Journal of Artificial Intelligence in Electrical Engineering, Vol. 3, No. 9, June 2014

Digital Watermarking Technology in Different Domains

Maryam Hamrahi[1], Behzad Mozaffari Tazehkand[2]
[1]Department of Electrical Engineering, Ahar Branch, Islamic Azad University, Ahar, Iran
Email: hamrahi87@yahoo.com

[2]Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran
Email: mozaffary@tabrizu.ac.ir

ABSTRACT

Due to high speed computer networks, the use of digitally formatted data has increased many folds. The digital data can be duplicated and edited with great ease which has led to a need for effective copyright protection tools. Digital Watermarking is a technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm .Digital watermarking is a well-known technique used for copy rights protection of multimedia data. A number of watermarking techniques have been proposed in literature. Digital Watermarking is the process that embeds data called a watermark into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. A variety of techniques in different domains have been suggested by different authors to achieve above mentioned conflicting requirements. All the watermarking techniques are different from each other and are used for differing applications.

KEYWORDS: Watermarking, Domain, DCT, DWT.

1. INTRODUCTION

There is then an increasing need for software that allows for protection of ownership rights, and it is in this context where watermarking techniques come to our help. Perceptible marks of ownership or authenticity have been around for centuries in the form of stamps, seals, signatures or classical watermarks, nevertheless, given current data manipulation technologies, imperceptible digital watermarks are mandatory in most applications. A digital watermark is a distinguishing piece of information that is adhered to the data that it is intended to protect, this meaning that it should be very difficult to extract or remove the watermark from the watermarked object. Since watermarking can be applied to various types of data, the imperceptibility constraint will take different forms, depending on the properties of the recipient. Every watermarking system consists at least of two different parts:

watermark embedding unit and watermark detection and extraction units. Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. Digital Watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection. Digital watermarking is a process of embedding imperceptible content protection and/or content authentication information (Watermark) into the digital content to be protected (the host media). Although the performance expected from a given watermarking system depends on the target application area robust embedding scheme and efficient detection procedure are inherently desired. In general, a watermarking system of the type we will discuss consists of an embedder and a detector, as illustrated in Figure 1.

2. CLASSIFICATION OF WATERMARKING

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows.

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking

The approach of digital watermarking has been employed to protect intellectual property of audio, images and video data [1, 2, 3, and 4]. According to the watermarking extraction process, techniques can be divided into three types:

- Non-blind schemes require both the original image and the secret key(s) for watermark embedding.
- Semi-blind schemes require the secret key(s) and the watermark bit sequence.
- Blind schemes require only the secret key(s).

Non-blind watermarking schemes require original image and secret key for watermark detection whereas semi-blind schemes require secret key and watermark bit sequence for extraction. Blind schemes need only secret keys for extraction.

3. BASIC CHARACTERS

3.1. Robustness

*Robustness refers to the ability to detect the watermark after common signal processing operations***3.2.** The watermark should not affect the quality of the original signal, thus it should be invisible/ inaudible to human eyes/ ears.

3.3. Secure and Reliable

Watermark has the unique correct signs marking everyone, and thus to achieve the purpose of copyright protection.

3.4. Low-Complexity

Low-complexity algorithms will ensure effective and timely manner to watermark embedding, detection and extraction.

3.6. Secure Hiding Place

Watermark is hidden in the contents of carrier data, not the first section, and that will prevent the destruction caused by the format change. Data payload refers to the number of bits that can be embedded in one second of the host signal.

3.7. Security Imperceptibility

The security of a watermark refers to its ability to resist hostile attacks. A hostile attack is any process specifically intended

to thwart the watermark's purpose. The types of attacks we might be concerned about fall into three broad categories:

- Unauthorized removal
- Unauthorized embedding
- Unauthorized detection

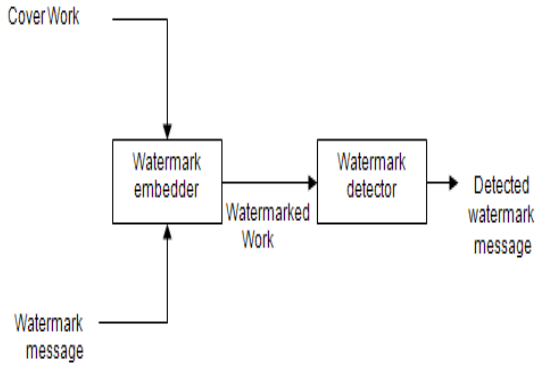

Fig.1. A generic watermarking system

4. INFORMATION HIDING TECHNIQUES

Steganography is derived from the Greek for covered writing and essentially means "to hide in plain sight". As defined by Cachin [5] steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new techniques for information hiding have become possible. This document will examine some early examples of steganography and the general principles behind its usage. There will then be a discussion of some specific techniques for hiding information in a variety of files and the attacks that may be used to bypass steganography.

Figure 2 shows how information hiding can be broken down into different areas. The other major area of steganography is copyright marking, where the message to be inserted is used to assert copyright over a document. This can be further divided into watermarking and fingerprinting which will be discussed later.

Steganography hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret. This makes steganography suitable for some tasks for which encryption aren't, such as copyright marking. Adding encrypted copyright information to a file could be easy to remove but embedding it within the contents of the file itself can prevent it being easily identified and removed. Some of them can also be found in [6, 7, 8].

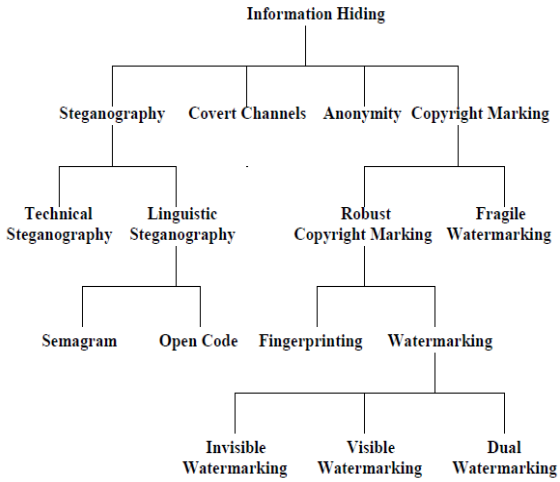

Fig.2. Information Hiding Techniques

5. WATERMARK DOMAINS

Watermarks and watermarking techniques can be divided into various categories in various ways.

5.1. Spatial Domain

In spatial domain techniques, the watermark embedding is done on image pixels. An invisible spatial domain watermarking technique was proposed by R.B.Wolfgang et al. [9]. This method is probably the easiest way of hiding

information in an image and yet it is surprisingly effective. It works by using the least significant bits of each pixel in one image to hide the most significant bits of another. LSB algorithm uses specific key and m-sequence generator to get random signals, and then arranges them into a 2-dimensional watermark signal according to a certain rules, inserts one by one into cover-images with the corresponding pixel value by the Huffman method.

5.2. Discrete Cosine Transform (DCT) domain

The character of this algorithm is robust, well hidden and resistant to a variety of signal deformation resistance .As the JPEG, MPEG and other methods of data compression are operated in the DCT transform domain, the digital watermark of DCT transform domain has inherent ability of loss compression resistance. The disadvantage is its large amount of calculation. In this domain, watermark means transforming the spatial image into the frequency domain and inserting the watermark information by changing the frequency coefficient. Of course, the transform is not necessary the whole image. This involves selecting the pixels to be modified based on the frequency of occurrence of that particular pixel. The frequency domain can overcome the greatest disadvantage of techniques operating in the spatial domain. The frequency domain watermark is less susceptible compared with the spatial domain, the LSB technique can also be applied in the frequency domain. The watermark normally applies to the lower frequency within an image, as higher frequencies are usually lost when an image is compressed or frequencies are considered to contain perceptually signification information. Frequency-based techniques result in a watermark that is dispersed throughout the image and are less susceptible to attack by cropping. [10]

5.3. Discrete Wavelet Transform (DWT) Domain

The wavelet domain method transforms both the image and watermark into the discrete wavelet domain. This method uses a multi-resolution wavelet decomposition of both the original image and the watermark. It is based on the Human Vision System. When the image is decompose by wavelet transformation, its components are separated into bands scale, much like the retina of the eye splits an image into several components. In recent years, many watermarking schemes have been developed using these popular transforms [11]. W. Zhu et al. [12] suggested an invisible watermark inserted in the wavelet coefficients. The watermark is added to every high pass wavelet coefficient and thus is visually invisible. A simple technique using wavelets to hide information is exactly like one of the techniques discussed in the previous section [13]. The Discrete wavelet transform will allow the independent processing of the resulting components much like the human eyes. The low – frequency components have to be modified in order to embed the information in a reliable and robust way. DWT has high robustness of the approach to JPG compression and additive noise and linear filtering. [14] Many other transforms had been also considered for digital watermark technique. For example, the discrete Fourier transform (DFT), the Fast Fourier Transform (FFT) and Fourier-Mellin transform and fractal transform [15].

6. CONCLUSIONS

Digital watermarking technology, closely related to information security, information hiding, cryptography and authentication technologic s, is a cutting edge research area of the international academic research in recent years. To embed a hidden robust watermark to digital multimedia is the ultimate goal of watermarking system. Generally watermarking schemes have to satisfy two conflicting requirements

a) It must not introduce any distortion in the host signal. That is watermark must be perceptually undetectable.

b) The watermark must be immune against intentional or unintentional attacks or removals.

A variety of techniques in different domains have been suggested by different authors to achieve above mentioned conflicting requirements. All the watermarking techniques are different from each other and are used for differing applications. The watermarking research is progressing very fast and numerous researchers from various fields are focusing to develop some workable scheme. Different companies also working to get commercial products.

REFERENCES

[1]W. Zhu, et al, "Multi-resolution Watermarking for Images and Video", IEEE Tran. on Circuits & Systems for Video Technology, Vol.9, No.4, June 1999, pp.545-550.

[2] Bassia P., Pitas I., and Nikolaidis 2001, "Robust Audio Watermarking in Time Domain", IEEE Trans. On Multimedia, Vol. 3, pp. 232-241.

[3] Bender W., Gruhl D., Morimoto N. and Lu A. 1996, "Techniques for Data Hiding", IBM Systems Journal, Vol. 35, No. 3&4, pp. 313- 335.

[4]J. T. Brassil, et al., "Electronic Marking and Identification Techniques to Discourage Document Copying", IEEE Journal on Selected Areas in Communications, Vol.13, No.8, Oct 1995, pp.1495-1504.

[5]C. Cachin, "An Information-Theoretic Model for Steganography", Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science, May 1998

[6]David Kahn, "Codebreakers : Story of Secret Writting", Macmillan 1967.

[7]David Kahn, "The History of Steganography", Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.1-7.

[8]F.A.P.Petitcolas, et al., "Information Hiding - A Survey", Proceedings of the IEEE, Vol.87, No.7, July 1999, pp.1062-1078

[9]R. B. Wolfgang and E. J. Delp, "A watermark for digital images," Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, Sept. 16-19, 1996, vol. 3, pp. 219-222.

[10]Neha Singh and Arnab Nandi , Digital Watermarking: mark this technology, http://www.electronicsforu.com/efylinux/efyhome/cover/watermar.pdf.

[11]Navas. K A, Sreevidya S, Sasikumar M "A benchmark for medical image watermarking", 14th International workshop on systems, signals & image processing and 6th EURASIP Conference focused on speech & image Processing, Multimedia Communication and services IWSSIP-2007 & EC-SIPMCS-2007, Maribor, Slovenia, 27-30 June 2007, pp 249-252.

[12]W.Zhu, et al, "Multi-resolution Watermarking for Images and Video",

IEEE Tran. on Circuits & Systems for Video Technology, Vol.9, No.4, June 1999, pp.545-550.

[13]C. Shoemaker, Hidden Bits: A Survey of Techniques for Digital Watermarking, http://www.vu.union.edu/~shoemakc/watermarking/watermarking.html#watermark-object, Virtual Union, 2002

[14]N.F. Johnson, S.C. Katezenbeisser, S.C. Katzenbeisser et al., Eds. Northwood, "A Survey of Steganographic Techniques" in Information Techniques for Steganography and Digital Watermarking, MA: Artec House, Dec. 1999, pp 43-75.

[15]Peter Meerwald and Andreas and Jakob-Haringer-Str. , Uhl,A survey of Wavelet-domain Watermarking Algorithms, Department of Scientific Computing ,University of Salzburg, Jakob-Haringer-Str. A-5020 Salzburg, Austria