DIGITAL WATERMARKING SCHEMES FOR AUTHORIZATION AGAINST COPYING OR PIRACY OF COLOR IMAGES

Keshav S Rawat, *Member, IEEE,* **Dheerendra S Tomar**, *Member, IEEE*

Abstract

This paper presents digital watermarking methods for authorization against copying or piracy of color images. 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. This paper presents the survey on digital watermark features, its classifications and applications. Various watermarking techniques have been studied in detail in mainly three domains: spatial, frequency and statistical domain. In spatial domain, Least-Significant Bit (LSB), SSM-Modulation-Based Technique has been developed. For DCT domain, block based approach and for wavelet domain, multi-level wavelet transformation technique and CDMA based approaches has been developed. The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications. This paper also presents the various error matrices for analyses the robustness of watermarking method.

Keywords-Digital watermark, discrete wavelet transform, discrete cosine transform, robustness.

I. INTRODUCTION

Watermarking is also a sub-discipline of information hiding. The watermarking process is generally applicable to waveform type of information sources. Digital watermarking is a technique, which allows an individual to add hidden copyright notices, or other verification messages to digital audio, video or image signals and documents. Such a messages is group of bits describing information pertaining to the signal or to the author of a signal (name, place, etc). The technique takes its name from watermarking of paper or money as a security measure. Digital watermarking can be a form of stenography, in which data is hidden in the message without the end user's knowledge.

The watermarking process contains two phases- the watermark embedding and watermark recovery.

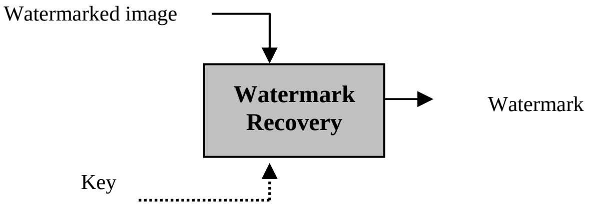

Fig.1. Watermark Embedding Scheme.

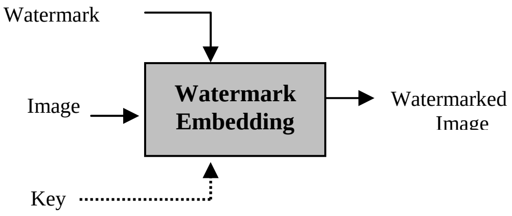

Fig.2.Watermark Recovery Scheme.

In watermark embedding phase, the watermark is embedded with image and in extraction phase, the watermark is recovered from the suspicious watermarked image. The Figure 1 shows the watermark embedding process and figure 2 shows the watermark recovery process.

II. WATERMARKING CLASSIFICATION

Some of the important types of watermarking based on different watermarks [1]-[2]-[5] 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. Further, such watermarks are protected against such as statistical analysis.

The drawbacks of visible watermarks are degrading the quality of image and detection by visual means only. Thus, it is not possible to detect them by dedicated programs or devices. Such watermarks have applications in maps, graphics and software user interface.

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 /or author authentication and for detecting unauthorized copier.

2.3. Public watermark: Such a watermark can be read or retrieved by anyone using the specialized algorithm. In this sense, public watermarks are not secure. However, public watermarks are useful for carrying IPR information. They are good alternatives to labels.

2.4. 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.

2.5. Private watermark: Private watermarks are also known as secure watermarks. To read or retrieve such a watermark, it is necessary to have the secret key.

2.6. Perceptual watermarks: A perceptual watermark exploits the aspects of human sensory system to provide invisible yet robust watermark. Such watermarks are also known as transparent watermarks that provide extremely high quality contents.

III. APPLICATIONS OF WATERMARKING

There are various watermarking applications for images, as listed below [2] [3] [4].

3.1. Copyright protection is probably the most common use of watermarks today. Copyright owner information is embedded in the image in order to prevent others from alleging ownership of the image.

3.2. 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.

3.3. Prevention of unauthorized copying is accomplished by embedding information about how often an image can be legally copied. An ironic example in which the use of a watermark might have prevented the wholesale pilfering of an image is in the ubiquitous “Lena” image, which has been used without the original owner’s permission.

3.4. 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.

3.5. 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.

IV. CHARACTERISTICS OF WATERMARKING

There are many characteristics [10] [11] that watermarking holds, some of them are as follows-

4.1. Invisibility: an embedded watermark is not visible.

4.2. Robustness: piracy attack or image processing should not affect the embedded watermark.

4.3. Readability: A watermark should convey as much information as possible. A watermark should be statistically undetectable. Moreover, retrieval of the digital watermark can be used to identify the ownership and copyright unambiguously.

4.4. 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. The owner of the intellectual property image is the only one who holds the private secret keys. 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. If we put emphasis on invisibility, then vice versa. Therefore, developing robustness watermark with invisibility is an important issue.

V. RGB TO YC_BC_R

In the watermark embedding phase, the color space of the color host image is first converted from RGB to YCbCr. The original image X is converted to the YCbCr color space. Following equation is the formula of YCbCr transformation-

$$\begin{pmatrix} Y \\ Cb \\ Cr \end{pmatrix} = \begin{pmatrix} 0.29 & 0.58 & 0.11 \\ -0.16 & -0.33 & 0.50 \\ 0.50 & -0.41 & -0.81 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix}$$

The Y component represents the luminance. The Cb and Cr components represent the chrominance. There are many kind of sampling method are available like 4:2:2 sampling and 4:1:1 sampling.

VI. IMAGE WATERMARKING TECHNIQUES

Digital image watermarking schemes mainly fall into two broad categories: Spatial-domain and Frequency-domain techniques.

6.1. Spatial Domain Techniques

Some of the Spatial Techniques of watermarking are as follow.

6.1.1. 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.

6.1.2. 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 or frequency domains. 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.

6.2. 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), Discrete Laguerre Transform (DLT) and the Discrete Hadamard Transform (DHT). 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 severe 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.

6.2.1. 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.

6.2.2. Discrete Wavelet Transformation (DWT): The Discrete Wavelet Transform (DWT) [9] 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.

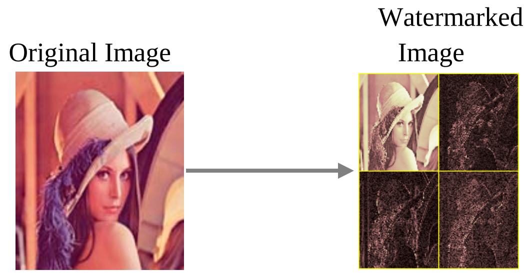

Fig.3 One Level DWT

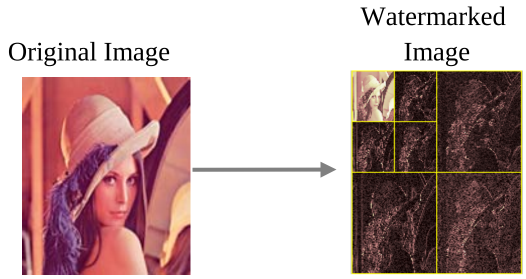

Fig.4 Two Level DWT

Watermarked

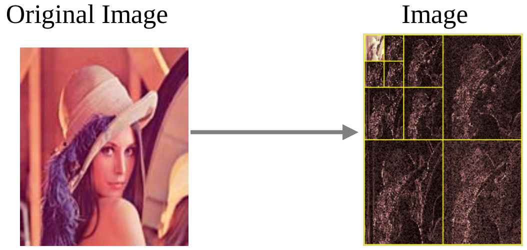

Fig.5 Three Level DWT

The Discrete Wavelet Transform (DWT)[8] 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 [6]. We use the DWT to implement a simple watermarking scheme. The 2-D discrete wavelet transforms (DWT) decomposes the image into sub-images, 3 details and 1 approximation. The approximation looks just like the original; only on 1/4 the scale. The 2-D DWT is an application of the 1-D DWT in both the horizontal and the vertical directions. The DWT separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The low-pass and high-pass filters of the wavelet transform naturally break a signal into similar (low pass) and discontinuous/rapidly-changing (high-pass) sub-signals. The slow changing aspects of a signal are preserved in the channel with the low-pass filter and the quickly changing parts are kept in the high-pass filter's channel. Therefore we can embed high-energy watermarks in the regions that human vision is less sensitive to, such as the high-resolution detail bands (LH, HL, and HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality [7]. The fact that the DWT is a multi-scale analysis can be used to the watermarking algorithm's benefit.

VII. ANALYSIS OF ROBUSTNESS

The similarity measurement between original watermark and extracted watermark is obtained through Normalized Correlation (NC) coefficient and Accuracy Rate (AR).

7.1. Normalized Correlation (NC): The Normalized correlation Coordinate (NCC) computes the similarity measurement of original watermark and extracted watermark, which is defined as

$$NC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} W(i,j) * W'(i,j)}{\sum_{i=1}^{N} \sum_{j=1}^{N} W^2(i,j)}$$

Where N×N is the size of watermark, W(i,j) and W'(i,j) represents the watermark and recovered watermark images respectively.

7.2. Accuracy Rate (AR): The Accuracy Rate (AR) is used to measure the difference between the original watermark and the recovered one. *AR* is computes as follows:

$$AR= CP/ NP$$

Where *NP* is the number of pixels in the original watermark and *CP* is the number of correct pixels obtained by comparing the pixels of the original watermark to the corresponding ones of the recovered watermark.

VIII. CONCLUSION

The digital watermarking technique is very impressive for image authentication or protection for attacks. The frequency domain technique are good for applications where exact watermark need to be extracted and channel do not consists any noise. The robustness is the very important requirements of digital watermarking. So that improving the robustness in a watermarking is may be decreasing the imperceptibility, and vice versa.

REFERENCES

[1] 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.

[2] F. Hartung and M. Kutter, “Multimedia watermarking techniques,“ Proceedings of the IEEE, Volume 87, Issue7, 1999, pages 1079-1107.

[3] F. Hartung and M. Kutter, Stefan Katzenbeisser and FabienA. P. Petitcolas, editors, Information Hiding Techniques for Steganography and Digital watermarking,Artech House, 2000.

[4] Juergen Seitz, Digital Watermarking for Digital Media,Information Science Publishing, 2005.

[5]http://www.networkmagazineindia.com/200108/security1.htm.

[6] Michael Weeks, Digital Signal Processing Using MATLAB and Wavelets, Infinity Science Press, 2006.

[7] G. Langelaar, I. Setyawan, and R. L. Lagendijk, “Watermarking Digital Image and Video Data,” IEEE Signal Processing Magazine, Number 17, September 2000,pages 20-43.

[8] Evelyn Brannock, Michael Weeks, Robert Harrison, Computer Science Department Georgia State University ” Watermarking withWavelets: Simplicity Leads to Robustness”.

[9] 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.

[10] 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.

[11] 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.