Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Visible and Invisible Watermarking using Discrete Wavelet Transform

Unmesh Mandal, Prof. Samir Kumar Bandyopadhyay
Department of Computer Science &Engineering
University of Calcutta, India

Abstract— This paper presents visible and invisible watermarking scheme for color images using Discrete Wavelet Transform. In the embedding process for the visible watermarking the original image is first decomposed into two levels DWT and the watermark is embedded into the second level. For the invisible watermarking scheme the original image is decomposed into four levels and then the watermark is embedded. At the extraction process the watermarked images are again decomposed into the same levels and then the original image is subtracted. The experimental results show that the proposed algorithm gives watermarked images with good visual quality.

Keywords— Digital Watermarking, Wavelet Transform, Visible Watermarking, Invisible Watermarking, Image Hiding and DFT

I. INTRODUCTION

Digital watermarking is the art and science of embedding information into media files and texts. This process is very helpful to conserve the right of the owner of the documents. These processes are being used from the ancient ages. Digital watermarking into images can be categorized into two basic domains, Special domains and Frequency Domains. The frequency techniques are considered more robust and effective than the spatial domain techniques. The main frequency transforms are Discrete Cosine Transform (DCT), Discrete Furrier Transform (DFT) and Discrete Wavelet Transform (DWT). There is a need for visible and invisible watermark to verify a document for validity. When the user gets the watermarked image from other sources, can check the authenticity of the information in the image by comparing it with the original image. The user must be able to extract the valid watermark from the watermarked image even if the watermark is invisible to the human eye. The valid extracted watermark from the watermarked image will ensure the authenticity of the document.

II. RELATED WORKS

There are multiple previous research works on Digital Watermarking. A brief description of some most recent researches are given here.

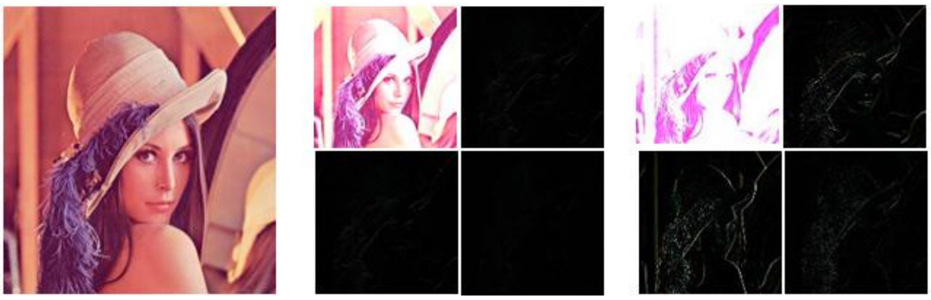
Mohananthini and Yamuna [1], in their proposed method presented a digital image watermarking based on Discrete Wavelet Transform (DWT). The watermark as well as the cover image seldom looses the quality in both embedding and extraction process. Their scheme shows good performance on different types of cover images in terms of jpeg compression. Ahmed Mahmood, Charlie Obimbo, TarfaHamed and Robert Dony [2] proposed a watermarking scheme. In which the medical image is divided into blocks and the watermark is inserted to the ROI by shifting the blocks. Their watermarking approach can survive against some watermarking attacks such cropping, and noise. A DCT blind watermarking scheme based on spread spectrum communications is proposed by Amir, Jamzad [3]. Their method preserves high PSNR for the watermarked image. The scheme also can survive some common attacks. Nisar Ahmed Memon and Gilani [4] proposed a watermarking technique to ensure the integrity of the medical image that avoids the distortion of the image in ROI by embedding the watermark information in RONI. They used patient information, hospital logo and message authentication code computed using a hash function in their watermarking scheme. Xia, Boncelet, and Arce [5] proposed two–level wavelet decomposition using the haar wavelet filters. They added the pseudo random noise codes only to the large coefficients of the high and middle frequency bands of the DWT transformed image. Rupinder Kaur [6] presented their scheme as a quality indicator of a watermarked medical image when the image is subjected to intentional operations like noise, cropping, alteration or unintentional operations like compression, transmission or filtering operations. The performance of their proposed method is evaluated by calculating MSE and PSNR of original and extracted mark. Jabade et al. [7] discussed about the importance, applications and the attributes of wavelet transform based watermarking which is widely used today. Loukhaoukha [8] proposed the security of digital watermarking scheme based on SVD and Tiny-GA. They demonstrated that their watermarking algorithm is fundamentally flawed and has a very high probability of false positive detection of watermarks. Frikken and Atallah [9] proposed a set of schemes and their analysis for multiple watermark placements that maximizes resilience to the cropping attacks on the watermarked image. Novel digital image watermarking scheme using biorthogonal wavelets are proposed by Yamuna and Sivakumar[10]. Peining Tao et al [11] generalized an idea in a recent paper that embeds a binary pattern in the form of a binary image in the LL and HH bands at the second level of Discrete Wavelet Transform (DWT) decomposition and a comparison of embedding a watermark at first and second level decompositions. Embedding the watermark in lower frequencies is robust to a group of attacks like JPEG compression, blurring, adding Gaussian noise, rescaling, rotation, cropping, pixelation, and sharpening. Embedding the watermark in higher frequencies is robust to another set of attacks like histogram equalization, intensity adjustment, and gamma correction. The watermarks extracted from all four bands are identical. Their experiments indicate that first level decomposition appear advantageous for two reasons: The area for watermark embedding is maximized, and the extracted watermarks are more textured with better visual quality. A novel image watermarking technique in the wavelet domain is suggested and tested in [12] by Sharkas, ElShafie, and Hamdy. To achieve more security and robustness, their proposed techniques relies on using two nested watermarks that are embedded into the image. A primary watermark of a PN sequence is first embedded into an image forming the secondary watermark, before being embedded into the host image. Their technique is implemented using Daubechies mother wavelets where an arbitrary embedding factor α is introduced to improve the invisibility and robustness. A multiple watermarking scheme on DWT is proposed by Mohananthini and Yamuna [13]. In the embedding process, the multiple watermarks are embedded to original image. In the extracting process, the original watermarks are retrieved from the watermarked image. Their proposed method has good imperceptibility on the watermarked image and superior in terms of Peak Signal to Noise Ratio (PSNR). Giakoumaki, Pavlopoulos, and Koutsouris [14] elaborated the perspectives of digital watermarking in a range of medical data management and distribution issues simultaneously addressed medical data protection, archiving, and retrieval, as well as source and data authentication. Woo, Du and Pham [15] proposed a multiple digital image watermarking method which is can be used to control the privacy and to detect the unauthenticated changes in medical images. Experimental result shows that the visual quality of watermarked image of their proposed scheme is very good. Mintzer and Braudaway [16] discussed three types of watermarking applications in the context of multiple watermarking and identify different ways how to employ and to interpret multiple watermarking. Mohananthini and Yamuna [17] compared single and multiple watermarking by using discrete wavelet transform and different embedding methods. In single watermarking the watermark is embedded in a host image and the multiple watermarking the watermarks is embedded one after the other. The different embedding methods are additive, multiplicative and hybrid watermarking with importance on its robustness versus the imperceptibility of the watermark. The objective quality metrics are demonstrated that, the additive embedding method achieves superior performance against watermark attacks on multiple watermarking techniques. Focusing on the way how single watermarking techniques are actually fused into multiple watermarking schemes, Sheppard, Shafavi-Naini, and Musrrat Ali et al. [18] applied differential evolution (DE) algorithm to balance the tradeoff between robustness and imperceptibility by exploring multiple scaling factors in image watermarking. The original image is partitioned into blocks and the blocks are transformed into Discrete Cosine Transform (DCT) domain. Experimental results show that their proposed scheme maintains a satisfactory image quality and watermark can still be identified from a seriously distorted image. Nasir, Weng and Jiang [19] proposed novel and robust color image watermarking unique in spatial domain based on embedding four identical watermarks into the blue component of the host image. In the extraction process, the original image is available and five watermarks can be extracted from different regions of the watermarked image and only one watermark is detected or constructed from the five watermarks according to the highest value of normalized cross correlation (NCC). The experimental results show that their proposed scheme is robust for several attacking operations including median filter, JPEG2000, JPEG-loss compression, image cropping, image scaling, rotation, rotation-scaling, rotation- cropping, randomly removal of some rows and columns lines and self-similarity. Their proposed technique is also secure, and only the one with the correct key can extract the watermark. Sheppard, Shafavi-Naini, Ogunbona [20] distinguished three main categories of multiple watermarking techniques: The first category is composite watermarking. In this method all watermarks are combined into a single watermark which is subsequently embedded in one single embedding step. The second category is successive watermarking. In which watermarks are embedded one after the other. This approach is also denoted Re-watermarking in literature. The third category is segmented watermarking. In this method the host data is partitioned into disjoint segments a priory and each watermark is embedded into its specific share.

III. PROPOSED SCHEMES

The proposed scheme uses the DWT to transform the original image into multiple levels with multiple resolutions. The embedding of the watermark image in different levels shows different amount of visibility. For example if the watermark image is embedded in two levels DWT then the watermark is visible but it is little blurred. If we decompose the original image into more levels and embed the watermark then the visibility gets reduced. When four levels of decomposition of the original image is reached then the watermark is rarely visible in the watermarked image. As the resolution of the images gets reduced in the process of decomposition into more levels the original image must be large enough, so that the resolution of the LL band from the last level of decomposition is greater than or equals to the resolution of the watermark image. Otherwise the watermark cannot be embedded into the desired level's LL band. A variable named α is used to control the visibility and the robustness of the watermark in the watermarked image.

Discrete Wavelet Transform:

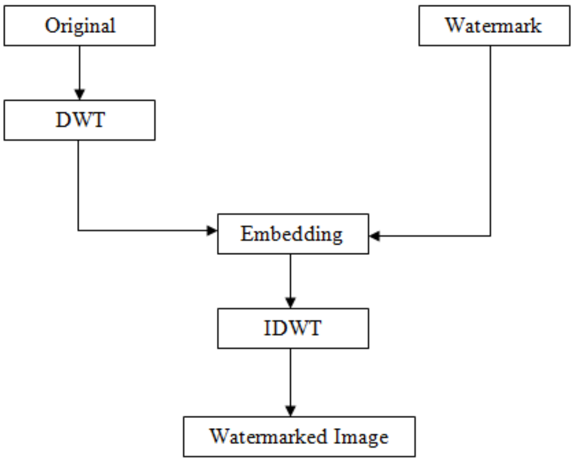
Two dimensional DWT is used to decompose the original image into multiple sub images with lower resolutions. Each level of decomposition produces four bands of data, one corresponding to Low Pass Band (LL) and other three corresponding to Horizontal (HL), Vertical (LH), and Diagonal (HH) sub bands. The Low Pass Band (LL) can be farther decomposed in each level to get multiple level of decomposition of the original image.



Original Image Level 1 Decomposition Level 2 Decomposition of LL1

Watermark Embedding Process:

In the visible watermark embedding process the original image is first decomposed into 2 level two dimensional wavelet transform. Then the watermark is embedded in the LL band from the second level of decomposition. To get the invisible watermarking the original image firstly needed to be decomposed into four levels. The watermark is embedded in the LL band from the fourth decomposition. Then Inverse Discrete Wavelet Transform (IDWT) is used to get the watermarked images.



Watermark Embedding Process

Step 1. The original image is decomposed by 2 levels (for visible water marking) and 4 levels (for invisible Watermarking) using discrete wavelet transform.

Step 2. The watermark W is applied to the color original image in LL2 and LL4 sub-bands. The watermarked image can be obtained by the following equation

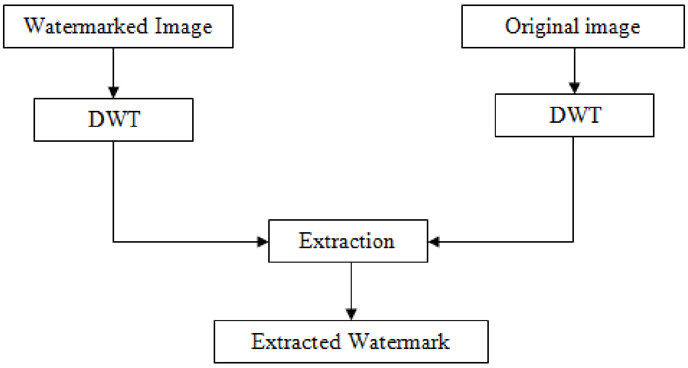
$$\mathbf{WI(I,j)=(I(I,j)+W(I,j))^{*}\alpha.}$$

Where, WI = Watermarked image,
W= Watermark,
I = original Image,
α= scaling factor.

Step 3. The inverse wavelet transforms are performed to get the watermarked images.

Watermark Extraction Process:

In the watermark extraction process the original and the watermarked image is decomposed into the same numbers of levels. For the extraction of the watermark from the visible watermarked image the number of levels is two, and for the invisible watermark the number of levels is four. Then the LL band of the original image is subtracted from the LL band of the watermarked image to get the watermark.



Watermark Extraction Process

Step 1. The watermarked image and the original image is decomposed by 2 levels and 4 levels, using discrete wavelet transform.

Step 2. The watermarks can be extracted from the watermarked image sub-bands LL2 and LL4. Then it is divided by the watermark strength factor α. This is summarized as follows,

$$\mathbf{W`(I,j)=(WI(I,j)-I(I,j))/\alpha.}$$

Where, W`= Extracted Watermark,
WI = Watermarked image,
I = original Image,
α= scaling factor.

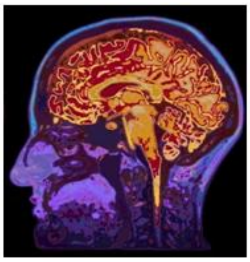
IV. EXPERIMENTAL RESULTS

The above procedure has been implemented in MTALAB, and the results are tested with one Satellite image and one medical image shown in (1) and (4) respectively. The watermark that we want to embed is shown in (7). For the original image (1) the visible watermarked image is (2) and the invisible watermarked image is at (3). For the original image (4) the visible watermarked image is (5) and the invisible watermarked image is at (6).

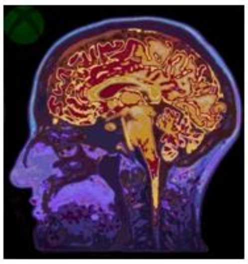
(1)
Original Image

(2)
Visible Watermarked Image

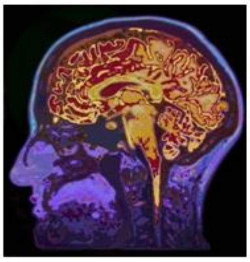
(3)
Invisible Watermarked Image



(4)
Original Image



(5)
Visible Watermarked Image



(6)
Invisible Watermarked Image

(7)
Watermark

V. CONCLUSIONS

In this paper watermark is embedded directly into the original color image and two watermarked image is created. One with the visible watermark and another with invisible watermark. The watermark can be extracted from both the watermarked images. The algorithm produces the result images as well as the extracted watermark with good visual quality. The performance of the proposed scheme is analysed by comparing with the existing schemes. As future initiative the embedding process can be done after few more level of decomposition. Then the watermark will be very difficult to find visually in the watermarked image.

REFERENCES

[1] Mohananthini. N, Yamuna. G, "A Robust Image Watermarking Scheme based Multiresolution Analysis", International Journal of Image, Graphics and Signal Processing, Vol. 4, No. 11, 2012, pp. 09-15.

[2] Ahmed Mahmood, Charlie Obimbo, TarfaHamed and Robert Dony, "Improving the Security of the Medical Images", International Journal of Advanced Computer Science and Applications, Vol. 4, No. 9, 2013

[3] Amir Hossein Taherinia, Mansour Jamzad, "A robust spread spectrum watermarking method using two levels DCT", International Journal of Electronic Security and Digital Forensics (IJESDF), Vol. 2, No. 3, 2009.

[4] Nisar Ahmed Memon& S. A.M. Gilani, "Watermarking of chest CT scan medical images for content authentication", International Journal of Computer Mathematics, Vol. 88, Issue 2, 2011, pp.265-280.

[5] X. Xia, C. Boncelet, and G. Arce, “A multiresolution watermark for digital images”, Proc. IEEE Int. Conf. Image Processing 1997(ICIP'97), Vol.1, Santa Barbara, 1997, pp. 548-551.

[6] Rupinder Kaur, “A Medical Image Watermarking Technique for Embedding EPR and Its Quality Assessment Using No-Reference Metrics”, International journal of Information Technology and Computer Science, Vol. 02, 2013, pp. 73-79.

[7] Vaishali S. Jabade and Dr. Sachin R. Gengaje, “Literature Review of Wavelet Based Digital Image Watermarking Techniques”, International Journal of Computer Applications (0975 – 8887), Vol. 31, No. 1, 2011.

[8] Khaled Loukhaoukha, “On the Security of Digital Watermarking Scheme Based on SVD and Tiny-GA”, Journal of Information Hiding and Multimedia Signal Processing, Vol. 3, No. 2, 2012, pp. 135 – 141.

[9] Keith Frikken and Mikhail Atallah, “Cropping-Resilient Segmented Multiple Watermarking”, Algorithms and Data Structures Lecture Notes in Computer Science, Vol. 2748, 2003, pp 231- 242.

[10] Yamuna Govindarajan and SivakumarDakshinamurthi, “A Novel Digital Image Watermarking Scheme Using Biorthogonal Wavelets”, ICTACT Journal on Image and Video processing, May 2011, Vol. 1, Issue 4, pp. 236-240.

[11] P. Tao and A.M. Eskicioglu, “A robust multiple watermarking scheme in the discrete wavelet transform domain, Quality of Service and Control of Next-Generation Communication Networks II”, Proceedings of the SPIE, Vol. 5601, 2004, pp. 133-144.

[12] MahaSharkas, Dahlia R. ElShafie, and NadderHamdy, “A Novel Dual-Purpose Image Watermarking Technique”, International Journal of Signal Processing, Vol. 3, No. 4, 2006.

[13] Mohananthini. N and Yamuna. G, “Color Image Multiple Watermarking Scheme based on Discrete Wavelet Transform”, IJERT - International Conference on Science, Engineering and Management (ICSEM ’13), 2013, pp 783 – 787.

[14] Giakoumaki, A, Pavlopoulos, S. and Koutsouris, D, “Multiple Image Watermarking Applied to Health Information Management”, IEEE Transactions on Information Technology in Biomedicine, Vol.10 , 2006, pp. 722 - 732. 20. C.-S. Woo, J. Du, B. Pham, “Multiple watermark method for privacy control and tamper detection in medical images”, in Proc. APRS Workshop on Digital Image Computing, Australia, 2005, pp.59-64.

[15] C.-S. Woo, J. Du, B. Pham, “Multiple watermark method for privacy control and tamper detection in medical images”, in Proc. APRS Workshop on Digital Image Computing, Australia, 2005, pp.59-64.

[16] F. Mintzer and G. W. Braudaway, “If one watermark is good, are more better?”, in Proceedings of the International Conference on Accoustics, Speech, and Signal Processing, 1999, pp. 2067–2070.

[17] Mohananthini Natarajan and Yamuna Govindarajan, “Performance Comparison of single and multiple watermarking techniques”, International Journal of Computer Network and Information Security, Vol. 6, No.7, 2014, pp. 28 - 34.

[18] Musrrat Ali, Chang WookAhn, and Millie Pant, “A robust image watermarking technique using SVD and differential evolution in DCT domain”, International Journal for Light and Electron Optics, Vol. 125, No. 1, 2014, pp. 428 - 434.

[19] Ibrahim Nasir, Ying Weng, Jianmin Jiang, “Novel Multiple Spatial Watermarking Technique in Color Images”, IEEE Fifth International Conference on Information Technology: New Generations, 2008.

[20] N. P. Sheppard, R. Shafavi-Naini, and P. Ogunbona, “On mul-tiple watermarking”, in Proceedings of the ACM Multimedia and Security Workshop (MMSW), 2001, pp. 3 - 6.

