Techniques of Watermarking

[1]Jaspreet Kaur, [2]Sandeep Singh Kang
[1,2]CEC, Landran, Mohali, Punjab, India

Abstract
A digital watermark is a piece of information which is embedded in the digital media and hidden in the digital content in such a way that it is inseparable from its data. This piece of information known as watermark, a tag, or label into multimedia object such that the watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video, or text.

This paper is focused on noteworthy work and techniques used for images during preliminary and principal development stage of digital watermarking by various researchers with the utility of giving a fundamental understanding of the basic principles of digital watermarking as it has evolved. This may serve as the concrete foundation and the base for understanding further advances in this technology in later years. This paper gives a summary of different innovative techniques in this emerging area.

Keywords
Digital Watermarking, watermarking, techniques of watermarking, role of watermarking in security.

I. Introduction

Watermark, a recognizable image or pattern in paper used to identify authenticity. Digital watermarking is the process of embedding copyright information such as author/owner/usage restrictions into the original file. Digital watermarks are created by converting copyright information into apparently random digital "noise" using an algorithm that is imperceptible to all but special watermark-reading software. So while a JPEG file that is read by a Web browser may display a pretty picture, that same file will display the copyright when read by the watermark software. The demand for this type of technology can be expected to grow enormously as businesses seek to assert some control over their property on the "everything is free" Internet. This may give rise to the possibilities of illegal copy or reproduction. Securing digital images while transferring through networks and later extracting it in the original form is a very challenging task. Several advance computation techniques have been developed which provide security to digital media while transmission through open networks. There have been several proposals from various researchers, to hide and extract watermark from digital image using spatial and frequency domain techniques. However, in most of the methods, there is a gradual reduction in the fidelity of the original cover image with the increase in embedded information content. The rapid growth of the Internet increased the access to multimedia data tremendously [1, 2]. The development of digital multimedia is demanding as an urgent need for protect multimedia data in internet. Digital watermarking techniques provides copyright protection for digital data [3-6].

II. Techniques used for watermarking

A. Embedding and Extraction

In this technique the insignificant portion of the fractional part of the pixel intensity value of the cover image is encoded to provide watermark. A watermark in the insignificant part has helped to maintain the fidelity of the cover image. As seen from the results, imperceptibility is well preserved. Large capacity of watermarking is an added advantage of this scheme. Thus, large capacity watermark may be successfully embedded and extracted using this scheme, which can be extremely useful for companies engaged in developing watermarking applications and digital information security products. Embedding and extraction algorithms are used in this technique [7].

B. Secure Spread Spectrum Watermarking

We describe a digital watermarking method for use in audio, image, video and multimedia data. We argue that a watermark must be placed in perceptually significant components of a signal if it is to be robust to common signal distortions and malicious attack. However, it is well known that modification of these components can lead to perceptual degradation of the signal. To avoid this, we propose to insert a watermark into the spectral components of the data using techniques analogous to spread spectrum communications, hiding a narrow band signal in a wideband channel that is the data. The watermark is difficult for an attacker to remove, even when several individuals conspire together with independently watermarked copies of the data. It is also robust to common signal and geometric distortions such as digital-to-analog and analog-to-digital conversion, resampling, quantization, dithering, compression, rotation, translation, cropping and scaling. The same digital watermarking algorithm can be applied to all three media under consideration with only minor modifications, making it especially appropriate for multimedia products. Retrieval of the watermark unambiguously identifies the owner, and the watermark can be constructed to make counterfeiting almost impossible. We present experimental results to support these claims [8].

C. DCT-based watermarking

The image is first divided into 8 × 8 pixel blocks. After DCT transform and quantization, the midfrequency range DCT coefficients are selected based on a Gaussian network classifier. The mid-frequency range DCT coefficients are then used for embedding. Those coefficients are modified using a linear DCT constraints. It is claimed that the algorithm is resistant to JPEG compression. [9]

D. Spread Spectrum

Cox et al. [1997] [2] used the spread spectrum to embed the watermark in the frequency components of the host image. First the Fourier Transform is applied to the host image is inserted to obtain a modified values V_ using the following equation:

$V\_ = V + \alpha \times W$. (3)

The scaling parameter α is used to determine the embedding strength of the watermark. Different spectral components exhibit different tolerance to modification.

To verify the presence of the watermark, the cross correlation value between the extracted watermark W_ and the original watermark W is computed as follows:

$sim = W\_ \times WT$

(W_ × W_T)(W × WT)

Here, we call the cross correlation the similarity (sim). Experimental results showed that this method resists JPEG compression with a quality factor down to 5%, scaling, dithering, cropping and collusion attacks.

E. Wavelet Based Watermarking

The multi resolution data fusion is used for embedding where the image and the watermark are both transformed into the discrete wavelet domain. The watermark is embedded into each wavelet decomposition level of the host image. During detection, the watermark is an average of the estimates from each resolution level of wavelet decomposition. This algorithm is robust against JPEG compression, additive noise and filtering operations.

F. Robust Watermarking Technique

Contrary to the LSB approach, the key to making a watermark robust is that it should be embedded in the perceptually significant components of the image. A good watermark is one which takes into account the behavior of human visual system. For the spread spectrum based watermarking algorithm, a scaling factor can be used to control the amount of energy a watermark has. The watermark energy should be strong enough to withstand possible attacks and distortions. Meanwhile a large watermark energy will affect the visual quality of the watermarked image. A perceptual model is needed to adjust the value of the scaling factor based on the visual property of the host image to achieve the optimal trade-off between robustness and invisibility.

G. Invisible Watermarking

This technique presents a novel invisible robust watermarking scheme for embedding and extracting a digitalwatermark in an image. The novelty lies in determining a perceptually important subimage in the host image. Invisible insertion of the watermark is performed in the most significant region of the host image such that tampering of that portion with an intention to remove or destroy will degrade the esthetic quality and value of the image. One feature of the algorithm is that this subimage is used as a region of interest for the watermarking process and eliminates the chance of watermark removal. Another feature of the algorithm is the creation of a compound watermark using the input user watermark (logo) and attributes of the host image. This facilitates the homogeneous fusion of awatermark with the cover image, preserves the quality of the host image, and allows robust insertion-extraction.Watermark creation consists of two distinct phases. During the first phase, a statistical image is synthesized from a perceptually important subimage of the image. A compound watermark is created by embedding a watermark (logo) into the statistical synthetic image by using a visible watermarking technique. This compound watermark is invisibly embedded into the important block of the host image. The authentication process involves extraction of the perceptive logo as well statistical testing for two-layer evidence. Results of the experimentation using standard benchmarks demonstrates the robustness and efficacy of the proposed watermarking approach. Ownership proof could be established under various hostile attacks [10].

H. Watermarking of Digital Audio and Image using Matlab Technique

Watermarking, a Watermark is encrypted using RSAAlgorithm and is embedded on the audio file using LSB technique. LSB technique is an old technique which is not very robust against attacks. Here, in audio watermarking we have embedded the encrypted watermark on the audio file, due to which removal of the watermark becomes least probable. This would give the technique a very high robustness. In the retrieval, the embedded watermark is retrieved and then decrypted. This method combines the robustness of Transform domain and simplicity of spatial domain methods. For image Watermarking, DWT technique is used. DWT technique is used in Image watermarking. Here, the watermark is embedded in the image as a pseudo-noise sequence. This gives a remarkable security to the image file as only if the exact watermark is known can the embedded watermark be removed from the watermarked image.

I. Watermarking While Preserving The Critical Path

The first intellectual property protection technique using watermarking that guarantees preservation of timing constraints by judiciously selecting parts of the design specification on which watermarking constraints can be imposed. The technique is applied during the mapping of logical elements to instances of realization elements in a physical library. The generic technique is applied to two steps in the design process: combinational logic mapping in logic synthesis and template matching in behavioral synthesis. The technique is fully transparent to the synthesis process, and can be used in conjunction with arbitrary synthesis tools. Several optimization problems associated with the application of the technique have been solved. The effectiveness of the technique is demonstrated on a number of designs at both logic synthesis and behavioral synthesis [11].

J. Buyer-seller watermarking protocols

This technique integrate watermarking techniques with cryptography, for copyright protection, piracy tracing, and privacy protection. In this paper, we propose an efficient buyerseller watermarking protocol based on homomorphic public-key cryptosystem and composite signal representation in the encrypted domain. A recently proposed composite signal representation allows us to reduce both the computational overhead and the large communication bandwidth which are due to the use of homomorphic public-key encryption schemes. Both complexity analysis and simulation results confirm the efficiency of the proposed solution, suggesting that this technique can be successfully used in practical applications. [12].

K. Watermarking using Cellular Automata Transform

Another watermarking technique is using cellular automata transform. An original image is CA-transformed and watermark is embedded in to coefficients of CA-transformed pattern. this watermarking model has flexibility in data hiding. it is possible to embed watermark in many CAT plans with different rule number parameters and CA bases class of CAT and all kind of image models such as shape, letter, photo can be used as watermark data. Using CAT with various rule number parameters, it is possible to get many channels for embedding [13].

III. Conclusion

In this paper, we have surveyed many of the techniques proposed for watermarking. Thus this paper may serve as a ready reference for any new researcher willing to explore the basics and foundation works in the area of digital waternarking since its evolution to the point where it started gaining prominence in the area of digital media control. This paper gives a base to understand the recent advances in digital watermarking which may have happened after the previous works described in this paper but not covered in this paper.

References

[1] S.Katzenbeisser, F.A.P. Petitcolas, "Information Hiding Techniques for steganography and Digital Watermarking", Norwood,MA: Artech House,2000, [Online] Available: http://www.sersc.org/journals/IJAST/vol11/1.pdf

[2] Cox, J. Kilian, F. Leighton, T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Processing, vol. 6,pp. 1673–1687, 1997.

[3] N. Nikolaidis, I. Pitas, “Copy right Protection of images using robust digital signatures”, in proceeding, IEEE International Conferences on Acoustics, Speech and signal processing , Vol.4, 1996, pp. 2168-2171.

[4] Houng.Jyh Wang, c.c, Jay Kuo,“Image protection via watermarking on perceptually significant wavelet coefficient”, IEEE 1998 workshop on multimedia signal processing, Redondo Beach, CA, Dec. 1998.

[5] S.Craver, N. Memon, B.L, M.M Yeung, “Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implication”, IEEE Journal on selected Areas in communications. Vol.16 Issue:4, 1998, pp. 573-586.

[6] [Online] Available: http://www.ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4809139 {new technique}

[7] [Online] Available: http://www.ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=560429[new technique]

[8] [Online] Available: http://www.ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=771066

[9] [Online] Available: http://www.delivery.acm.org/10.1145/1250000/1242473/a5zheng.pdf?ip=203.129.220.149&CFID=39257849&CFTOKEN=22823083&__acm__=1314075846_24ff889602dc608a399fdd270631e437

[10] [Online] Available: http://www.delivery.acm.org/10.1145/1420000/1413865/a12mohanty.pdf?ip=203.129.220.149&CFID=39257849&CFTOKEN=22823083&__acm__=1314075842_8220e809658bae8eb4f2777727740a1a

[11] [Online] Available: http://www.delivery.acm.org/10.1145/340000/337328/p108meguerdichian.pdf?ip=203.129.220.149&CFID=39257849&CFTOKEN=22823083&__acm__=1314076721_6e5b1838c807bb04f402437df8ef7e1e

[12] [Online] Available: http://www.delivery.acm.org/10.1145/1600000/1597820/p9deng.pdf?ip=203.129.220.149&CFID=39257849&CFTOKEN=22823083&__acm__=1314077257_0250ffb426d4391121f40d59710b3b59

13] [Online] Available: http://www.ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1414417