Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review Paper of Different Techniques on Digital Image Watermarking Scheme for Robustness

Komal Tomar
M.Tech (CSE) DIT University,
Dehradun, Uttarakhand, India

Abstract— ***Digital watermarking technique is becoming more important in this developing society of internet. Digital watermarking is used to protect the information against the illegal distribution in the form of images, videos and audios. Digital watermark techniques are used in various areas such as copyright protection, broadcast monitoring and owner identification. Digital image watermarking technique is the process of embedding watermark in the form of image that contain the special information and then it detect and extract that special information. The robustness, copyright protection, fidelity, capacity and some more are essential requirements of watermarking schemes so that they can handle several types of attacks. This paper reviews different aspects and techniques of digital image watermarking and different Walsh Coding Algorithm.***

Keywords— Digital Image Watermarking, Discrete Cosine Transform, Discrete Wavelet Transform, Discrete Fourier Transform, Walsh Coding Algorithm

I. INTRODUCTION

Digital watermarking is the embedding or hiding of information within a digital file without noticeably altering the file itself. Now digital image watermarking is increasing attention due to the fast developing in the internet traffic. Digital watermarking achieved is popularity due to its significance in content authentication and copyright protection for digital multimedia data. It is inserted invisible in host image so that it can be extracted at later times for the evidence of rightful ownership [1]. Various digital watermarking techniques are purposed for copyright protection of multimedia data from being misused [2, 3]. Watermarking is the process of embedding data into a multimedia element such as an image, audio or video file for the purpose of authentication. This embedded data can be later extracted or detected the multimedia data for security purposes. A watermark is information about origin, ownership and copy control. This information is embedded in multimedia content with take care of imperceptibility and robustness. General block diagram of watermarking is shown in Fig.1.

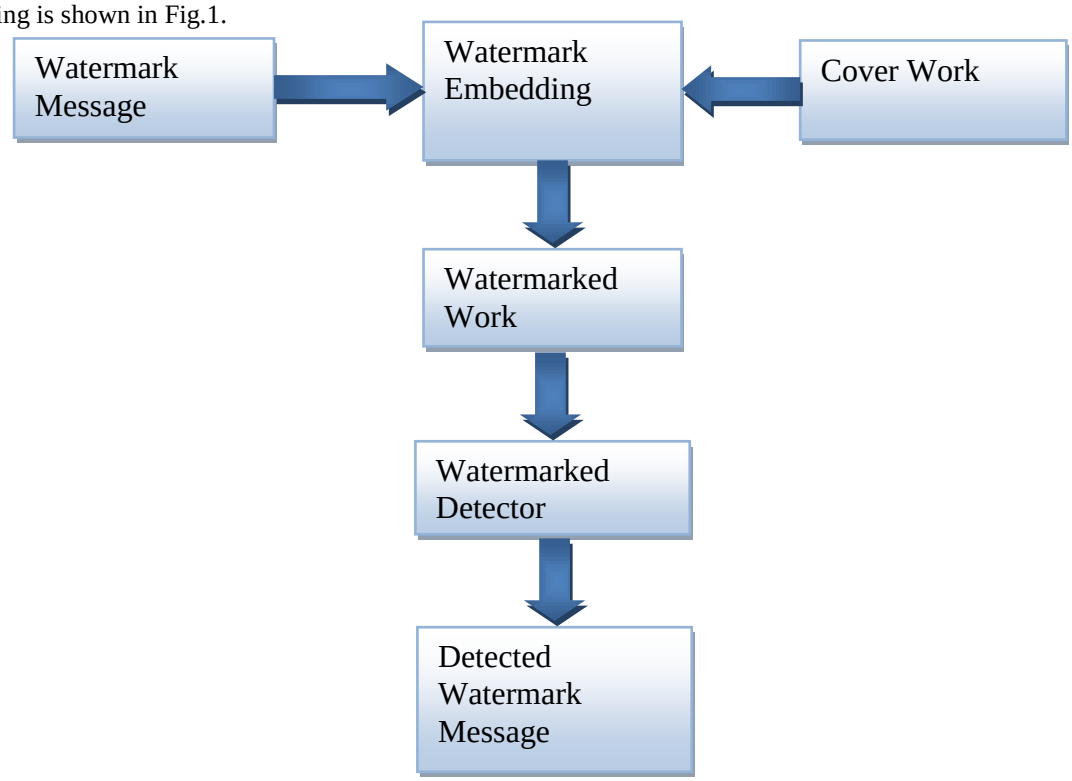

Figure 1: The Watermarked Embedding and Detection Process

According to the embedding domain of the host image, digital image watermarking techniques can be categorized into one of the two domains via spatial and transform. The simplest technique in the spatial domain methods is to insert the watermark image pixels in the least significant bits (LSB) of the host image pixels [4]. In capacity of data hiding is high in these methods but hardly robust. Watermarking in transform domain is more secure and robust to various attacks. In Frequency domain, watermark is not added to the image intensities or pixels, but to the values of its transform coefficients. Then to get the watermarked image, one should perform the transform inversely. It includes DCT (Digital Cosine Transform), DFT (Digital Fourier Transform), and DWT (Digital Wavelet Transform).

This paper is organized into five sections. Section I explains the basic introduction for watermark. Section II explains Different Digital Watermarking schemes .Section III focuses on aspects of image watermarking and Section IV explains different applications of image watermarking techniques.

II. DIGITAL WATERMARKING SCHEMES

Watermarking schemes can be classified as follows:

1) Spatial Domain: The watermarking system directly alters the main data elements (like pixels in an image) to hide the watermark data.

2) Transformed Domain: The watermarking system alters the frequency transforms of data elements to hide the watermark data. This has proved to be more robust than the spatial domain watermarking.

A. Spatial Domain Based Watermarking Schemes

I. LSB Based Schemes

In their paper, Macq and Quisquater [5] 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.

B. Transformed Domain Based Schemes

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. We can use either of Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) but DCT is the most exploited one.

1. DFT Based Watermarking Schemes

We start from DFT. There are few algorithms that modify these DFT magnitude and phase coefficients to embed watermarks. Ruanaidh et al. proposed a DFT watermarking scheme in which watermark is embedded by modifying the phase information within the DFT. It has been shown that phase based watermarking is robust against image contrast operation [6].

2. DWT Based Watermarking Schemes

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image [7]. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets. Wavelet transform provides both frequency and spatial domain of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet. This section analyses suitability of DWT for image watermarking and gives advantages of using DWT as against other transforms. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1and HH1 represent the fine-scale of DWT coefficients. To obtain the next scale of wavelet coefficients, the sub-band LL1 is further processed until some final scale N is reached. When N is reached we will have 3N+1 sub-bands consisting of the multi-resolution sub-bands LLN and LHx, HLx and HHx where x ranges from 1 until N. Due to its excellent spatiofrequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively[7].

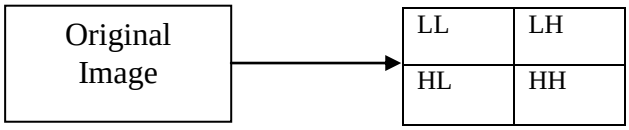

Figure 2: DWT Decomposition of Image Using 1-Level Pyramid

3. DCT Based Watermarking Schemes

Cox et al. [8] used DCT based spread spectrum communication for multimedia watermarking. This method has become very popular and has been used by many researchers. In this method, a set of independent and identically distributed Gaussian random sequences are embedded in the most perceptually significant frequencies of an image. As in spread

spectrum communication the signal energy in any frequency is undetectable if the narrow band signal is transmitted over broader bandwidth. That will cause a watermark to spread over all frequencies so that energy in any single frequency is very small. The Cox method is an incomplete method. Thus, it requires the original image in the extraction process.

We list the algorithm steps purpose by V.M. Potdar, S.Han and E. Chang [9]:

Segment the image into non-overlapping blocks of 8 x 8.

- Apply forward DCT to each of these blocks.
- Apply some block selection criteria.
- Apply coefficient selection criteria.
- Embed watermark by modifying the selected coefficients.
- Apply inverse DCT transform on each block.

The technique proposed by R. Mehul and R. Priti [10] provide the watermark is inserted in four different frequency ranges by selecting coefficients in zigzag order. This technique produced good results when attacks are applied but failed to achieve robustness to both compression and image processing tasks simultaneously when only one copy of watermark is inserted.

Sun et al. [11] presented an algorithm for embedding a watermark in the AC coefficients of the host image. In this technique, the embedding is achieved in an additive way by transferring the original image to the DCT form and their coefficients are statistically modelled by symmetric alpha-stable distributions. The algorithm is blind and the original image is not required.

Betancourth et al. [12] presented another watermarking scheme for embedding binary digits in the DCT blocks of the host image. The algorithm uses the middle and low frequency components for embedding. The algorithm is non-blind and the original image is needed for watermark extraction. The method has been tested against some attacks such as: cropping, JPEG, and rotation.

Ding et al. [13] presented an algorithm to embed watermark data into the DCT middle frequency coefficients. To enhance robustness and imperceptibility, the 256 × 256 test image is divided into 8 × 8 blocks and the components are modified. The method uses a Hamming code for error correction. The watermarking algorithm has been tested with most of the image processing attacks and proved its robustness.

Ridzon et al. [14] introduced a digital watermarking to embed part of the image inside the DCT blocks using the AC coefficients values excluding the DC components. The technique is implemented on colour images by using the YCbCr colour model instead of the RGB. There is a drawback in this method in that the watermarked image has some distortion.

Xiao et al [15] proposed a method of semi-fragile watermarking using DCT coefficients. The algorithm uses the zigzag order. The host image is divided to sub blocks of 8 × 8 and the watermark is embedded using the AC coefficients including the DC component. The method was tested on grey scale images and results show robustness against JPEG attacks.

Amrollahzadeh et al. [16] proposed a digital watermarking algorithm to use the DCT by utilizing very low frequencies for embedding. In this method, the grey scale image is subdivided into pixel blocks of size 8 × 8. Then after taking the DCT, the embedding technique uses the odd and even method. The algorithm is blind and does not require the original image. The method is robust and was assessed using several attacks.

C. Other Watermarking Technique

Walsh functions Algorithms

One dimensional and two dimensional Walsh functions have been used for watermarking in digital images. Falkowski et al. [17] proposed a watermark algorithm for embedding in 256 × 256 grey scale images. In this method, the cover image is divided into 8 × 8 blocks and the lowest frequency band is used for embedding. The scheme is non-blind and based on the multi-resolution and two dimensional complex Hadamard transforms.

The same authors [18] introduced two dimensional multi-resolutions Hadmard Transform which has been used for grey scale image watermarking. The image is segmented into 8 × 8 blocks and the algorithm utilizes the low frequency band for embedding. In the extraction process the original image is required to retrieve the watermark, so the method is non-blind.

Kountchev et al [19] proposed an algorithm uses a Complex Hadamard Transform (CHT) for embedding watermarks in digital images. A 100 × 100 logo image was used as the watermark to be embedded in a 512 × 512 cover image utilizing the low frequency area. The technique is blind and is required the original image in the extraction.

Rao et al. [20] proposed a digital image watermarking using Hadmard Transforms and an object oriented approach. In this method, a 2D Hadmard Transform is applied on the 16 × 16 watermark image. The 256 × 256 cover image is converted to the frequency domain to use the middle and high frequency of the AC components for embedding.

Marjuni et al [21] presented an algorithm used a WHT combined with the DCT. In the embedding process, the original image is divided into 8 × 8 blocks and the DCT applied. The 64 × 64 watermark was used for embedding. The experimental results show that the proposed algorithm was robust against several attacks, such as cropping, noise, and compression attacks.

Wassermann et al. [22] proposed a digital watermarking algorithm based on DCT domain and images of 2D Hadamard Transform. In the scheme the original image undergoes permuted before it is divided into blocks and the DCT is applied. The 64 × 64 watermark is coded by 2D Hadamard Transform. Then the DCT coefficients are selected for embedding. The watermarked image is obtained by applying the IDCT and inverse the permutation. The presented scheme uses a

grey scale image of size 512 × 512. The NC is utilized for testing the quality of the extracted watermarks. The PSNR also applied to compare between the original and the watermarked images. The resulted PSNR value ranging from 36.5 dB to 42.2 db.

Parameters used in Image watermarking:

- **PSNR (Peak Signal to Noise Ratio):** To measure the quality of a watermarked image, the peak signal to noise ratio is used.

$$PSNR = 10.\log_{10} (MAX^2{}_1 / MSE) \quad [23]$$

- **SNR (Signal to Noise Ratio) :** It measures the sensitivity of the images. It measures the signal strength relative to the background noise.

$$SNR_{db} = 10\log_{10} (P_{signal} / P_{noise}) \quad [24]$$

III. ASPECTS OF DIGITAL IMAGE WATERMARKING

Digital watermarking has many applications according to the type of the watermark and the used technique. Watermarking systems can be divided by number of properties that are fidelity, data payload, blind detection, false positive rate, capacity, robustness, security, watermark keys, cost, sensitivity and scalability. Some of them are common to more practical applications. These properties are discussed due to their importance in watermarking applications. Some properties are:

1) **Fidelity:** The watermarking process should not distort the original image to ensure its commercial value.
2) **Transparency:** Transparency is perceptual similarity between the original and the watermarked versions of the cover work. The digital watermark should not affect the quality of the original image after it is watermarked.
3) **Robustness:** Robustness is the ability to detect the watermark after common signal processing operations. Watermark should be robust against variety of geometrical and non-geometrical attacks.
4) **Capacity:** This property describes how much data should be embedded as a watermark to successfully detect during extraction.

IV. APPLICATION OF DIGITAL IMAGE WATERMARKING

In this section we present the review of some common applications

1) **Broadcasting Monitoring:** This type of monitoring is used to confirm the content that is supposed to be transmitted [26], [27] and [25]. As an example, commercial advertisements could be monitored through their watermarks to confirm timing and count.
2) **Fingerprinting:** A watermarked object contains information about the owner permissions. Several fingerprints can be hosted in the same image since the object could belong to several users [27], [25].
3) **Publication Monitoring and Copy Control:** The watermark contains owner data and specifies the corresponding amount of copies allowed. This presupposes hardware and software able to update the watermark at every use [27]. It also allows copy tracking of unauthorized distribution since owner data is recorded in the watermark.
4) **Temper Detection:** Fragile watermarks are used for tamper detection. If the watermark is destroyed or degraded , it indicates presence of tampering and hence digital content cannot be trusted [28].
5) **Medical Application:** Name 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 [29].
6) **Copyright Protection:** It gives the kind of allowance for the owner to embed such information that relates to him/her for the purpose of preventing those without official authorization from asserting such copyright.

V. CONCLUSIONS

This study discusses a number of techniques for the watermarking of digital images, also focus on the limitations and promises of each. LSB substitution does not provide robustness therefore it is not very efficient approach for digital watermarking. DCT domain watermarking proved to be highly considerable amounts of random noise. In this paper, we have reviewed some recent algorithms, proposed a classification based on their intrinsic features, inserting methods and extraction forms. In this paper we also have presented a review of the significant techniques in existence for watermarking those which are employed in copyright protection. Along with these, an introduction to digital watermarking, aspects of watermarking and its applications have been presented.

ACKNOWLEDGMENT

The author thanks Deep Kumar, Assistant Professor of Computer Science and Engineering, DIT University, Dehradun for his guidance and active support during the progress of our research. Without his support and encouragement this research would have been trivial.

REFERENCES

[1] I.J.Cox, J.Kilian, T.Leighton and T.Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transaction on Image Processing, 6(12), 1673-1687, December, 1997.

[2] M.D.Swanson, M.Kobayashi and A.H.Tewfik, "Multimedia data embedding and watermarking technologies", Proc. IEEE, Vol.86, pp. 1064-1087, June 1998.

[3] S.H.Low, N.F.Maxemchuk and A.M.Lapone, "Document identification for copyright protection using centroid detection", IEEE Trans. Commun., vol.46, pp. 372-383, Mar. 1998.

[4] C.I.Podilchuk and E.J.Delp, "Digital Watermarking: Algorithms and Applications", IEEE Signal Processing Magazine, pp.33-46, July 2001.

[5] Macq B.M., Quisquater J.J., "Cryptology for digital TV broadcasting", Proceedings of IEEE, ISSN: 0018-9219, vol. 83, pp. 944-957, June 1995.

[6] Wolfgang R.B., Delp E.J., "A watermarking technique for digital imagery: Further studies", Proc. Int. Conf. on. Imaging Science, Systems and Technology, Las Vegas, NV, vol. 3, pp. 112-118, June 1997.

[7] Chaturvedi Navnidhi and Basha S.J, "Comparison of Digital Image watermarking methods DWT and DWT-DCT on the basis of PSNR," International Journal of Innovative Research in Science, Engineering and Technology(IJIRSET), ISSN: 2319-8753, Vol. 1, Issue 2, December 2012.

[8] Christian R., Dugelay J.L., "A Survey of Watermarking Algorithms for Image Authentication", EURASIP Journal on Applied Signal Processing, Volume 2002, Issue 6, pp. 613-621, 2002.

[9] V.M. Potdar, S.Han and E.Chang, "A survey of digital image watermarking techniques", 3rd IEEE International conference on Industrial Informatics, pp. 709-716, 2005.

[10] R. Mehul and R.Priti, "Discrete Wavelet Transform Based Multiple Watermarking Scheme", Proceeding of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 14-17, 2003.

[11] Hyvarinen A., Oja E., "A fast fixed-point algorithm for independent component analysis", Neural Computation, 9(7), pp. 1483-1492, 1997.

[12] Johnson N., Katezenbeisser S., "A Survey of Steganographic Techniques", Eds. Northwood, MA:Artec House, 43, 1999.

[13]] 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

[14] Kim W., Lee S.H., Jang H.W., Kim J., "Multi-bits Fingerprinting for Image", SIP 2003, pp 152-155, 2003. http://www.actapress.com/PaperInfo.aspx?PaperID=15683

[15] Koch E., Zhao J., "Towards robust and hidden image copyright labeling", Proc. IEEE Workshop on Non-Linear Signal and Image Processing, Neos Marmaras, Thessaloniki, Greece, pp. 452-455, June 1995.

[16] Koch E., Zhao J., "Towards robust and hidden image copyright labeling", IEEE Int. Workshop on Non- Linear Signal and Image Processing, Neos Marmaras, Greece, pp. 452-455, June 1995.

[17] B. J. Falkowski, and Lip-San Lim, Image Watermarking Using the Complex Hadamard Transform, IEEE International Symposium on Circuits and Systems, Geneva, Switzerland, 2000, Vol.4, pp. 573-576

[18] B.J. Falkowski and Lip-San Lim, Image watermarking using Hadamard Transforms, Electronic Letter, 2000, Vol.36, pp. 211-213

[19] R. Kountchev, S. Rubin, M. Milanova, V. Todorov, R. Kountcheva, Resistant Image Watermarking in the Phases of the Complex Hadamard Transform Coefficients, IEEE International Conference on information Reuse and Integration, 2010, pp. 159-164

[20] C. S. Rao, K. V. S. Murthy, V. M. Gupta, G. V. P. Raju, S. V. Raju, A. Balakrishna, Implementation of Object Oriented Approach for Copyright Protection Using Hadamard, IEEE, Transforms, International Conference on Computer and Communication Technology, ICCCT, 2010, pp. 473-480

[21] A. Marjuni, R. Logeswaran, M. F. Ahmad Fauzi, An Image Watermarking Scheme based on FWHT-DCT, IEEE International Conference on Networking and Information Technology, 2010, pp. 289-293

[22] J. Wassermann, A. Dziech, New robust watermarking embedding scheme based on combination of basis images of 2D Hadmard Transform and Quantization Index Modulation, Recent Researches in Communications and Computers, pp78-82

[23] Ali Musrat, Ahn Chang Wook, Pant Millie, "An Optimized watermarking Technique based on DE in DWT-SVD Domain," IEEE Symposium on Differential Evolution, pp. 99-104, 2013.

[24] Kaur Gurpreet and Kaur Kamaljeet, "Image Watermarking Using LSB(Least Significant Bit)," International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), ISSN : 2277 128X, Vol. 3, Issue. 4, April 2013.

[25] V.M. Potdar, S.Han and E.Chang, "A survey of digital image watermarking techniques", 3rd IEEE International conference on Industrial Informatics, pp. 709-716, 2005.

[26] I.J.Cox, M.L. Miller, J.A.Bloom,J.Fridrich, and T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, 2008.

[27] J.Liu and X.He, "A review study on digital watermarking", 1st International Conference on Information and Communication Technologies, pp. 337-341, 2005.

[28] J. Fridrich, "Image watermaking for tamper detection", in Proc. IEEE International Conference Image Processing, Chicago, IL, Oct. 1998, pp. 404-408.

[29] G. Coatrieux, L. Lecornu, Member, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member IEEE, "a review of digital image watermarking health care"

