A STUDY OF DIGITAL IMAGE WATERMARKING

Manpreet Kaur *

Sonika Jindal **

Sunny Behal **

ABSTRACT

*Watermarking is a very important field for copyrights of various electronic documents and media. With images widely available on the Internet, it may sometimes be desirable to use watermarks. Digital watermarking is the processing of combined information into a digital signal. A watermark is a secondary image, which is overlaid on the host image, and provides a means of protecting the image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Digital watermarking technique is very impressive for image authentication or protection for attacks. In this paper we aim to present a survey on different types of digital watermarks and methods to do image watermarking. Problems and challenges to produce watermarked images are also analyzed and reported***.**

Keywords: *Digital Watermark, Steganography, Authentication, Frequency Domain, Spatial Domain, Least Significant Bit.*

* Department of Computer Science and Engineering, Shaheed Bhagat Singh College of Engineering & Technology, Ferozepur, Punjab, India.

** Assistant professor, Department of Computer Science and Engineering, Shaheed Bhagat Singh College of Engineering & Technology, Ferozepur, Punjab, India.

1. INTRODUCTION

Over the past few years, there has been tremendous growth in computer networks and more specifically the World Wide Web. This phenomenon, coupled with the exponential increase of computer performance, has facilitated the distribution of multimedia data such as images. Publishers, artists, and photographers, however, may be unwilling to distribute pictures over the Internet due to a lack of security, images can be easily duplicated and distributed without the owner’s consent. Digital watermarks have been proposed as a way to tackle this tough issue. This digital signature could discourage copyright violation, and may help determine the authenticity and ownership of an image.

Digital watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity [1]. Watermarking is very similar to steganography in a number of respects. Both seek to embed information inside a cover message with little to no degradation of the cover-object. Watermarking however adds the additional requirement of robustness. An ideal steganographic system would embed a large amount of information, perfectly securely with no visible degradation to the cover object. An ideal watermarking system however would embed an amount of information that could not be removed or altered without making the cover object entirely unusable.

We can also define a watermark as the digital data embedded in multimedia objects such that the watermark can be detected or extracted at later times in order to make an assertion about the object. The main purpose of digital watermarking is to embed information imperceptibly and robustly in the host data. Typically the watermark contains information about the origin, ownership, destination, copy control, transaction etc.[2].

This paper is organized as follows. Section 2 shows the classification of image watermarking. Section 3 is focused on applications of digital image watermarking. Section 4 explains different techniques of watermarking. Section 5 describes various characteristics of image watermarking. Section 6 presents various limitations and challenges to watermarking. Section 7 represent attacks on system and section 8 represents conclusion.

2. DIGITAL IMAGE WATERMARKING CLASSIFICATION

Some of the important types of watermarking based on different watermarks [3] are given below:

2.1 Visible watermarks

Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the center part of the image.

2.2 Invisible watermark

Invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content and author authentication and for detecting unauthorized copier.

2.3 Fragile watermark

Fragile watermark are also known as tamper-proof watermarks. Such watermark are destroyed by data manipulation or in other words it is a watermarks designed to be destroyed by any form of copying or encoding other than a bit-for-bit digital copy. Absence of the watermark indicates that a copy has been made.

3. APPLICATIONS OF DIGITAL IMAGE WATERMARKING

There are various watermarking applications for images, as listed below [4] [5]:

3.1 Fingerprints

The fingerprint embeds information about the legal receiver in the image. This involves embedding a different watermark into each distributed image and allows the owner to locate and monitor pirated images that are illegally obtained. Associating unique information about each distributed copy of digital content is called fingerprinting, and watermarking is an appropriate solution for that application because it is invisible and inseparable from the content[6].Prevention of unauthorized copying is accomplished by embedding information about how often an image can be legally copied [7].

3.2 Image and content authentication

In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. Digital signature essentially represents some kind of summary of the content. If any part of the content is modified, its summary, the signature, will change making it possible to detect that some kind of tampering has taken place. One example of digital signature technology being used for image authentication is the trustworthy digital camera [8].

3.3 Medical applications

Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster [9].

4. CLASSIFICATION OF IMAGE WATERMARKING TECHNIQUES

The frequency sensitivity refers to the eye's response to spatial, spectral, or time frequency changes. Spatial frequencies are perceived as patterns or textures, and spatial frequency sensitivity is usually described as the eye's sensitivity to luminance changes [10]. It has been shown that an eye is the most sensitive to luminance changes in the mid-range spatial frequencies, and that sensitivity decreases at lower and higher spatial frequencies. Digital image watermarking schemes mainly fall into two broad categories:

- Spatial-domain techniques.
- Frequency-domain techniques.

4.1 Spatial Domain Techniques

Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. However, the mark appears immediately when the colors are separated for printing. This renders the document useless for the printer; the watermark can be removed from the color band. This approach is used commercially for journalists to inspect digital pictures from a photo-stockhouse before buying unmarked versions.

4.1.1 Least Significant Bit(LSB)

The earliest work of digital image watermarking schemes embeds watermarks in the LSB of the pixels. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (i.e., least significant) bit, of selected pixels of the image. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. For instance, an attacker could simply randomize all LSBs, which effectively destroys the hidden information

4.1.2 SSM Modulation Based Technique

Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. This is done for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming, and to prevent detection. When applied to the context of image watermarking, SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.

4.2 Frequency Domain Techniques

Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients. For example, the HVS is more sensitive to low-frequency coefficients, and less sensitive to high-frequency coefficients. In other words, low-frequency coefficients are perceptually significant, which means alterations to those components might cause distortion to the original image. On the other hand, high-frequency coefficients are considered insignificant; thus, processing techniques, such as compression, tend to remove high-frequency coefficients aggressively. To obtain a balance between imperceptibility and robustness, most algorithms embed watermarks in the midrange frequencies.

4.2.1 Discrete Cosine Transformation (DCT)

DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image.

4.2.2 Discrete Wavelet Transformation (DWT)

The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well [11]. One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well [12]. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image [13]. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies [14].

5. CHARACTERISTICS OF WATERMARKING

There are many characteristics [15] [16] that watermarking hold are as follows:

5.1 Invisibility

An embedded watermark is not visible. Invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content or author authentication and for detecting unauthorized copier.

5.2 Robustness

Piracy attacks or image processing should not affect the embedded watermark. Even if the visible watermark is removed (by an attack), there is the invisible one as the backup. The visible watermark is inserted into the original image while the invisible watermark is added to it. Therefore, it is a watermark within a watermark creating a dual watermarked image. This is another method of developing robust watermarking techniques. For robustness we can also add watermark at more than one position in the image, if one or two are removed then the other is there.

5.3 Security

A watermark should be secret and must be undetectable by an unauthorized user in general. A watermark should only be accessible by authorized parties. This requirement is regarded as a security and the watermark is usually achieved by the use of cryptographic keys. As information security techniques, the details of a digital watermark algorithm must be published to everyone. A particular watermark signal is related with a special number used embedding and extracting. The special number is kept secretly and is used for confirming legal owners of digital products later. If we lay strong stress on robustness, and then invisibility may be weak. Therefore, developing robustness watermark with invisibility is an important issue.

6. CHALLENGES AND LIMITATIONS OF DIGITAL IMGAE WATERMARKING

Watermarking research has many technical challenges. The robustness and imperceptibility trade-off makes the research quite interesting. To attain imperceptibility, the watermark should be added to the high frequency components of the original signal. On the other hand, for robustness the watermark can be added to the low frequency components only. Thus, the watermarking scheme can be successful if the low frequency components of the original signal are used as the host for watermark insertion. In this section, we discuss the various technical issues related to watermarking, such as properties of the human visual system and spread-spectrum communication, which are commonly exploited for making watermarking schemes successful.

6.1 Properties of visual signal

Since image and videos are visual signals, it is necessary to understand the behavior of visual signals in order to find ways to hide additional information in them. Visual signals are generally recognized as amplitude plots, intensity versus space displays of image information and intensity versus space and time displays of video scenes. These waveforms reveal a lot of information about the properties of the signals. Some of the properties of visual signals are listed below:

6.1.1 Nonstationarity

Nonstationarity property is common to all signals. Image and video signals contain a wealth of segments of flat or slowly changing intensity, as well as edges and textured regions. While the edges need to be preserved to maintain perceptual quality, the textured regions need to be judiciously used to store additional information

6.1.2 Periodicity

There exists line to line and frame to frame periodicity in image and video signals. They are not exactly periodic but there exists redundancy between frames and lines. These redundancies are exploited in any compression scheme, and need to be considered during the watermarking process.

6.2 Properties of the Human Visual System (HVS)

The success of any watermarking scheme lies in making the best use of the human visual system (HVS). In this section, we discuss the various properties of the human visual system which are exploited in designing watermarking algorithms.

6.2.1 Texture Sensitivity

The visibility of distortion depends on the background texture. The distortion visibility is low when the background has a strong texture. In a highly textured image block, energy tends to be more evenly distributed among the different DCT coefficients. In a flat-featured portion of the image the energy is concentrated in the low frequency components of the spectrum. This indicates that in strong texture regions more watermark signal can be added.

6.2.2 Brightness Sensitivity

The human eye is sensitive in perceiving a low intensity signal in the presence of backgrounds of different intensity. As the surrounding region intensity is increased, the relative intensity in dark areas is reduced and the sensitivity in the light areas is increased. When the mean value of the noise square is the same as that of the background, the noise square tends to be most visible against a mid-grey background. This characteristic is known as Weber’s law. This means that the eye has high sensitivity at low intensity levels and greatly reduced sensitivity at high intensity levels.

7. ATTACKS ON WATERMARKING SYSTEM

A watermarked object is likely to be subjected to certain manipulative processes before it reaches the receiver. Common signal processing functions such as analog-to-digital conversion, digital-to-analog conversion, sampling, quantization, requantization, recompression, linear and nonlinear filtering, low-pass and high-pass filtering, addition of Gaussian and non Gaussian noise are common manipulations. An attack is any processing that impairs or misleads the watermark detector. The performance of a watermarking algorithm against these attacks reflects its quality. Similarly, it is anticipated that an embedded system realization of watermarking can face several physical attacks similar to the ones suggested for cryptography. The requirements for fulfilling desired characteristics and the requirements for performance against attacks are mutually conflicting. There are many watermarking algorithms proposed and metrics has been developed for their comparison so that the user can make a decision to use one of the algorithms that best suits his need.

7.1 Attacks

We discuss various possible intentional and unintentional attacks that a watermarked object is likely to be subjected to. We classify the attacks into four different types, such as removal and interference attacks, geometric attacks, cryptographic attacks, and protocol attacks. Besides these four types, there is another class of attacks called estimation based attacks. In estimation based attacks, estimates of either the watermark data or the original object can be obtained using stochastic methods. The estimation based attacks can be classified as removal, protocol, or desynchronization depending on the way the estimate is used [17].

7.1.1 Removal and interference attacks

Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal. Moreover, interference attacks are those which add additional noise to the watermarked object. Lossy compression, quantization, collusion, denoising, remodulation, averaging, and noise storm are some examples of this category of attacks. The collusion attack occurs when a number of authorized recipients of the multimedia object come together to generate an un-watermarked object by averaging all the different watermarked objects

7.1.2 Geometric attacks

Geometric attacks are specific to images and videos. Geometric attacks do not actually remove the watermark, but manipulate the watermarked object in such a way that the detector cannot find the watermark data. This type of attack includes affine transformations such as rotation, translation, and scaling. Warping, line/column removal and cropping are also included in this family of attacks. Another example of geometric attack is the mosaic attack. In the mosaic attack, the watermarked image is divided into several parts and rearranged using proper HTML code, thus constructing a water-marked image in which the watermark detector will fail to provide desired results. Local pixel jittering is an efficient spatial domain geometric attack.

7.1.3 Cryptographic attacks

The above two type of attacks, removal and geometric, do not breach the security of the watermarking algorithm. On the other hand, cryptographic attacks deal with the cracking of the security. For example, finding the secret watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack [18]. In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography.

7.1.4 Protocol attacks

The protocol attacks exploit the loopholes in the watermarking concept. One example of such attack is the IBM attack [10]. The IBM attack is also known as the deadlock attack, inversion attack, or fake–original attack. This attack embeds one or several additional watermarks such that it is unclear which the watermark of the original owner was. Watermarking of an already watermarked image is called re-watermarking. In some inversion attacks, a fake original object is created that produces the same results through the detector as that of the real original object.

8. CONCLUSION

The purpose of this paper is to present a survey of digital image watermarking approaches. The comprehensive review of literature made has uncovered various aspects of Digital Image watermarking. It is concluded that digital watermarking technique is very impressive for image authentication and for protection against attacks.

REFERENCES

1. Literature Survey on Digital Image Watermarking Er-Hsien Fu EE381K-Multidimensional Signal Processing 8/19/98.
2. I. J. Cox and M. L. Miller, *"Electronic watermarking: the first years"*. Fourth, IEEE Workshop on Multimedia Signal Processing, 2001, pp. 225-230.
3. F. A. P. Petitcolas, R.J. Anderson, R. J. and M. G. Kuhn," Information hiding - A survey," Proceedings of the IEEE, Volume 87, Issue 7, 1999, pages 1062-1078.
4. F. Hartung and M. Kutter,Stefan Katzenbeisser and FabienA. P. Petitcolas, editors, Information Hiding Techniques for Steganography and Digital watermarking , Artech House, 2000 [6] .
5. Juergen Seitz, Digital Watermarking for Digital Media,Information Science Publishing, 2005.
6. Elias Kougianos , Saraju P. Mohanty , Rabi N. Mahapatra "Hardware assisted watermarking for multimedia" Computers and Electrical Engineering 35 (2009) 339–358.
7. Keshav S Rawat et. al. / Indian Journal of Computer Science and Engineering Digital watermarking scheme for authorization against copying or piracy of color image volume. 1 No. 4 295-300.
8. Edin Muharemagic and Borko Furht "a survey of watermarking techniques and applications" 2001.
9. G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE'a review of digital image watermarking in health care'.

10. Friedman, *G.L.*, “The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image,” IEEE Transaction on Consumer Electronics, Vol. 39, No. 4, November 1993, pp. 905-910.
11. Evelyn Brannock, Michael Weeks, Robert Harrison, Computer Science Department Georgia State University “Watermarking with Wavelets: Simplicity Leads to Robustness”, Southeastcon, IEEE, pages 587 – 592, 3-6 April 2008.
12. D. Kundur, D. Hatzinakos, Digital Watermarking for Telltale Tamper Proofing and Authentication, in proceeding of the IEEE, (1999),pp. 1167-1180.
13. G. Bouridane. A, M. K. Ibrahim, Digital Image Watermarking Using Balanced Multi wavelets, IEEE Transaction on Signal Processing 54(4), (2006), pp. 1519-1536.
14. Cox, I.J.; Miller, M.L.; Bloom, J.A., “Digital Watermarking,” Morgan Kaufmann,2001.
15. Ming-Shing Hsieh, Din-Chang Tseng, Member, IEEE, and Yong-Huai Huang “Hiding Digital Watermarks Using Multi resolution Wavelet Transform”, IEEE Transactions on Industrial Electronics, Volume 48, Issue 5, pages 875-882, Oct. 2001.
16. Sin-Joo Lee, Sung-Hwan Jung, “A Survey of watermarking techniques applied to multimedia”, IEEE Transactions on Industrial Electronics, Volume 1, pages 272-277, 2001.
17. Edin Muharemagic and Borko Furht “Survey Of Watermarking Techniques And Applications”.
18. G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE’a review of digital image watermarking in health care’.