ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/272747716

Digital Image Watermarking: An Overview

Conference Paper · February 2011

CITATIONS
0

READS
2,274

1 author:

Jobin Abraham
Mahatma Gandhi University
20 PUBLICATIONS **45** CITATIONS

SEE PROFILE

All content following this page was uploaded by Jobin Abraham on 25 February 2015.

The user has requested enhancement of the downloaded file.

Digital Image Watermarking: An Overview

Jobin Abraham
Research Scholar
M.G University, Kottayam

Abstract

Digital data can be easily copied, modified and forgeries be created by anyone having a computer. Most prone to such malicious attacks are the digital images published in the Internet. Digital Watermarking can be used as a tool for discovering unauthorized data reuse and also for copyright protection.
Digital Watermarking is the technique of embedding some identification information known as watermark into the digital data by its owner. On embedding or data hiding a watermarked data is generated. Large numbers of watermarking schemes are currently available. An acceptable Watermarking must possess certain qualities as robustness and imperceptibility.
The recent research and developments in the field of Watermarking is reviewed and is subjected to a detailed study in this paper. The current status and issues are then discussed to give direction to future works.

Keywords: *digital watermarking, robust, image watermarking techniques, features, applications.*

1. Introduction

Digital data storage has gained popularity over the analog counterparts for information storage and handling. Digital techniques are far superior to analog counterparts. However, a difficulty faced in digital world is that the manipulation and duplication of digitalized information is very easy. For instance, anyone who has a computer system can easily create forgeries and then redistribute the images and other data's through the Internet [1]. Suitable techniques must be developed and made available to protect the data from unauthorized modifications and illegal reuse.

Digital watermarking is proposed as a method for protecting the ownership rights of digitalized data. Digital watermarking integrates or embeds some information as the owner name or logo in to a digital media. Thus watermark information will serve as the identification mark of its owner. With the aid of this embedded watermark whenever we suspect the data or an image is illegally edited and copied it is possible to produce enough evidence to prove the ownership.

1.1 History

Watermarking as technique for copyright protection evolved with the discovery of paper. The word Watermarking is coined from the conventional use of placing a visible watermark on paper. It was used as a method against counterfeiting books and currency notes.

The origin of data hiding or invisible watermarking may be traced to the age of ancient Greeks who transferred their information after modifying the contents in a text by swapping the positions of alphabets. The Greeks thus were able to send secret information across the border without getting noticed. In Rome the heads of slaves were shaven and a message is tattooed. When the hairs are fully grown they are send to the destinations through the enemy lines.

By 18^{th} century Watermarking began to be used as anti-counterfeiting measure on money and other documents. The first patent in Watermarking was filed by Emil Hembrooke in 1954, titled "Identification of Sound and like Signals". In early 1980s, Muzak Corporation used to watermark analog audio signal to identify their music. Their system used a notch filter to block the audio signal at 1 KHz for a varying duration to encode identification information using Morse code. About 1995, interest in digital Watermarking began to mushroom.

1.2 Steganography vs. Watermarking

Steganography is a sub discipline of cryptography and means data hiding. Cryptography is about maintaining the secrecy of the information by encoding them. This forbids from being read by any unauthorized person. Steganography attempts to maintain the information secrecy by not getting noticed also at the same time. Steganography in Greek means covered writing or secret writing. In Steganography information is hidden in a harmless source, known as cover media, in a way that it is not known to others. The existence of the information thus goes unnoticed.

Watermarking integrates information into a data without affecting its actual usage. Watermarking mostly uses same principles and techniques as Steganography for data insertion and hiding in a host media. However, information hiding as done in Steganography is many way different from cryptography where the chief concern is protecting the message content. Table 1 shows a comparison between the three.

Process	Method Adopted	Purpose	Feature
Cryptography	Data is encrypted using a secret key.	Protects the contents in point to point communication.	Maintains the message secrecy.
Steganography	Uses a cover media to hide the data.	Existence of a message is kept as secret.	Hides actual messages from unauthorized listeners/viewers
Watermarking	Inserts an unique owners identification mark.	Copyright Protection, Authentication	Do not protect the content; the ownership rights could be established.

Table. 1 A Comparison of watermarking vs. others

1.3 Uses of Watermarking

Protecting the digital data in our databases or internet from unauthorized reuse is tedious.. Practically, it may not be possible to stop the illegal data modification or copy generation. Using an embedded watermark in the source data the ownership rights can be established beyond doubt.

Watermarking makes the duplications identifiable and thus reuse becomes almost impossible. For instance the currency notes are watermarked by the government as proof for their authenticity. This makes forgeries difficult and identifiable from the original. Another popular use of Watermarking is for tamper proofing. The content of the watermarked data is verifiable and can discover any manipulations and unacceptable modifications if any.

Watermarking is now possible for any digital media as: text, audio, video or images. Digital watermarking is very much useful for varied application as: Proof of ownership, Means of tamper proofing, Labeling for user awareness, Covert communication, Broadcast Monitoring, device identification and controlled access.

2. Digital Image Watermarking

In Digital Image Watermarking the watermark signal is embedded into a source image that is to be protected against abuses. Watermark can be a string of bits representing a text or owners name or an image such as a trademark symbol or logo.

2.1 Desirable features of Watermarking System

A Watermarking process should introduce only small amount of noise or distortions while embedding the watermark. Losses should be minimal. Too much of distortions will degrade the usability of the digital data. Most of the Watermarking systems in the literature are not lossless. Most desirable features[2] of recent watermarking system are:

- Robustness
  By robust it means the watermarked image is able to survive manipulations and other attacks. Watermarking must also withstand severe signal processing attacks [3] as compressing or scaling. Robustness is the ability of the watermarked signal to *resist* the attacks or distortions introduced by malicious data processing. This feature makes watermarked images acceptable for legal purpose.

- Imperceptibility
  A watermark, in fact has the effect of adding noise. However, the watermark must not distract the viewer from the image itself. The modifications introduced on watermark insertion should be below the perceptible threshold. After embedding, the watermarked image must be visibly appealing and identical to the original media. A watermark is called imperceptible if the original signal and marked signal is indistinguishable.

- Reversibility
  Reversibility is a measure of the extent to which watermark signal removal is possible from the watermarked media. In certain applications as forensic or medical, the watermark removal is desirable once the purpose is served. After authentication the image can be restored to their original form by removing the watermarking.

- Lossless embedding
  The embedding process usually transforms the images to some domain as cosine transform or wavelet transform for adding the watermark signal. Distortions are normally introduced as an after effect of this conversion. A good watermarking system should be lossless, in that it should not distort the original contents or in other words should not affect the functionality of the media.

- Security
  Watermarks must exist undetectable. Even by use of known methods or algorithms the watermark removal should not possible to an intruder. Security means that even after the presence of the watermark is known to a malicious attacker it must not be possible for them to remove the same from the host media.

2.2 Classifications of Watermarking System

Watermarking systems are classified based on the method used for watermarking and also on certain features as visibility and strength of the watermark in the embedded media. The application scenario for which the watermarking is used has a significant say over the choice of the method used. Watermarking systems that are currently in use can be classified as follows

- Visible or Invisible

This classification is based on the perceptibility of the hidden watermark in the host media. Visible Watermarking techniques provide means for overt assertion of ownership rights. Whereas, Invisible watermarks are imperceptible to human eyes and hence provides covert protection of rights.

- Fragile or Robust

Robust watermarks are able to withstand degradations or attacks on watermarked images. Fragile watermarking however is broken or lost when they are a subject to attacks. The application for which Fragile and Robust watermarking used differs. A robust watermark is often used for the cases where copyright or ownership rights are to be ascertained.

Fragile watermarks breaks on modifications. Hence these methods are well suited for content authentication or tamper proofing [4]. Another sub-category is *semi-fragile* watermarking. Semi-fragile watermarking is designed to break under any changes that exceed a threshold specified by the user. In other words, a semi-fragile watermarking scheme allows some amount of modifications upon the original content and breaks beyond a limit permitted by its owner.

- Blind or Non-blind

At the stage of detection or watermark retrieval some techniques requires the original signal as well. The watermarked signal is then compared with the original signal to generate the watermark. Based on the need for original signal at the time of retrieval process, the watermarking schemes can be classified as Non-blind or Blind. Blind schemes [5] require only the algorithm for decoding and the watermarked image in detection phase. Whereas, a Non-blind technique need the original signal as one of the input to complete the detection process.

3. Watermarking Process

3.1 Watermarking System

A Watermarking system comprises two distinct stages: Embedding and Detection. Watermark embedding needs an algorithm and a unique watermark that is encoded into the host media by the algorithm. The figure.1 shows the embedding process. The embedding algorithm E accepts the watermark w and embeds this in the image I to create the watermarked signal I'.

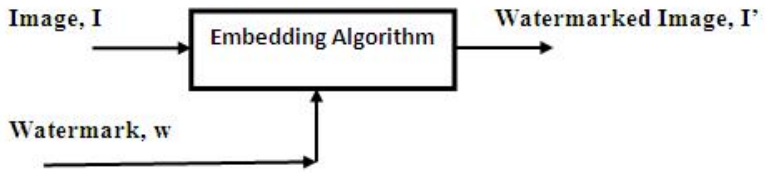

Figure.1 Embedding operation

The decoding section retrieves the watermark from the watermarked signal when it is required to of the owner to prove his ownership rights. Figure 2 illustrates the decoding operation.

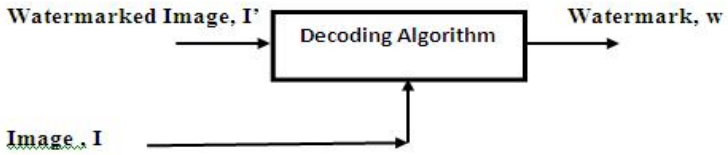

Figure.2 Decoding operation

The decoding algorithm retrieves the watermark w from I'. When decoding, there are techniques that do need the original image and others that do not need original images. The above is a blind watermarking technique that the original image to generate watermark w.

3.2 Watermarking Techniques

Watermark embedding can be considered as superposition of the watermark signal on the original image. Digital Image Watermarking is the process of embedding some information w in to an image x to form a watermarked image, say x´.

$$x' = E(x, w)$$

The original image is referred to as the host image/data into which the watermark w is hidden imperceptibly. A variety of algorithms are used for information integration. Watermarking methods are broadly classified as[6]:

- Spatial domain method
- Transform domain methods

In spatial domain watermark integration is done by modulating the intensity of certain pixels from the host image. The watermark is embedded to the least significant bit (LSB) of the original image. While some methods uses DCT[7] or DWT [10] transforms domains for selecting the coefficients whose magnitude is then changed. Spatial domain methods are less complex; however they are easier targets to attacks[7].

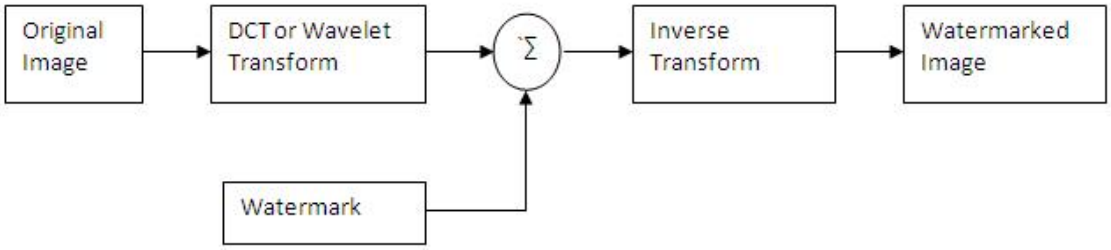

Figure. 3 Watermarking Procedure

Transform domain watermarking methods uses transforms as DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform) or DWT (Discrete Wavelet Transform). Figure.3 shows how a Watermarked image is generated. Transform domain watermarking methods have gained popularity as they are more robust to attacks. This is attributable to the fact that when image is inverse wavelet transformed the watermark w is distributed irregularly over the entire host image thus making the watermark removal almost impossible for attackers.

4. Applications of Digital Image Watermarking

The increased interest in Watermarking is accelerated by the copyright concerns that is now a necessacity with the advancement of computer technology and wide use of Internet. Watermarking is becoming a lot more popular and has applications [1][9] in many areas as:

- **Copyright Protection**

Copyright protection is the most prominent application of Watermarking. Who did first is the issue that is addressed by this application. In the internet age there is always the risk of published digital data be stolen and reused without obtaining any legal permission. Many a times information is tampered or modified to the levels that are unacceptable. In such cases of misuse the original creator of the document could establish his ownership rights.

- **Content Authentication**

Content Authentication assures the data integrity. Digital images may be subjected to editing or removal of certain pixels areas. There may not be even any visible difference between the original and manipulated image in first sight to a viewer. However small these modifications or manipulations are the integrity of the data should be verifiable.

- **Fingerprinting**

Fingerprinting permits us to trace the source of illegal copy generation whenever is reported. When licensed documents are distributed they are uniquely watermarked so that the individual buyer of the copy is identifiable. This shall enable us to trace the source of illegal copy distribution.

- **Captioning**

Captioning or labeling permits the creator of the digital data to add his identification marks or additional information as authors name, date, location, and version number etc. For instance a publisher of an image in Internet can label them using his contact number for securing rights for higher resolution copy of the same image. Here the watermark is visible and carries a piece of information for its viewers.

- **Covert communication**

A hidden piece of information can be transmitted in a host media to a destination without being noticed. This is similar to Steganography where the information is hidden in a cover media. The watermark must be imperceptible to the eyes of the viewer. If the effects of watermarking are too strong it will attract the attention of attacker who may eventually succeed in retrieving the embedded information.

- **Broadcasting Monitoring**

Production cost of broadcasting material such as news or shows are enormous. Therefore, production companies are very much concerned in protecting their videos from illegal reuses and other rebroadcasting activities. When television signals are broadcast, they contain watermarked video so as to enable the identification of rebroadcasts.

Watermark information could also be useful in linking a piece of document to its database for finding the similar versions or continuation of the same program. Another proposed usage is, watermark could serve in verifying whether the video is broadcast in full or as agreed while securing the telecast rights.

5. Threats and Challenges

Digital data can be easily copied, edited and transferred. The use of Watermarking does not ensure that our digital data is protected from being copied and edited. However, watermarking permits us to prove the copyright of the authors and also in protecting the authenticity.

Any operation, intentional or unintentional, upon the watermarked data that impairs the watermark can be called as an Attack[3]. Digital Images are subject to varied attacks as cropping, scaling, rotating, scaling, compression and noise. Most of the proposed conventional watermarks in literature are easily broken on attacks or on multiple attacks. Robustness to attacks is thus the most desired feature if the ownership right has to be established in the court.

The watermarks are weakened by signal processing as signal enhancement or D/A and A/D conversion. Many watermarks are unable to withstand strong lossy compression. Content-based watermarking approach that uses geometric wrapping to embed watermarks proposed in [11] offers high robustness against lossy compressions to some extent. Intentional attacks as removal of watermarks are possible if an attacker procures many copies of differently watermarked images and tries by averaging all copies. An attacker may also attempt to remove the watermark by trying to estimate the original image.

Another possible attack that can create ambiguity is, when an attacker re-watermarks the image using his logo. The attacker will be able to generate his watermark from the watermarked data and can claim to be the real owner.

6. Conclusion

In recent years watermarking has emerged as a trustable tool for proving the ownership rights and authenticity of digital documents. Digital watermarks could now be inserted into any digital media in a way they are imperceptible to human eyes but are detectable only to owners computer algorithm for the retrieval of watermark.

Digital Watermarking has close links with Steganography. It is many times assumed that cryptographic techniques like encryption or techniques as time stamping alone will ensure the secure authentication of data. Digital Watermarking is presented as a technique for hiding information in any digital media for the purpose of ownership

identification. Watermarking techniques mostly uses the principles of signal processing and sometimes even uses the cryptographic techniques for data hiding.

Most sought after feature of watermarking system is the ability to withstand attacks. The watermark should be retained in the host image even after the source image is subjected to repeated modifications or manipulations. Features as imperceptibility, robustness and reversibility are also significant while accessing the quality of a Watermarking System.

References

[1] Ingemar J.Cox and matt L Miller ,"The first 50 years of Electronic Watermarking", EURASIP Journal of Applied Signal Processing, 126-132, 2002.

[2] Jen Bang Feng, "Reversible watermarking: Current Status and Key Issues", International Journal of Network Security, Vol 2, PP161-171, May 2006

[3] S. Voloshynovskiy, S.Pereira, T.Pun , " Attacks on Digital Watermarks: Classification, Estimation based Attacks and Benchmarks", IEEE Communications Magazine, Vol.39, pp115-126, 2001.

[4] P. Meenakshi Devi , M. Venkatesan and K. Duraiswamy, "A Fragile Watermarking scheme for Image Authentication with Tamper Localization Using Integer Wavelet transform" , Journal of Computer Science 5(11) PP831-837, 2009.

[5] Dr. M.A Dorairangaswamy, "A Novel Invisible and Blind Watermarking Scheme for copyright protection of Digital Images", International Journal of Computer Science and Network Security, Vol.9, No.4, PP71-78, Nov 2009.

[6] Kamran Hameed, Adeel Mumtaz and S.A.M Gilani, "Digital image Watermarking in the wavelet transform domain", World Academy of Science, Engineering and Technology 13 2006.

[7] Sami Baba, Lala Krekor, Thawar Arif and Zyad Shaaban, "Watermarking Scheme for copyright protection of digital images", IJCSNS International Journal of Computer Science and Network Security, Vol.9, No.4, PP1-4, April 2009.

[8] Mona M El-Ghoneimy, "Comparison between two Watermarking Algorithms using DCT Coefficient, and LSB Replacement ", Journal of Theoretical and Applied Information Technology, PPP132-139, 2005

[9] Patrick Lam, Orion Winkelmeyer, " Watermarking Technologies-Analysis and Design Report ", 2005

[10] Kamran Hameed, Adeel Mumtaz and S.A.M Gilani, "Digital image Watermarking in the wavelet transform domain", World Academy of Science, Engineering and Technology 13 2006.

[11] Dima Profrock,Mathias Schlauweg, Erika Muller, "Content-Based Watermarking by Geometric Wrapping and Feature-Based Image Segmentation" PP 572-581, SITIS 2006

View publication stats