

Enhancement of Hybrid Image Watermarking Algorithm using Human visual System Model based on Discrete Wavelet Transform

V.Sundhararaj^a, R.Prabu^{a*}, B.Meenakshipriya^{a,b}, R.Madhankumar^{a,b,c}

^{a)} Department Of Department of Mechatronics, Kongu Engineering College,
Erode, Tamilnadu, India.

^{b)} Department Of Electronics and Communication Engineering, Paavai College of Engineering,
Tamilnadu, India.

^{c)} Department Of Department of Mechatronics, Kongu Engineering College,
Erode, Tamilnadu, India.

^{d)} Department Of Electronics and Communication Engineering, Paavai College of Engineering,
Tamilnadu, India.

*Corresponding Author: V.Sundhararaj

E-mail: sundar673@gmail.com

Received: 10/11/2015, Revised: 20/12/2015 and Accepted: 22/12/2016

Abstract

Wavelet based hybrid image watermarking algorithm for copyright protection and secure of digital image is obtainable using Human Visual System (HVS) model. In the proposed watermarking algorithm, four level Discrete Wavelet Transform is applied to selected image blocks to obtain 13 sub-bands of each block and then the Human Visual System (HVS) model is also used for selection of significant coefficient for embedding the data. As a substitute of using a pseudo random sequence, a visually meaningful binary logo image is used as watermark. Watermark embedding algorithm is carried out by transforming the original image in wavelet domain. To embed the watermark imperceptible and robustly, watermark bits are added to the Wavelet coefficients of each sub band selected by considering the Human Visual System (HVS) characteristics. Experimental results show model based hybrid image watermarking scheme is robustly and imperceptible against several image compression, median filtering, cropping and sharpening. Peak Signal to Noise Ratio (PSNR) and Bit Correction Rate (BCR) both are used to measure the quality of watermarked image and extracted watermark respectively.

Keywords: Watermark embedding, watermark extraction, Wavelet transform, HVS characteristics.

**Reviewed by ICETSET'16 organizing committee*

1. Introduction

Now days an increasing the use of Internet and effortless copying, tampering and distribution of digital data, copyright protection for multimedia data has become an important issue. Digital image watermarking emerged as a tool for protecting the multimedia data from copyright infringement. Based on the domain analysis, digital watermarking is divided into two categories. They are: spatial domain and frequency domain watermarking. Spatial

domain watermarking shows less resistance but are not robust against attacks and hence called fragile watermarking. While frequency domain techniques like discrete wavelet transform (DWT).

In digital watermarking an imperceptible signal mark is embedded into the original image. It is exclusively identifies the Ownership. These watermark method should not be removable by unauthorized person and should be robust against any attacks. Watermarking techniques can be broadly classified into two categories are spatial domain methods and transform domain methods. Transform domain watermarking techniques are more robust in comparison to spatial domain methods. It is due to the fact that when image is inverse wavelet transformed watermark is distributed unevenly over the image, making the attacker difficult to read or modify. Among the transform domain watermarking techniques Discrete Wavelet Transform (DWT) based watermarking techniques are gaining more popularity because of superior modeling of HVS. A detail survey on wavelet based watermarking techniques can be found in [1] Another advantage of the wavelet domain watermarking algorithms is that security can be improved by selecting a key dependent wavelet transform as implemented in [2]. They used randomly generated orthonormal filter bank as a major part of the private key. Besides selecting the filter bank randomly, to improve the private control over the watermark, middle frequency sub bands are also selected based on the private key.

Similarly, [2] proposed to use wavelet filter parameterization as a secret transform domain to improve the security of the watermarking method. This method shows good quality robustness to geometric attacks like cropping and rotation but is sensitive to common signal processing attacks like low pass filtering and image sharpening. As pointed out by [1] and [2], by embedding visually meaningful marks like logo or seal, it can be easy for convincing non-technical arbitrators by showing the extracted logo or seal than presenting a numerical value detected using statistical watermark detection techniques. Another advantage of using logo as watermark is that HVS characteristics can be exploited in recognizing noisy visual mark since HVS filters out random noise for better recognition of meaningful pattern. Many researchers have investigated watermarking methods by embedding binary logos. [2] Showed a method for embedding seal in wavelet transform domain. In order to make the method robust to JPEG compression they quantized the wavelet coefficients depending on the quality factor before embedding watermark. A method of embedding logos in DCT domain was proposed by [3]. First they permuted the seal using pseudo-random number traversing method and added this to the middle frequency coefficient of the DCT coefficient block. Later they [3] proposed a method in which both the image and binary logo are hierarchically wavelet decomposed and detail bands of the logo are added to corresponding bands of the image. [3] Proposed a method for embedding binary logos in the Fourier domain. Before embedding the logo into the host data, they modulated the logo by adding pseudo-noise generated with a secret key. All the methods discussed above refer to binary watermark embedding only. But in many practical applications logos are gray scale images and these methods cannot be directly used for embedding them. Some authors like [3] have embedded gray scale logos by converting them into bit planes. But by converting the grayscale logos into bit planes, these methods are not exploiting the perceptual

characteristics of the logos and the host data in embedding the watermark. As pointed out by use of grayscale logo as watermark facilitates the embedding of arbitrary commercial logos and increases the quality of and overall number of possible logos identifiable by human observers. [3] Proposed a multiresolution fusion based watermarking method for embedding grayscale logos into wavelet-transformed images. For watermarking, the logo is 1-level wavelet decomposed. Each sub band of host image is divided into blocks of size equal to the size of sub band of the logo. Four sub bands of the logo that corresponds to different orientation are added to the same orientation blocks of the image. In this paper, a novel robust wavelet based grayscale logo watermarking technique is presented.

To embed the watermark robustly and imperceptibly, HVS characteristics are used in selecting the significant coefficients and adding the watermark to these coefficients. To recover the watermark from the distorted images, a method of reliable watermark extraction is presented, in which the watermark bits are extracted by taking into consideration the distortion caused by the attacks. To show the validity of the proposed method, the watermarked images are tested for different type of attacks and results are compared with the existing methods. The rest of the paper is organized as follows. The proposed watermarking method, watermarking embedding and HVS Characteristics are explained in Section 2. In Section 3, the experimental results are presented. Finally, the concluding remarks are given in Section 4.

2. Watermarking Method

Watermarking method is seen as a protected communication task consisting of two steps, watermark embedding and watermark retrieval process. In watermark embedding, the signal, i.e., the watermark, is transmitted through the host data that acts as a channel, whereas in watermark retrieval, the signal is received and extracted from the marked data. The security of the watermarking is maintained in the same way as in cryptography by using a secret key. In contrast to encrypted data, a watermarked data can still be used with the embedded watermark. The legal owner knows the exact embedding process, which is based on a secret key, and hence, can extract the watermark while it is not possible do, so for an unauthorized party.

2.1. Watermark Embedding

The proposed method embeds watermark by decomposing the host image and the watermark using wavelet transform. A visual mask based on HVS characteristics is used for calculating the weight factor for each wavelet coefficient of the host image and the significant coefficients from each subband are selected based on these weight factors. To embed the watermark in all selected wavelet coefficients, the watermark bits are repeatedly added to the selected coefficients with their corresponding weight factors. These weight factors give the maximum amount of modification that can be applied to a wavelet coefficient without any perceptual degradation. The watermark used for embedding is a gray scale logo image, which is very small compared to the size of the host image. The watermark needs to be very small in order to make it spatially localized and to make robust against attacks like

cropping and filtering. During the watermark recovery, the watermark repetitions are extracted.

2.2. HVS characteristics

A number of factors affect the noise sensitivity of the human eye like luminance, frequency band, texture and proximity to an edge. Human eye is less sensitive to the areas of the image where brightness is high or low. As observed by [2], human eye is less sensitive to noise in high frequency sub bands and bands having orientation of ± 45 . Sensitivity of human eye to noise in textured area is less and it is more near the edges. Based on these observations, developed a model for adaptively quantizing the wavelet coefficients for image compression. With some modification, [2] developed a masking function for calculating the weight factors to embed the pseudorandom binary sequence into high frequency sub bands of the host image. In our proposed method, we are using the model of [2] for calculating the weight factors for wavelet coefficients of the host image.

3. Experimental Results

The performance of the proposed Watermarking algorithm is tested on Lena gray scale image. Here the results are presented for gray scale 8-bit Lena image of size 512*512. The logo used for watermarking is an 8-bit gray scale image of size 64*64. Original Lena and logo images are shown is Fig.1a) and 1b) respectively. For 4-level wavelet decomposition Daubechies filter coefficients are used. If the original and the watermarked Lena images are observed we cannot find any perceptual degradation.



Fig. 1. a) Input Image1



b) Watermark Logo



Fig. 2 . a) Watermarked Image



b) Extracted Logo

Extracted logo from the watermarked image is shown in Fig 2b). It can be observed from Fig.2 that the

watermark bits are stored near edges and high textured regions where HVS is less sensitive. Robustness of the proposed method is evaluated for various types of image distortions.

4. Conclusion

A wavelet-based watermarking technique for digital images is presented. Watermark is embedded into the selected coefficients based on the weight factors calculated by analysis the HVS characteristics. A method for reliable watermark extraction based on the distortion in the surrounding pixels is presented. Robustness of the algorithm is tested against different type of attacks. The experimental results on test images have shown that the detection performance of the proposed based on watermark detector is superiority of the proposed method.

References

- [1] Mauro Barni, Franco Bartolini, MAY 2001 “Improved Wavelet-Based Watermarking Through Pixel-Wise Masking”IEEE TRANSACTIONS ON IMAGE PROCESSING VOL. 10, NO. 5, MAY 2001.
- [2] V. Padmanabha Reddy and Dr. S. Varadarajan, February, 2010 “An Effective Wavelet-Based Watermarking Scheme Using Human Visual System for Protecting Copyrights of Digital Images” International Journal of Computer and Electrical Engineering, Vol. 2, No. 1, February, 2010
- [3] M. MahbuburRahman, M. Omair Ahmad, AUGUST 2009 “A New Statistical Detector for DWT-Based Additive Image Watermarking Using the Gauss HermiteExpansion”IEEE TRANSACTIONS ON IMAGE PROCESSING VOL. 18, NO. 8, AUGUST 2009
- [4] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, “Perceptual watermarks for digital images and video,” Proc. IEEE, vol. 87, no. 7, pp. 1108–1126, Jul. 1999.
- [5] C. I. Podilchuk and W. Zeng, “Image-adaptive watermarking using visual models,” IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 525–539, Apr. 1998.
- [6] J. R. Hernández and F. P. González, “Statistical analysis of watermarking Schemes for copyright protection of images,” Proc. IEEE, vol. 87, no. 7, pp. 1142–1166, Jul. 1999.
- [7] C. I. Podilchuk and W. Zeng, “Image-adaptive watermarking using visual models,” IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 525–539, Apr. 1998.
- [8] M. D. Swanson, B. Zhu, and A. H. Tewfik, “Multiresolution scene-based video watermarking using perceptual models,” IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 540–550, Apr. 1998.