage avoidance 345, 346
copyright protection, unauthorized usage detection 344, 345, 346
copyrights 344, 346, 347, 349, 354, 359, 363, 366, 367
copyright violation 228, 324
cover signal 370, 379, 390, 391, 400, 405
cryptographic hash function 322
cryptography 2, 145, 159, 161, 255, 344, 347, 426, 455, 456, 458, 480
crypto-processors 160

D

darknet 407
data bus 160
data embedding 326
data hiding 21, 22, 23, 26, 31, 33, 325, 370, 383, 384, 390, 394, 399, 402, 403, 424
data hiding techniques 21, 144, 256, 257, 260, 261
data mining 111
data subsets 290, 316, 322
data tampering 289
decryption 426
deletion errors 411
DeltaE (CIE76) 39, 44, 45, 46, 50, 56
desynchronisation 128
detection process security 349
Difference of Gaussian (DOG) image pyramid technique 323
digital audio 243, 251, 252
digital audio watermarking 127, 141, 143, 243
digital authentication 1
digital content copyright protection 158

- digital content protection 426
 digital contents 345, 367
 digital contents distribution 347, 348, 361
 digital contents distribution protocol 367
 digital copying 1
 digital data, distribution of 324
 digital fingerprints 145
 digital hole 426
 digital images 1, 3, 11, 16, 17, 21, 32, 33, 232
 digital images, spatial authentication techniques for 1, 16
 digital image watermarking 232
 digital image watermarking techniques 57, 62, 90, 102
 digital media 58, 228, 229
 Digital Millennium Copyright Act (DMCA) (1998) 160, 161, 289
 digital multimedia 36, 55
 digital multimedia data 289
 digital multimedia signals 228
 digital piracy 345, 426
 digital rights management (DRM) 158, 159, 160, 161, 162, 166, 171, 172, 188, 193, 194, 195, 198, 199, 325, 344, 362, 363, 366, 407, 426
 digital seal 59
 digital signal processing (DSP) 127, 323, 456, 458, 459, 480
 digital signal processing (DSP), common operations of 229
 digital signatures 2, 59
 digital time series data transmission 144
 digital to analog (D/A) conversions 147, 325
 digital universe 58, 104
 digital video 236
 digital video watermarking 231, 236, 240
 digital watermarking algorithms 425, 426
 digital watermarking (DWM) 1, 2, 3, 5, 17, 18, 20, 59, 158, 161, 196, 197, 198, 200, 201, 202, 224, 228, 229, 254, 255, 256, 260, 261, 274, 280, 281, 282, 285, 369, 370, 371, 388, 394, 398, 399, 401, 402, 403, 404, 405, 425, 426, 448, 450
 digital watermarking for authentication 2, 17
 digital watermarking, fragile schemes 200
 digital watermarking, hardware implementation of 456
 digital watermarking, high-capacity schemes 200, 203
 digital watermarking, robust schemes 200, 222
 digital watermarking, spatial domain 1, 2, 3, 4, 5, 8, 11, 12, 13, 16, 17
 digital watermarking, spectral domain 2
 digitized multimedia data 58
 direct sequence (DS) SS watermarking 459
 dirty paper coding (DPC) 324, 326, 327, 328, 332, 333, 335, 336, 338, 339, 341
 discrete cosine transform (DCT) 113, 119, 122, 126, 146, 231, 250, 252, 371, 392, 393, 394, 410, 419, 422, 423, 424, 427, 429, 438, 439, 440, 441, 445, 446, 447, 448, 451, 457, 458, 459, 461, 462, 465, 466, 479, 480, 481, 484
 discrete Fourier transform (DFT) 2, 3, 22, 33, 146, 371, 410, 424, 427
 discrete wavelet transform (DWT) 113, 118, 119, 120, 122, 124, 144, 146, 149, 150, 152, 153, 154, 155, 228, 229, 230, 231, 232, 233, 234, 235, 236, 239, 240, 241, 243, 244, 245, 246, 249, 250, 252, 253, 371, 394, 398, 410, 427, 429, 441, 446, 447, 448, 457, 474, 477, 480
 distribution infrastructure 158, 159, 195
 dither modulation (DM) 371
 document authentication 160, 165, 198
 document labeling 160, 165, 170, 177
 document management 457, 482
 document management, watermark-based protocol for 457
 document monitoring 160
 document-to-watermark ratio (DWR) 456
 document tracking 160
 dongles 160
 DRM, hardware solutions 160, 194
 DRM, software solutions 160
 dual-transform algorithms 228, 229
 DWT sub-bands 228, 229, 232, 234, 239
E
 echo addition 128
 edges 201, 202, 204, 214, 215, 216, 217, 218, 221, 226
 eigenvalues 258

eigenvectors 258
embedded messages 145, 149, 153
embedded signals 327
encryption 426, 448
enriched media 111, 124
enriched video functionality 112
enrichment data 111, 112, 121
enrichment information 113
enterprise DRM (E-DRM) 159, 198
erasure errors 411, 417
ergodic attacks 114, 116
ergodicity 117
ergodic zero-memory Gaussian noise source 114
error control coding (ECC) 408, 409, 415, 416, 424,
expectation maximisation (EM) 115, 124

F

facets 200, 201, 202, 204, 206, 207, 208, 209, 226
fast Fourier transform (FFT) 21, 26, 27, 31, 32, 35, 231
fast Walsh transform (FWT) 455, 459, 465, 466, 467, 468, 474, 480, 481, 483
feature points 290, 296, 299, 300, 302, 307, 309, 317, 318, 319, 321, 322
feature points, robust 290, 296, 299, 302, 317
field programmable gate array (FPGA) 455, 457, 458, 459, 462, 464, 468, 473, 474, 477, 480, 481, 483, 484
filtering 129, 131, 134, 137
fingerprinting 37, 129, 145, 160, 347, 349, 350, 351, 354, 356, 362, 363, 364, 366, 367, 428, 446, 452
fingerprinting applications 129
fingerprinting techniques 347
forensic photography 1
forensics 407
format coherence 111
format marking 159
Fourier magnitude 21, 22, 23, 24, 25, 26, 28, 29, 31
Fourier magnitude spectrum 290
Fourier-Mellin transform 290

Fourier phase 21, 22, 23, 24, 25, 26, 31, 32
Fourier transform 22, 23, 24, 25
fragile audio watermarking 131
fraud detection 348
fraudulent distribution 349
frequency-domain techniques 243
fuzzy logic 406

G

Gaussian channel models 410
Gaussian distribution 114
Gaussian distribution, generalized 410
Gaussian mixture 115, 116
Gaussian mixture-based capacity evaluation (GMC) 115, 116, 119, 120
Gaussians 108
Gaussians, difference of 108
genetic algorithms (GA) 370, 383, 391, 396, 403, 404, 406
geometrical transformations 37
geometric attacks 57, 59, 60, 62, 63, 64, 90, 95, 97, 101, 102, 256, 267, 268, 276, 290, 295, 296, 300, 322
geometric distortions 57, 60, 63, 103, 108, 128, 290, 320
geometric distortions-invariant watermarking system 57
geometric transformations 2
geometry attacks 226
graphics processing unit (GPU) 457, 459
gray scale 36, 37, 42

H

Hahn moments 57, 62, 63, 86, 87, 91, 92, 93, 94, 95, 96, 99, 100, 101, 102, 107, 108
Hahn moments, discrete orthogonal 57, 91, 92, 101, 102, 107
Hahn polynomials 79, 86, 87, 88, 89, 101, 102, 108
Hamming code 410, 412
hardware assisted real-time watermarking 457
HAS, spectral masking 147
HAS, temporal masking 147
hidden data 370, 383, 384, 385, 405
hidden data, security of 369, 370, 378, 379, 382, 384, 392, 394, 399, 401

hidden information 21, 22, 24, 25, 35
 hidden information capacity 21, 35
 hidden information robustness 27, 35
 hidden information security 26, 32, 35
 hidden transmission channel 255
 hidden watermarking zones 291
 high watermarking capacity 203
 histograms 37, 42, 43
 host audio 127, 130, 131, 135, 136, 137, 138, 139
 host multimedia signal 128
 host signal interference (HSI) 371, 372, 374, 399
 host signals 324, 325, 327, 328, 336, 340, 341
 hue, saturation, value (HSV) color space 38, 39, 43
 human auditory system (HAS) 131, 134, 135, 136, 146, 147, 243
 human visual system 37, 38, 39, 40, 41, 44, 50, 56
 hypergeometric series 108

I

illegal access prevention 425, 426
 illegal copies tracking 37
 illegal distribution 369
 illegal multimedia distribution 254, 255, 324
 illegal redistribution 324
 illicit copies 347, 359
 illicit copy detection 347
 illicit copying 59
 illuminant 37, 38, 39, 56
 image and video watermarking 425, 426, 427, 428, 430, 447, 448
 image moments 70, 101, 108
 image normalization 108
 image pixel values 21
 image tampering 424,
 image watermarking 36, 37, 42, 44, 50, 51, 52, 53, 54, 55, 410, 419, 420, 421
 image watermarking algorithms 201, 210
 imperceptibility 112, 229, 231, 234, 235, 240, 241, 248, 349, 370, 373, 375, 378, 383, 384, 385, 388, 391, 392, 393, 394, 395, 396, 398, 399, 400, 405, 427, 428, 437
 implicit surface models 201

improved spread spectrum (ISS) modulation 373
 inaudible signals 147
 in-band enriched multimedia 112
 in-band enrichment 111, 112, 113, 122, 124, 126
 independent component analysis (ICA) 62, 94, 95, 99, 100, 102, 108, 144, 146, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157
 information embedding 144, 146, 149, 155
 information hiding 144, 146, 157, 369, 370, 387, 388, 399, 402, 403, 404, 405
 information security requirements 255
 information-theoretic tools 325
 information theory 113, 121, 125
 insertion errors 411, 417
 integrated circuit (IC) 457, 458, 459
 intellectual property 289, 291, 317
 intellectual property rights 345, 367
 interactive HDTV 111
 interactivity 111, 123
 intractable attacks 201, 204
 invariant image features 57, 62, 90, 102
 invariant properties 108
 invariant quantities 57, 67, 68, 91, 92, 104, 105, 108, 109
 invariant vectors 290
 irregular sampling 203, 204
 iTunes Store 161

J

joint time-frequency representation 2
 JPEG compression attacks 235, 241
 JPEG (Joint Photographic Experts Group) image format 23, 31, 35
 just another watermarking scheme (JAWS) algorithm 457

K

k-ads 290, 291, 306
 Krawtchouk moments 62, 63, 81, 82, 83, 84, 85, 87, 95, 96, 101, 102, 108
 Krawtchouk polynomials 63, 79, 81, 82, 84, 87, 89, 101, 108

L

labeling 428
least significant bit (LSB) 21, 23, 32
least significant bit (LSB) technique 146
legacy data structures 2
literature piracy 158
log-polar mapping 290, 295, 296, 319
log-polar mapping, inverse 290
lossy compression 129
low bit modulation (LBM) based spatial do-
main image watermarking scheme 458
low density parity check codes (LDPC) 410,
413, 414, 415, 421, 422
luminance (brightness) 23, 24, 25, 26, 31, 36,
43, 45, 46
Lu'v' color space 56

M

malicious data tampering 59
maximum-likelihood (ML) detection 410, 414
M-band wavelets 371, 396, 398, 401, 404
mean-squared error (MSE) 40
media encryption 426, 439
media watermarking 291, 317
meshes, semi-regular 226
mesh watermarking schemes, blind 200, 201,
203, 204, 205, 209, 211, 214, 221, 222,
223
message authentication codes (MAC) 2
metadata 111, 428
mobile radio networks 455, 456
moment generating function 108
MS e-Book Reader 160
multi-access channels (MAC) 329, 331, 337,
338, 339, 340, 341, 342
multimedia content, authentication of 145
multimedia data 1, 5, 21, 31
multimedia data, copyright protection of 1
multiple watermarking 324, 325, 326, 329,
330, 331, 335, 337, 338, 340, 341, 342,
343
multiple watermarking systems 226,
multiuser information theory 324, 325, 331,
340

N

natural images 21, 22
network overhead 111, 112
neural networks, probabilistic 370, 394
noise addition attacks 256, 276, 279
Noise to Mask Ratio (NMR) 130, 140
noisy channels 113
non-blind watermarking scheme 203
NURBS (non-uniform rational basis spline)
models 201

O

object oriented paradigm 161
object oriented paradigm, data hiding concept
of 161
optimized watermarking 369, 405
orthogonal image moments 108
orthogonality condition 78, 79, 80, 81, 82, 86,
108

P

parity bit patterns 21
pattern recognition 36
peak signal-to-noise ratio (PSNR) 40, 41, 43,
56, 147, 235, 241, 248
perceptual audio coding 130
perceptual audio quality measure (PAQM) 130
perceptual evaluation of audio quality (PEAQ)
130, 147
perceptual transparency 229
physical blockades 426
piracy 367
pixel flipping 159
pixels 1, 6, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17,
18, 290, 292, 295, 317
platform specific solution 161
Pochhammer symbol 79, 81, 86, 108
polygons 200, 201, 202, 208, 223, 224, 225,
226
power series 79, 108
principal component analysis (PCA) 146, 148
prisoners' problem 255
privacy homomorphism 350, 353, 360, 363,
367
probability density functions (pdf) 114, 115,
116, 119

product activation 160
proof of ownership 128, 129

Q

quadrature carrier multiplexing (QCM) 457, 462, 475, 478, 480, 483
quality of service (QoS) 455, 456, 458, 467, 473, 481, 482
quality of service (QoS) assessment 370, 398
quantization 285, 288
quantization-based blind watermarking of semi-regular meshes 200, 203
quantization index modulation (QIM) 326, 328, 341, 369, 371, 376, 377, 378, 379, 381, 399, 401, 405
quantization index modulation (QIM) technique 146, 149, 150, 152
quantization index modulation (QIM) watermarking 369, 371, 399, 405
quantization schemes 37

R

RAM (random access memory) 456, 469, 470
real time spatial domain watermark embedder 457
redundancy 146, 155
Reed Solomon (RS) code 410, 411, 412, 413, 415, 417, 418, 419
reliable watermark extraction 131, 135
RGB decomposition 36
RGB (Red, Green, Blue) color 22, 23, 36, 37, 38, 39, 40, 47, 53
rigid transformation 108
robust blind copyright protection 145
robustness 112, 127, 128, 129, 130, 131, 132, 134, 135, 136, 137, 139, 141, 142, 143, 145, 146, 147, 149, 150, 228, 229, 231, 232, 234, 235, 236, 240, 241, 243, 248, 249, 255, 256, 260, 262, 264, 265, 266, 267, 268, 269, 271, 273, 275, 276, 277, 278, 400, 401, 405, 406, 427, 428, 429, 437, 447, 455, 456, 458, 461, 465, 480, 483
robust watermarks 204, 218
rotation 57, 59, 60, 61, 62, 63, 64, 65, 66, 67, 69, 70, 77, 78, 83, 84, 90, 98, 99, 100, 101, 107, 108

rotation scaling and translation (RST) 289, 295, 296, 300, 302, 304, 307, 309, 317, 318, 319, 322

RST, invariant domain 322

S

salt and pepper noise attacks 241
scalar Costa scheme (SCS) 326, 328, 341
scalar uniform quantizers 328
scale invariant feature transform (SIFT) 61, 62, 67, 68, 70, 91, 92, 97, 102, 108, 290, 296, 298, 299, 300, 301, 302, 304, 317, 320, 323
scaling 57, 59, 60, 61, 64, 65, 66, 67, 83, 90, 97, 98, 99, 100, 107
Secure Digital Music Initiative (SDMI) 129
security 348, 349, 362, 363, 364, 365, 366
security intensive information 58
segmentation 285, 288
Shannon's limit 408, 411, 417
shape theory 289, 290, 291, 305, 318, 322
side information channels 113
side information (SI) 327, 331
signal processing algorithms 37
signal processing techniques 127, 137
signal separation 62, 109
signal to noise ratio (SNR) 408, 412, 414, 415, 419, 420, 421
similarity transformation 108
single watermarking 324, 325, 326
singular value decomposition (SVD) 228, 229, 231, 232, 233, 234, 235, 236, 239, 240, 241, 243, 244, 245, 246, 249, 250, 251, 252, 254, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288
singular value modification 256
singular values, elements of 228, 229, 232
singular values (SV) 228, 229, 231, 232, 245, 257, 258, 259, 260, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 287, 288
singular value substitution 256

singular vectors 288
soft computing 402, 405
Sony Rootkit 161
space coding 159, 191
spatial domain 323
spatial domain techniques 1
spatial scaling 128
spatial watermark insertion scheme 1
spread spectrum (SS) modulation 369, 371, 372, 373, 374, 388, 390, 395, 396, 397, 398, 399, 403
spread spectrum (SS) watermarking 455, 456, 457, 458, 459, 460, 461, 462, 465, 467, 474, 475, 478, 480, 481, 483
spread spectrum watermarking 145, 405
spread transform dither modulation (STDM) 371
SSIM (mean structural similarity) 41
SS watermarking 369, 371, 372, 373, 388, 390, 395, 396, 397, 398, 399, 403
SS watermarking, fragile 456
Stanford Bunny mesh 204
stationarity 116, 117, 122
steganographic systems 35
steganography 21, 25, 26, 27, 31, 32, 33, 34, 35, 36, 44, 52, 144, 145, 148, 156, 157, 158, 159, 161, 169, 181, 196, 197, 254, 255, 256, 260, 262, 263, 279, 280, 281, 282, 283
steganography, active 407, 415, 416, 424
stego 27, 35, 370, 379, 382, 383, 388, 392, 393, 400, 402
stego image 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 35
stego medium 22, 35
stego watermarking techniques 407
substitution errors 411
support vector machine (SVM) 370, 383, 388, 391, 392, 399
SVD, normal 288
SVD Transform, energy 257
SVD Transform, existence and uniqueness 257
SVD Transform, low-rank approximation 257
SVD Transform, stability 257
symmetric fingerprinting 367
synchronization errors 411

T

tamper detection 425, 426, 427
Tchebichef moments 61, 62, 84, 85, 87, 96, 101, 102, 108
Tchebichef polynomials 84, 85, 86, 87, 88, 108
TCQ watermarking 369, 406
text copyright protection 158
three dimensional (3-D) meshes 2, 4, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226
three-dimensional (3-D) meshes, digital watermarking of 200
three dimensional (3-D) meshes, similarity transformation of 226
three dimensional (3D) meshes, watermarking of 2
three dimensional (3-D) models 200, 215, 226
time-domain techniques 243
transform domain 323
transform domain algorithms 2
transform domain techniques 1
translation 57, 59, 60, 61, 62, 63, 64, 66, 67, 70, 73, 77, 78, 83, 84, 90, 100, 105, 106, 107, 108
transmission noise 147
transparency 325, 326, 328, 329
transparent embedding 128
trellis coded quantization (TCQ) 369, 371, 380, 381, 382, 383, 406
trellis codes 410
Trimedia TM-1000 VLIW processor 457
trusted third parties (TTP) 345, 352, 353, 354, 356, 357, 358
turbo codes 410, 415

U

unauthorized digital copying 1, 59
unauthorized tampering 369
unauthorized usage 324
uncompressed music 131
uniform scalar quantizer 328
universal domain 323
universal images (UI) 291, 304
users simplicity 348

V

valence 202, 210, 226
 variable transformation 107
 vertices 201, 202, 204, 205, 206, 207, 208, 209, 210, 211, 217, 218, 226
 very large scale integration (VLSI) 369, 401
 video enrichment 111
 video rotation attacks 241
 virtual graphs 1, 6, 7, 8, 12, 13, 17, 18
 visible watermarking design 457
 vision system 37, 38, 39
 visual attacks 26, 35
 visual information fidelity (VIF) 41
 visual spectrum 38
 VLSI architecture 455, 457, 462, 467, 468, 469, 470, 471, 472, 473, 474, 478, 479, 480, 481, 483, 484
 VLSI chip 458, 481, 484
 voxels 1, 4, 11, 12, 13, 16
 voxel (volumetric pixel) models 201

W

watermark bit carriers (primitives) 204, 205, 207, 209, 210, 211, 212, 213, 214, 215, 216, 217, 221, 222
 watermark bits 204, 205, 214, 228, 229, 232, 240, 245, 246
 watermark decoding 131, 135
 watermark detection 128, 129, 130, 131, 135, 139, 425, 426, 427, 428, 429, 433, 434, 443, 452
 watermark detector 427, 428, 444
 watermarked bit rate 131
 watermarked meshes 201, 203, 204, 209, 212, 221, 222, 226
 watermark embedder 427, 428
 watermark embedding algorithms 158
 watermark embedding capacity 128
 watermark embedding procedures 232, 233, 234, 239, 243, 244, 246, 247, 327
 watermark extraction 200, 201, 204, 209, 213, 215, 216, 219, 221, 425
 watermark extraction procedures 232, 234, 240, 245, 246
 watermark extractor 427

watermark, imperceptibility 146, 147, 150, 152
 watermarking 21, 22, 32, 57, 59, 60, 61, 62, 63, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 111, 112, 113, 114, 115, 116, 117, 118, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 382, 383, 424, 388, 390, 391, 392, 394, 395, 396, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 421, 422, 423, 424,
 watermarking algorithms 1, 2, 3, 4, 37, 127, 128, 130, 131, 132, 134, 136, 143, 228, 229, 231, 232, 234, 236, 243, 247, 249, 455, 457, 461, 462, 474, 478, 479, 480, 481, 483, 484
 watermarking algorithms, frequency domain 427
 watermarking algorithms, imperceptible 228, 229, 232, 243, 249
 watermarking algorithms, robust 228, 229, 232, 249, 251, 253, 326, 328, 329, 332, 333, 336
 watermarking algorithms, spatial domain 427, 437, 447
 watermarking applications 36
 watermarking capacity 111, 113, 115, 118, 124, 125
 watermarking decoders 409, 410, 414
 watermarking detectors 409, 410, 415
 watermarking, fragile 145, 149, 151, 326, 328, 329, 332, 336
 watermarking framework 112, 117
 watermarking, images 289, 290, 291, 292, 294, 296, 298, 299, 302, 307, 309, 310, 311, 317, 318, 319, 320, 321, 322, 323
 watermarking philosophy 111
 watermarking, robust 145, 147, 149, 150, 201, 204, 212, 213, 214, 215, 216, 218, 219, 220, 221, 223, 326, 328, 329, 332, 333, 336
 watermarking schema 323
 watermarking, semi-fragile 145, 326, 328, 329
 watermarking techniques 37, 49, 111, 123,

- 229, 230, 231, 232, 249, 252, 344, 345, 346, 347, 350, 361
watermarking techniques, frequency-domain 229, 243
watermarking techniques, spatial-domain 229
watermarking techniques, transform-domain 229
watermarking, videos 289, 308, 309, 320, 321
watermark removal 37
watermarks 1, 2, 3, 4, 5, 6, 12, 13, 16, 17, 19, 20, 57, 59, 60, 61, 62, 63, 64, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 107, 108, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 228, 229, 427, 428, 429, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452
watermarks, annotation part 326, 329
watermarks, digital 59, 107, 255, 259
watermarks, fragile 201, 203, 204, 205, 206, 207, 208, 211, 212, 216, 217, 218, 219, 220, 221, 222, 223, 226, , 427, 428, 433, 434, 436, 437, 438, 442, 450
watermarks, high-capacity 204, 212, 213, 214, 216, 218, 219, 221
watermarks, imperceptible 202
watermarks, robust 1, 202, 427, 428, 429, 434, 436, 437, 438, 445, 448, 449, 450
watermarks, semi-fragile 203
watermarks, tamper detection part 326, 329
wavelet coefficients 228, 229, 231, 232
wavelet packets 371
wavelets 370, 371, 396, 398, 401, 402, 404
Wavelet transform 226
weak noise signals 243
Weibull distribution 410
white Gaussian noise 114, 122
wireless communication systems 456, 467
wireless mobile communication services 456
word error probability (WER) 131

X

XYZ color space 39, 56

Y

YCbCr color space 38, 39, 41, 43

Yuv color space 38, 47