ISSN No. 0976-5697

Volume 4, No. 3, March 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

A Review on Spatial & Transform Domain Digital Watermarking Techniques

Charu Kavadia
M.Tech. Scholar, Dept. of Computer Science &
Engg. Arya College of Engineering & IT
Jaipur, India
charukavadia@gmail.com

Arpita Lodha
M.Tech. Scholar, Dept. of Computer Science &
Engg. Arya College of Engineering & IT
Jaipur, India
lodhaarpi2803@gmail.com

Abstract: This paper presents a review on different Domain digital watermarking techniques and their properties. The watermarking is a method of embedding objects into cover image for authentication of image. The important challenge during watermarking is to minimize the distortion in cover image while maintaining the security of watermark against attacks. Presently two main methods are available for watermarking one is spatial domain and other is transformed domain, both methods have their relative advantages and disadvantages and should be selected according to the application specific requirements. This paper presents generalized reviews of both techniques.

Keywords: Watermarking, Spatial Domain Processing, Transform Domain Processing.

I. INTRODUCTION

The enormous popularity of the World Wide Web in the early 1990's demonstrated the commercial potential of offering multimedia resources through the digital networks. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights. Digital watermarking has been proposed as one way to accomplish this. A digital watermark is a digital signal or pattern inserted into a digital image. Since this signal or pattern is present in each unaltered copy of the original image, the digital watermark may also serve as a digital signature for the copies. A given watermark may be unique to each copy (e.g. to identify the intended recipient), or be common to multiple copies (e.g. to identify the document source). In either case, the watermarking of the document involves the transformation of the original into another form. This distinguishes digital watermarking from digital fingerprinting, where the original file remains intact and a new created file 'describes' the original file's content.

Digital watermarking is also to be contrasted with public-key encryption, which also transform original files into another form. It is a common practice nowadays to encrypt digital documents so that they become un-viewable without the decryption key. Unlike encryption, however, digital watermarking leaves the original image (or file) basically intact and recognizable. In addition, digital watermarks, as signatures, may not be validated without special software. Further, decrypted documents are free of any residual effects of encryption, whereas digital watermarks are designed to be persistent in viewing, printing, or subsequent re-transmission or dissemination [1].

II. PRINCIPLE OF WATERMARKING

A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself. Figure 1 shows the basic block diagram of watermarking process [3].

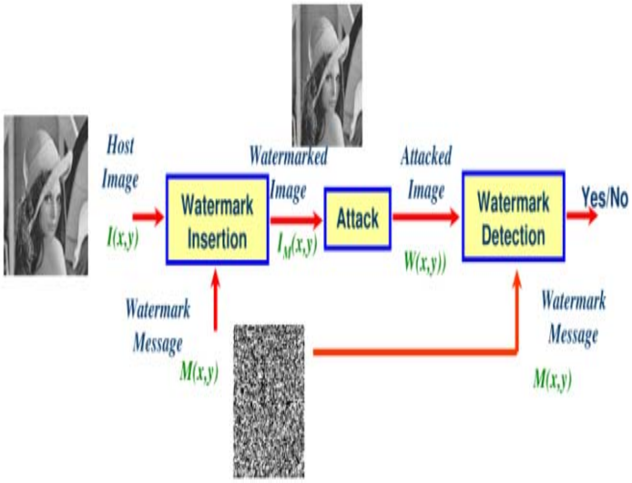

Figure 1: A general watermarking system

CONFERENCE PAPER
II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark.

III. SPATIAL & TRANSFORM DOMAIN WATERMARKING SCHEMES

The watermarking schemes where watermark is added by modifying pixel values of host image is called spatial domain method & in transform domain the watermark is inserted into transformed coefficients of image.

A. Spatial Domain Techniques:

a. Lsb Based Schemes:

One of the simplest technique in digital watermarking is in spatial domain using the two dimensional array of pixels in the container image to hold hidden data using the least significant bits (LSB) method. Note that the human eyes are not very attuned to small variance in color and therefore processing of small difference in the LSB will not noticeable. Since it relies on modifications of the least significant bits, the watermark is easily destroyed. Further, this method is restricted to images, in that it seeks to insert the watermark into image regions that lie on the edge of contours [5].

b. Patch Work Based Schemes:

Another, well known spatial domain based scheme is patchwork-based technique. Patchwork randomly chooses pairs of image points, and increases the brightness at one point by one unit while correspondingly decreasing the brightness of another point. The second method is called “texture block coding” wherein a region of random texture pattern found in the image is copied to an area of the image with similar texture. Autocorrelation is then used to recover each texture region. The most significant problem with this scheme is that it is only appropriate for images that possess large areas of random texture. The scheme could not be used on images of text [7].

c. Correlation Based Watermarking Schemes:

The most straightforward way to add a watermark to an image in the spatial domain is to add a pseudorandom noise pattern to the luminance values of its pixels. This technique exploits the correlation properties of additive pseudo-random noise patterns as applied to an image. A Pseudo-random Noise (PN) pattern is added to the cover image. To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image is computed. If the correlation exceeds a certain threshold T, the watermark is detected [4].

d. Cdma Based Image Watermarking Scheme:

Rather than determining the values of the watermark from “blocks” in the spatial domain, we can employ CDMA spread-spectrum schemes to scatter each of the bits randomly throughout the cover image, thus increasing capacity and improving resistance to cropping. The watermark is first formatted as a long string rather than a 2D image. For each value of the watermark, a PN sequence is generated using an independent seed. These seeds could either be stored or themselves generated through PN methods. The summation of all of these PN sequences represents the watermark, which is then scaled and added to the cover image. To detect the watermark, each seed is used to generate its PN sequence which is then correlated with the entire image. If the correlation is high, that bit in the watermark is set to “1”, otherwise a “0”. The process is then repeated for all the values of the watermark. CDMA improves on the robustness of the watermark significantly but it requires more computation [6].

B. Transformed Domain Based Schemes:

a. Dft Based Watermarking Schemes:

In these algorithms we modify the DFT magnitude and phase coefficients to embed watermarks. It has been shown that phase based watermarking is robust against image contrast operation. There are many variance are also available in this method where some uses log-polar coordinate system for an image. This scheme is robust against geometrical attacks. Some proposed a scheme to insert watermark by directly modifying the mid frequency bands of the DFT magnitude component.

b. Dct Based Watermarking Schemes:

DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Global DCT approach is used to embed a robust watermark in the perceptually significant portion of the Human Visual System (HVS). 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. In spatial domain it represents the LSB [2].

However in the frequency domain it represents the high frequency components. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they have minimized they avoid the most visual important parts of the image (low frequency) without over-exposing themselves to removal through compression and noise attacks.

c. Dwt Based Watermarking Schemes:

The DWT is a very attractive transform, because it can exploit the characteristics of the Human Visual System (HVS), and makes it possible to hide watermarks with more energy in an image, which makes watermarks more robust. It can be used as a computationally efficient

“Advance Computing and Creating Entrepreneurs (ACCE2013)”

version of the frequency models for the HVS [5]. For instance, it appears that the human eye is less sensitive to noise in high resolution DWT bands and in the DWT bands having an orientation of 45° (i.e., HH bands). Furthermore, DWT image and video coding, such as embedded zero-tree wavelet (EZW) coding, are included in the upcoming image and video compression standards, such as JPEG2000. Thus DWT decomposition can be exploited to make a real-time watermark application. A large number of algorithms operating in the wavelet domain have been proposed till date.

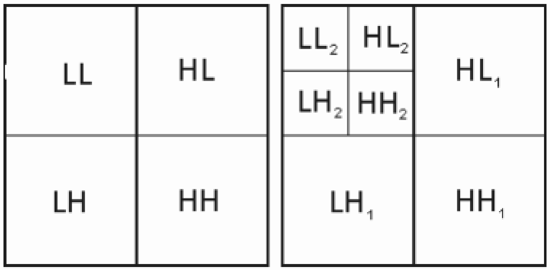

Figure 2: 1-Scale and 2-Scale 2-Dimensional Discrete Wavelet Transform.

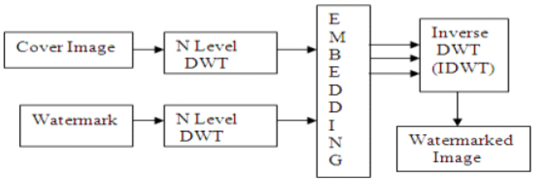

Figure 3: Generalized DWT based Watermarking Scheme

IV. CONCLUSION

The paper describes some of the most commonly spatial and transformed domain approaches used for digital watermarking. The conclusion about the schemes can be drawn on the basis of explanations of techniques given in previous chapters that the spatial domain techniques are much easier and required less computational resources but these techniques are not immune to different attacks on the other hand transformed domain methods provides much robust watermarking on the additional computational cost. Hence the selection of techniques is fully depends upon the applications and the resources available.

V. REFERENCES

[1] Mahmoud El-Gayyar Instructor Prof. Dr. Joachim von zur Gathen Media Informatics University of Bonn Germany May 06.

[2] J.Samuel Manoharan, Dr.Kezi C.Vijila & A.Sathesh "Performance Analysis of Spatial and Frequency Domain Multiple Data Embedding Techniques towards Geometric Attacks", International Journal of Security (IJS), Volume (4) : Issue (3).

[3] Darshana Mistry "Comparison of Digital Water Marking methods", International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 2905-2909.

[4] Keshav S Rawat, Dheerendra S Tomar "Digital Watermarking Schemes For Authorization Against Copying or Piracy of Color Images", Indian Journal of Computer Science and Engineering Vol. 1 No. 4 295-300.

[5] Sviatoslav Voloshynovskiy, F. Deguillaume, Shelby Pereira and Thierry Pun "Optimal adaptive diversity watermarking with channel state estimation" University of Geneva - CUI, 24 rue du General Dufour, CH 1211, Geneva 4, Switzerland.

[6] B Surekha, Dr GN Swamy "A Spatial Domain Public Image Watermarking"International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011.

[7] Wu, X., Hu, J., Gu, Z. and Huang, J "A secure semi fragile watermarking for image authentication based on integer wavelet transform with parameters" Conferences in Research and Practice in Information Technology Series; Vol. 108, 2005.

[8] Ho, C.K. and Li, C.T. Semifragile watermarking scheme for authentication of JPEG images. Proceeding of the IEEE international Conference on Information Technology: Coding and Computing, I, Pp. 7 – 11 2004.

[9] Parthasarathy, A.K. and Kak. S.,"An Improved Method of Content Based Image Watermarking", IEEE Transactions On Broadcasting, Vol. 53, No. 2, Pp.468-479.(2007)

CONFERENCE PAPER
II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India