JISEAT
ISSN: 2454-9606

JISEAT Journals for International Shodh in Engineering and Technology

Journals for International Shodh in Engineering and Technology
Website: http://jiseat.com (Volume 01, Issue 07, June 2016)

A Review on Digital Image Watermarking Approaches

Mukesh Rathore
M. Tech. Scholar
Acropolis Institute of Technology & Research,
Indore (India)
rathore4386@gmail.com

Mukti Awad
Assistant Professor
Acropolis Institute of Technology & Research,
Indore (India)
muktiawad@acropolis.in

Abstract: **Digital watermarking is an efficient solution for the copyright protection, which inserts copy right information, the watermark into the content themselves. Ownership of the contents can be established by retrieving the inserted watermark. Apart from copyright protection, watermarking can be used for diverse applications like copy control, authentication, fingerprinting, annotations and covert communication. The essential requirements of a digital watermarking scheme are imperceptibility, invisibility, robustness against common signal processing operations as well as deliberate attacks, low embedding cost as well as high embedding rate. All these requirements are conflicting to each other and it is difficult to meet all these requirements with the highest degree of accuracy. This paper reviews about different research works on digital image watermarking.**

Keywords: **DCT, DFT, DWT, EZW, LSB, HVS, JND, JPEG2000, SVD.**

I. INTRODUCTION

Digital watermarking offers copyright protection of data. It is done by embedding additional information called digital signature or watermark into the digital contents such that it can be detected, extracted later to create a declaration about the multimedia data [1, 2]. For image watermarking, the algorithms can be considered into one of the two domains: spatial domain or transform domain [1, 2]. In Spatial domain the data is embedded directly by modifying pixel values of the host image, while transform domain schemes embed data by modifying transform domain coefficients. Algorithms used for special domain are less robust for various attacks as the changes are made at least Significant Substitution (LSB) of original data. While in the transform-domain the watermark is embedded by varying the magnitude of coefficients in a transform domain with the help of discrete cosine transform, discrete wavelet transform (DWT), and singular value decomposition (SVD) techniques [3, 4]. This provide most robust algorithm for many common attacks [5]. Here, a survey of various digital watermarking techniques is present. The algorithms are reviewed from their source of implementation and some enhancement work presented by various authors.

II. LITERATURE REVIEW

SVD Based Schemes

Ganic and Eskicioglu [6] offered SVD based digital image watermarking scheme in discrete wavelet transform (DWT) domain. The embedding is achieved by modifying the singular values of the wavelet transformed sub-bands with the singular values of the watermark image. This method is robust beside different attacks because of using all bands in embedding process, but it is a non-blind method and the transparency of the watermarked image is not good. Kapreand Joshi [7] proposed a method that is similar to above one. Moreover, they showed/asserted that modifications in all frequencies make watermarking schemes using DWT robust to a wide range of attacks. However, embedding data in high frequency band is more robust to geometric attack." So, for making more robust SVD-DWT scheme proposed in [8] is a new watermarking scheme, this approach embed the watermark in only high frequency band and progress a new hybrid Semi-blind image watermarking scheme that is unaffected to a diversity of attacks.

In recent years, wavelet based watermarking algorithms have been enhanced using optimization techniques. One of these techniques includes singular value decomposition, which is one of the most powerful numerical analysis tool used to analyze matrices. In SVD transformation, a matrix can be decomposed into three matrices that are of the similar size as original matrix. SVD transformation preserves both one-way and non-symmetric properties, usually not obtainable in DCT and DFT transformations. Wie Cao et al. established SVD in

JISEAT Journals for International Shodh in Engineering and Technology

Journals for International Shodh in Engineering and Technology
Website: http://jiseat.com (Volume 01, Issue 07, June 2016)

DT-CWT domain [9]. Using SVD in digital image processing has advantages like the size of the matrices from SVD transformation is not static and can be a square or a rectangle; singular values in a digital image are less precious if general image processing is performed and singular values cover inherent algebraic image properties. The singular values of the host image are modified to embed the watermark image by employing multiple singular functions. Watermark is embedded and extracted by adjusting value between selected coefficients and actual output trained by support vector reversion. SVD factorization is done on different non-overlapping blocks by taking wavelet transform. Watermarks are created by singular value of diverse block [10-12].

There are a few techniques in digital watermarking used to imperceptibly convey information by embedding the watermark into the cover data [13]. But, problem arises in establishing identity of owner of an object. To solve this problem, an identity is established by printing the name of the owner or logo on the objects. However, in the modern era where objects have been patented or the rights are reserved (copyright), more modern techniques are to establish the identity and leave the object untampered have come into picture [14].

According to Mandhani (2004), in contrast to printed watermarks, digital watermarking is a technique where bits of information are embedded in such a way that they are completely invisible. The problem with the traditional way of printing logos or names is that the logos or names may be easily tampered or duplicated. In digital watermarking, the actual bits are dispersed in the image in such a way that they cannot be identified and they show elasticity against attempts to remove the hidden data [13].

LSB Based Schemes

In their paper, Macq and Quisquater [15] briefly discussed the issue of watermarking digital images as part of a general survey on cryptography and digital television. The authors provided a description of a procedure to insert a watermark into the least significant bits of pixels located in the vicinity of image contours. Since it relies on modifications of the least significant bits, the watermark is easily destroyed. Further, their method is restricted to images, in that it seeks to insert the watermark into image regions that lie on the edge of contours.

Rhoads [16] described a method that adds or subtracts small random quantities from each pixel. Addition or subtraction is determined by comparing a binary mask of bits with the LSB of each pixel. If the LSB is equal to the corresponding mask bit, then the random quantity is added, otherwise it is subtracted. The watermark is subtracted by first computing the difference between the original and watermarked images and then by examining the sign of the difference, pixel by pixel, to determine if it corresponds to the original sequence of additions and subtractions. This method does not make use of perceptual relevance, but it is proposed that the high frequency noise be pre-filtered to provide some robustness to low pass filtering. This scheme does not consider the problem of collusion attacks.

Patch Work Based Schemes

Another, well known spatial domain based scheme is patchwork-based technique given by Bender et al. [17]. They described two watermarking schemes. The first is a statistical method called patchwork. 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. Other Patchwork based algorithm can be found in [18, 19].

CDMA Based Image Watermarking Scheme

Rather than determining the values of the watermark from “blocks” in the spatial domain, one 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 [20, 21]. 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.

JISEAT Journals for International Shodh in Engineering and Technology

Journals for International Shodh in Engineering and Technology
Website: http://jiseat.com (Volume 01, Issue 07, June 2016)

Transformed Domain Based Schemes

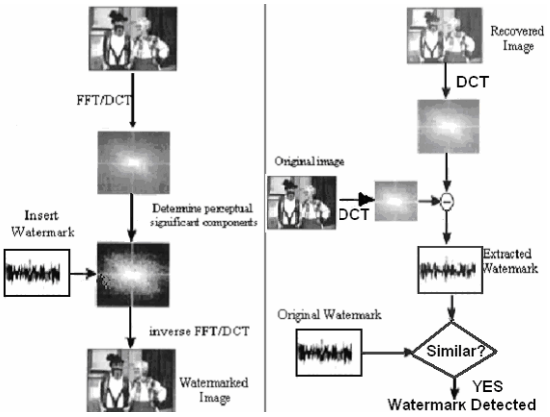

Figure 1: A General Frequency domain based watermarking model as presented by Cox [23]

As presented in literature, transformed domain based watermarking schemes are more robust as compared to simple spatial domain watermarking schemes. 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. One can use either of Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) but DCT is the most exploited one. A General transformed domain based scheme, as presented by Cox, is shown in Figure 1. A very good discussion on DCT/DWT/DFT based watermarking schemes is given in [22].

DWT Based Watermarking Schemes

If watermarking techniques can exploit the characteristics of the Human Visual System (HVS), it is possible to hide watermarks with more energy in an image, which makes watermarks more robust. From this point of view, the DWT is a very attractive transform, because it can be used as a computationally efficient version of the frequency models for the HVS [24]. 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 [25]. Thus DWT decomposition can be exploited to make a real-time watermark application.

Many approaches apply the basic schemes described at the beginning of this section to the high resolution DWT bands, LH, HH, and HL [26, 27]. A large number of algorithms operating in the wavelet domain have been proposed till date.

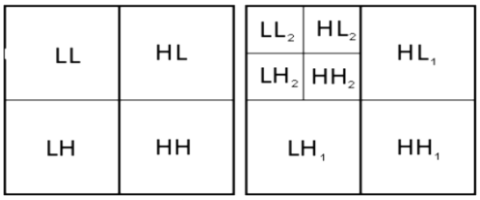

Figure 2: 1-Scale and 2-Scale 2-Dimensional Discrete Wavelet Transform

DWT Based Blind Watermark Detection

Lu et al. [28] presented a novel watermarking technique called as "Cocktail Watermarking". This technique embeds dual watermarks which complement each other. This scheme is resistant to several attacks, and no matter what type of attack is applied; one of the watermarks can be detected. Furthermore, they enhance this technique for image authentication and protection by using the wavelet based Just Noticeable Distortion (JND) values. Hence this technique achieves copyright protection as well as content authentication simultaneously. Zhu et al. [29] presented a multi-resolution watermarking scheme for watermarking video and images. The watermark is embedded in all the high pass bands in a nested manner at multiple resolutions. This scheme doesn't consider the HVS aspect; however, Kaewkamnerd and Rao [30, 31] improve this scheme by adding the HVS factor in account. Voyatzis and Pitas [32], who presented the "toral automorphism" concept, provide a technique to embed binary logo as a watermark which can be detected using visual models as well as by statistical means. So, in case the image is degraded too much and the logo is not visible, it can be detected statistically using correlation. Watermark embedding is based on a chaotic (mixing) system. Original image is not required for watermark detection. However, the watermark is embedded in spatial domain by modifying the pixel or luminance values.

A similar approach is presented for the wavelet domain [33], where the authors proposed a watermarking algorithm based on chaotic encryption. Zhao et al. [34] presented a dual domain watermarking technique for image authentication and image compression. They used the DCT domain for watermark generation and DWT domain for

JISEAT Journals for International Shodh in Engineering and Technology

Journals for International Shodh in Engineering and Technology
Website: http://jiseat.com (Volume 01, Issue 07, June 2016)

watermark insertion. A soft authentication watermark is used for tamper detection and authentication while a chrominance watermark is added to enhance compression. They use the orthogonality of DCT-DWT domain for watermarking [34].

DWT Based Non-Blind Watermark Detection

This technique requires the original image for detecting the watermark. Most of the schemes found in literature use a smaller image as a watermark and hence cannot use correlation based detectors for detecting the watermark; as a result they rely on the original image for informed detection. The size of the watermark image (normally a logo) normally is smaller compared to the host image. Xia et al. presented a wavelet based non-blind watermarking technique for still images where watermarks are added to all bands except the approximation band. A multi-resolution based approach with binary watermarks is presented here [35]. Here, both the watermark logo as well as the host image is decomposed into sub bands and later embedded. Watermark is subjectively detected by visual inspection; however, an objective detection is employed by using normalized correlation. Lu et al. presented another robust watermarking technique based on image fusion. They embedded a grayscale and binary watermark which is modulated using the "toral automorphism" described in [36]. Watermark is embedded additively. The novelty of this technique lies in the use of secret image instead of host image for watermark extraction and use of image dependent and image independent permutations to de-correlate the watermark logos [37]. Raval and Rege presented a multiple watermarking scheme. The authors argued that if the watermark is embedded in the low frequency components, it is robust against low pass filtering, lossy compression and geometric distortions. On the other hand, if the watermark is embedded in high frequency components, it is robust against contrast and brightness adjustment, gamma correction, histogram equalization and cropping and vice-versa. Thus, to achieve overall robustness against a large number of attacks, the authors proposed to embed multiple watermarks in low frequency and high frequency bands of DWT [38].

Kundur and Hatzinakos [39] presented image fusion watermarking scheme. They used salient features of the image to embed the watermark. They used a saliency measure to identify the watermark strength and later embedded the watermark additively. Normalized correlation is used to evaluate the robustness of the extracted watermark. Later the authors proposed another scheme termed as FuseMark [40] which includes minimum variance fusion for watermark extraction. Here, they propose to use a watermark image whose size is a factor of the host by 2xy. Tao and Eskicioglu presented an optimal wavelet based watermarking scheme. They embedded binary logo watermark in all the four bands. But they embedded the watermarks with variable scaling factor in different bands. The scaling factor is high for the LL sub band but for the other three bands it is lower. The quality of the extracted watermark is determined by Similarity Ratio measurement for objective calculation [41]. Ganic and Eskicioglu inspired by Raval and Rege [38] proposed a multiple watermarking scheme based on DWT and Singular Value Decomposition (SVD). They argued that the watermark embedded by Raval and Rege [38] scheme was visible in some parts of the image especially in the low frequency areas, which reduced the commercial value of the image. Hence they generalized their scheme by using all the four sub bands and embedding the watermark in SVD domain. The core technique is to decompose an image into four sub bands and then applying SVD to each band. The watermark is actually embedded by modifying the singular values from SVD [42].

III. CONCLUSION

Performing literature analysis is very important in any research project. It clearly establishes the need of the work progress. It generates related queries regarding improvements in the study already done and permits unsettled challenges to show and project. This paper discusses the previous work done against watermarking techniques. Hence evidently define all boundaries regarding the development of the research. In this paper, different techniques for digital image watermarking has been introduced which are very efficient and robust in the sense of image quality after the watermark is extracted from the image. The technique used are DCT, DFT, DWT and SVD.

REFERENCE

[1] Cox, I., Millar, M., and Bloom, J., "Digital watermarking", Morgan-Kaufmann, San Francisco, CA, ISBN: 1-55860-714-5, 2002.
[2] http://www.watermarkingworld.com, "Digital Watermarking Frequently Asked Questions", December 2004.
[3] Saraju P. Mohanty, "Watermarking of digital images", MSc thesis, Indian Institue of Science, January 1999.

JISEAT Journals for International Shodh in Engineering and Technology

Journals for International Shodh in Engineering and Technology
Website: http://jiseat.com (Volume 01, Issue 07, June 2016)

[4] Peter Meerwald, "Digital Image Watermarking in the Wavelet Transform Domain", MSc thesis in University of Salzburg, 2001.
[5] Ingemar J. Cox, Matt L. Miller, Jeffrey A. Bloom, "Watermarking applications and their properties", in International Conference on Information Technology, ITCC, pp. 6-10, 2000.
[6] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Can Invisible Watermarks Solve Rightful Ownerships?" IBM Technical Report RC 20509, IBM Research, IBM Cyberjournal, July 1996, (Online available at: http://www.research.ibm).
[7] Kruus, P., Caroline, S., Michael, H. and Mathew, M. (2002), "A Survey of Steganographic Techniques for Image Files", Advanced Security Research Journal, Network Associates Laboratories, pp.41-51.
[8] National Bureau of Standards, Data Encryption Standard (DES), US Department of Commerce. Federal Information Processing Standards Publication 46 (FIPS PUB 46), 15 January 1977.
[9] Kharrazi, M., Sencar, H. T. and Memon, N. (2004), "Image Steganography: Concepts and Practice", WSPC/Lecture Notes Series: 9in x 6in, pp.1-31
[10] Chandramouli, R. and Menon, N. (2001), "Analysis of LSB based image steganography techniques", IEEE Proceedings on Image Processing, Vol.3, pp.1019-1022.
[11] Tiwari, N. and Shandilya, M. (2010), "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format", International Journal of Computer Applications (0975 – 8887) Vol. 6, no.2, pp.1-4
[12] Deshpande, N., Kamalapur, S. and Daisy, J. (2006), "Implementation of LSB steganography and Its Evaluation for Various Bits", 1st International Conference on Digital Information Management, pp.173-178.
[13] Katzenbeisser, S. and Petitcolas, F.A.P., (2000). Information hiding techniques for steganography and digital watermarking. Artech House Publishers.
[14] Mandhani, N. K. (2004). Watermarking Using Decimal Sequences. Thesis submitted to the Graduate Faculty of the Louisiana State University, USA.
[15] Macq B.M., Quisquater J.J., "Cryptology for digital TV broadcasting", Proceedings of IEEE, ISSN: 0018-9219, vol. 83, pp. 944-957, June 1995
[16] Rhoads G.B., "Indentification/authentication coding method and apparatus", World Intellectual Property Organization, vol. IPO WO 95/14289, 1995
[17] Bender W., Gruhl D., Morimoto N., "Techniques for data hiding", Proc. SPIE, vol. 2420, page 40, Feb. 1995
[18] Weng S.W., Zhao Y., Pan J.S., "Reversible watermarking based on improved patchwork algorithm and symmetric modulo operation", Lecture Notes in Computer Science on Knowledge-based Intelligent Information and Engineering Systems, Springer, Berlin/Heidelberg, vol. 3684, 2002
[19] Yeo K., Kim H.J., "Generalized patchwork algorithm for image watermarking", Multimedia Systems, Springer, Berlin-Heidelberg, vol. 9, pp. 261-265, 2003
[20] Johnson N., Katezenbeisser S., "A Survey of Steganographic Techniques", Eds. Northwood, MA:Artec House, 43, 1999
[21] Langelaar G., Setyawan I., Lagendijk R.L., "Watermarking Digital Image and Video Data", IEEE Signal Processing Magazine, vol. 17, pp. 20-43, Sep. 2000
[22] Potdar et al., "A survey of digital image watermarking techniques", Proc. 3rd IEEE Int. Conf. on Industrial Informatics, Frontier Technologies for the Future of Industry and Business, pp. 709-716, Perth, WA, Aug. 2005
[23] Cox I.J., Kilian J., Leighton T., Shamoon T., "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997
[24] Barni M., Bartolini F., Cappellini V., Lippi A., Piva A., "A DWT-based technique for spatio-frequency masking of digital signatures", Proc. SPIE/IS&T Int. Conf. Security and Watermarking of Multimedia Contents, vol. 3657, San Jose, CA, pp. 31-39, Jan. 25-27, 1999
[25] Wikipedia-JPEG. http://www.jpeg.org
[26] Hernández J.R., Amado M., Gonzalez F.P., "DCT-Domain watermarking techniques for still images: Detector performance analysis and a new structure", IEEE Transactions of Image Processing, vol. 9, pp. 55-68, Jan. 2000
[27] Hyvarinen A., Karhunen J, Oja E., "Independent Component Analysis", Wiley- Interscience, 2001
[28] Lu C.S., Liao H.Y., Huang M., Sze S.K., "Combined Watermarking for Images Authentication and Protection", Proc. 1st IEEE Int. Conf. on Multimedia and Expo, vol. 3, no. 30, pp. 1415 – 1418, Aug. 2000
[29] Zhu X., Gao Y., Zhu Y., "Image-adaptive watermarking based on perceptually shaping watermark blockwise", Proc. ACM Symposium on Information, computer and communications Security, ASIACCS '06, pp. 175-181, Mar. 2006
[30] Kaewkamnerd N., Rao K.R., "Multiresolution based image adaptive watermarking scheme", EUSIPCO, Tampere, Finland, Sept. 2000. http://www.ee.uta.edu/dip/paperfEUSIPCO water.pdf\
[31] Kaewkamnerd N., Rao K.R., "Wavelet based image adaptive watermarking scheme", IEE Electronics Letters, vol. 36, pp. 312-313, Feb. 2000
[32] Voyatzis G. and Pitas I., "Digital Image Watermarking using Mixing Systems", Computer & Graphics, Elsevier, vol. 22, no. 4, pp. 405-416, 1998
[33] Xiao W., Ji Z., Zhang J., Wu W., "A watermarking algorithm based on chaotic encryption", Proc. IEEE Region 10 Conf. on Computers, Communications, Control and Power Engineering TENCON, vol. 1, pp. 545-548, Oct. 2002
[34] Zhao Y., Campisi P., Kundur D., "Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images", IEEE Transactions on Image Processing, vol. 13, no. 3, pp. 430-448, Mar. 2004
[35] Hsu C.T., Wu J.L., "Hidden signatures in images", Proc. ICIP-96, IEEE Int. Conf. on Image Processing, vol. 3, Lausanne, Switzerland, pp. 223-226, Sept. 16-19, 1996. http://citeseer.ist.psu.edu/mohanty99digital.htm
[36] Voyatzis G., Pitas I., "Digital Image Watermarking using Mixing Systems", Computer Graphics, Elsevier, vol. 22, no. 4, pp. 405-416, August 1998
[37] Lu C. S., Huang S.K., Sze C.J., Liao H.Y., "A new watermarking technique for multimedia protection", Multimedia Image and Video Processing, Eds. Boca Raton, FL: CRC, pp 507-530, 2001

JISEAT Journals for International Shodh in Engineering and Technology

Journals for International Shodh in Engineering and Technology
Website: http://jiseat.com (Volume 01, Issue 07, June 2016)

[38] Raval M.S., Rege P.P., "Discrete Wavelet Transform Based Multiple Watermarking Scheme", Proc. Int. Conf. on Convergent Technologies for Asia-Pacific Region, TENCON 2003, vol. 3, pp. 935 - 938, Oct. 2003

[39] Kundur D., Hatzinakos D., "A robust digital image watermarking scheme using wavelet-based fusion", Proc. ICIP 97, IEEE Int. Conf. on Image Processing, Santa Barbara, CA, pp. 544-547, Oct. 1997

[40] Kundur D., Hatzinakos D., "Towards Robust Logo Watermarking using Multi-resolution Image Fusion", IEEE Transactions on Multimedia, vol. 6, no. 1, pp. 185-198, Feb. 2004

[41] Tao P., Eskicioglu A.M., "A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain", Symposium on Internet Multimedia Management Systems V, Philadelphia, PA, pp. 134-144, 2004

[42] Ganic E., Eskicioglu A. M., "Robust digital watermarking: Robust DWT-SVD domain image watermarking: embedding data in all frequencies", Proc. of the 2004 multimedia and security workshop on Multimedia and Security, pp. 166-174, Sep. 2004