Simulation and Implementation Novel Hybrid Blind Method of Image Security

Anil C. Suthar[1], Chiragkumar B. Patel[2], and Gopal R. Kulkarni[3]

[1]Research Scholar, E&C Department KSV University, Gandhinagar, Gujarat, India
[2]Assistant Professor, E&C Department, L.C. Institute of Technology, Bhandu, Gujarat, India
[3]Principal, D.I.E.T., Satara, Maharashtra, India
Email: [1]acsuthar@ieee.org, [2]chiragkumar@live.com,[3]grkulkarni29264@rediffmail.com

Abstract. In this paper, we propose a novel hybrid mixed frequency domain scheme. The secret message bits are embedding on the singular values of the blocks within low frequency sub-band in host digital image. Using low-frequency approximation sub-graph transformation coefficients restore high-frequency element sub-images transformation coefficients. When detecting secure message, by comparing replaced part coefficient we can find out whether the image has been tamper. Simulation results are evidence for that the algorithm has strong detection and location capability and maintain better original image quality. To embed secure message imperceptibly, robustly and securely, we model the adaptive quantization parameters by considering the human visual system (HVS) distinctiveness. Experimental results demonstrate that the proposed scheme is robust to variety of attacks. Secure message extraction is efficient and blind in the sense only quantization strategies but not the host image is -required.

Keywords: Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Data hiding algorithm, Stenography.

1 Introduction

The development of effective digital image copyright protection methods have recently become an urgent and necessary requirement in the multimedia industry due to the ever-increasing unauthorized manipulation and reproduction of original digital objects. The new technology of digital image security has been advocated by many specialists as the best method to such multimedia copyright protection problem [5]. In general, the message-securing scheme shall satisfy two properties. First, the secure message should not influence the quality of the host media and be unnoticeable to human eyes. Second, if secure message is used for internet applications such as transmitting data through a noisy channel or compressing data, the secure message must continue to exist under those situations [1],[7].

Sathyanarayana S V (Ed.): ARTCom 2012, LNEE pp. 342–348, 2012.

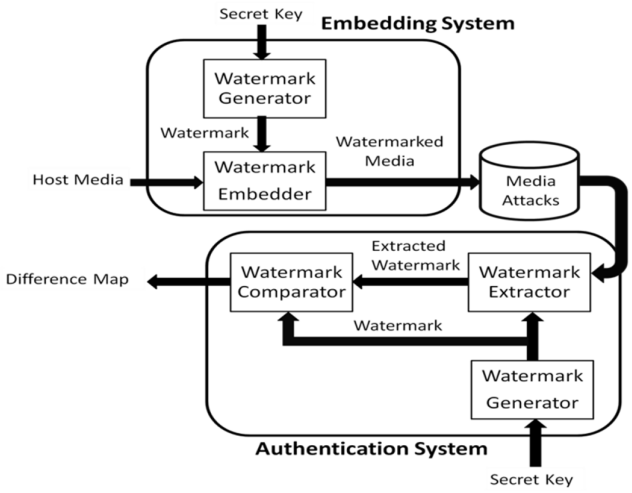

Fig. 1. Fundamentals principal of message securing

Figure 1 indicates the fundamental way to securing the image. DCT and DWT has own merits and demerits for securing the image [3], [9], [11].

2 Various Techniques to Be Used

In order for a digital image security method to be effective it should be imperceptible, and robust to common image manipulations like compression, filtering, rotation, scaling cropping, and collusion attacks among many other digital signal processing operations. Current digital image watermarking techniques can be grouped into two major classes:

1. Spatial Domain Watermarking
2. Frequency Domain Watermarking

Compared to spatial domain techniques, frequency-domain watermarking techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms. Commonly used frequency-domain transforms include the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) [3], [9], [11] and Discrete Fourier Transform (DFT). However, DWT has been used in digital image watermarking more frequently due to its excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system. Further performance improvements in DWT-based digital image watermarking algorithms could be obtained by combining DWT with DCT [3], [9], [11]. The idea of applying two transform is based on the fact that hybrid for compensate for the drawbacks of each other, resulting in effective image security [8].

2.1 Discrete Wavelet Transform

Wavelets are unique functions, which, in a form analogous to sine and cosine in Fourier analysis, are used as basal functions for representing signals. For 2-D images, applying DWT corresponds to handing out the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL1, LH1, HL1 and HH1 [7]. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub -bands LH1, HL1 and HH1 represent the fine-scale of DWT coefficients. To acquire the next coarser scale of wavelet coefficients, the sub-band LL1 is further processed until some final scale N is reached. High frequency bands are the details information at different scales different resolutions [4]. Three tree discrete wavelet transform level as shown in Fig 2.

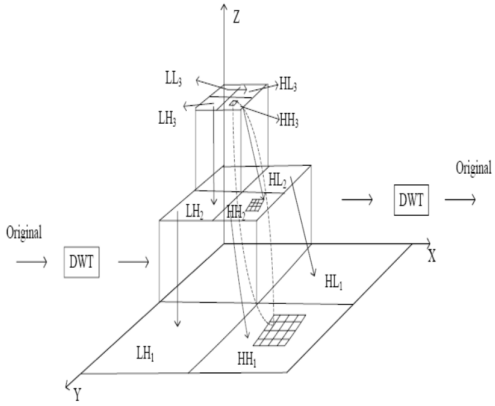

Fig. 2. Three tree discrete wavelet transforms

F_L	F_L	F_L	F_M	F_M	F_M	F_M	F_H
F_L	F_L	F_M	F_M	F_M	F_M	F_H	F_H
F_L	F_M	F_M	F_M	F_M	F_H	F_H	F_H
F_M	F_M	F_M	F_M	F_H	F_H	F_H	F_H
F_M	F_M	F_M	F_H	F_H	F_H	F_H	F_H
F_M	F_M	F_H	F_H	F_H	F_H	F_H	F_H
F_M	F_H	F_H	F_H	F_H	F_H	F_H	F_H
F_H	F_H	F_H	F_H	F_H	F_H	F_H	F_H

Fig. 3. Different regions in discrete cosine transform domain

2.2 Discrete Cosine Transform

This transform allows an image to be broken up into various frequency bands and making it easier to embed watermarking information into the middle frequency bands of an image [11]. It concentrates the information energy in the bands with low frequency, and therefore shows its popularity in image compression techniques [2], [6].

The middle frequency bands are elected such a way, they have diminished to avoid the largest visual important parts of the image without overexposing themselves to eliminate during compression and noise attacks. Different region in frequency domain shows in Fig 3. In the DCT domain image is rich in AC and DC frequency components. Through the inverse DCT transform to restore the original image. Forward DCT and inverse DCT both require complex mathematical calculations [10]. Two-dimensional forward DCT transform (FDCT) such as formula (1). Two-dimensional inverse DCT transform (IDCT) which such as formula (2).

$$F(k,l) = \alpha_k \alpha_l \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} I(m,n) \cos \frac{(2m+1)k\pi}{2M} \cos \frac{(2m+1)l\pi}{2N} \tag{1}$$

$$I(m,n) = \alpha_k \alpha_l \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} F(k,l) \cos \frac{(2m+1)k\pi}{2M} \cos \frac{(2m+1)l\pi}{2N} \tag{2}$$

$$\alpha_k = \begin{cases} 1/\sqrt{M} & k = 0 \\ \sqrt{2/M} & 1 \le k \le M-1 \end{cases} , \alpha_l = \begin{cases} 1/\sqrt{N} & l = 0 \\ \sqrt{2/N} & 1 \le l \le N-1 \end{cases}$$

For improve watermark embedding speed and security, we use DCT on the three discrete wavelet decompositions LL3 and LH3 for each of a reversible transformation. F_L is used to signify the lowest frequency components of the block, while F_H is used to signify the higher frequency components [11]. F_M is elected as the embedding section as to make available supplementary confrontation to lossy compression technique, despite the fact that avoid significant modification of the cover image. There is quite good time differentiated rate in high frequency part of signals DWT transformed. Also there is quite good frequency differentiated rate in its low frequency part.

3 Secure Image Embedding and Detecting Algorithm

3.1 Secure Image Embedding Algorithm

In Proposed algorithm, We are encrypted secreat image using key through random sequence for more security [1]. Also, we are appling a two dimension discrete wavelet transform(DWT) to original or host image. After appling DWT, we are able to use

mid frequency(band) cofficient for watermarking. Normaly in image security technique, secrete message (watermark) is embedded behind host image but in this algorithem watermark image is encrypted using key. So, we are using encrypted image in embedding algorithem. After embedding a encrypted secure image behind host image, we are appling a DCT –DWT combine method as embedding algorithm (figure 4) and detecting algorithm (figure 5) for secured image in that secreat message is invisible.

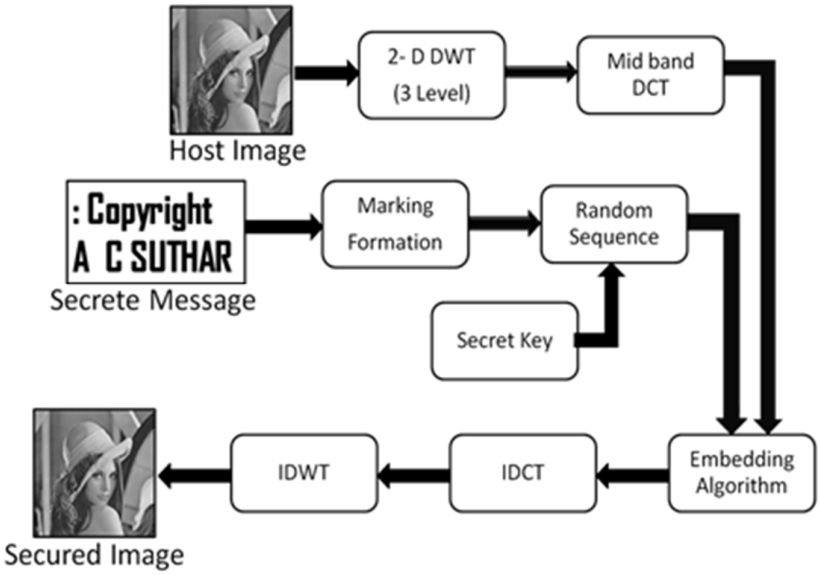

Fig. 4. Secure image embedding algorithm

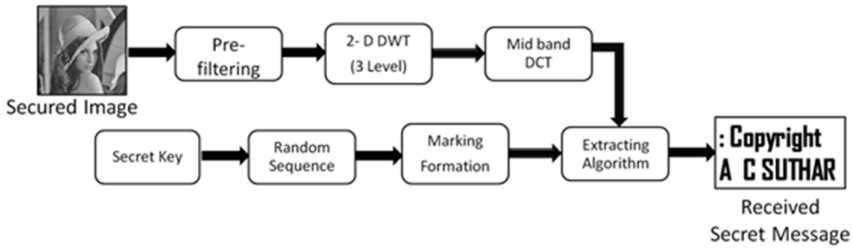

Fig 5. Secure image detecting algorithm

4 Simulation of Experiment

We are tested the performance of proposed algorithem on MATLAB. Performance of the proposed scheme is tested with grayscale lena image as host or original image whose size is 512×512 because we are comparing the performance of the proposed scheme with Mei's scheme [3] that is a similar approach of hybrid mixed frequency

domin scheme based message securing scheme. Our objective of this experiment to achieve high Power to Signal Noise Ratio (PSNR) and robutness of proposed scheme in terms of NC. The PSNR is used for measuring the visual fidelity between the host image and secured image. Also, we will compare our results of secured image after different attack with Mei's Scheme[3] for better analysis. We are achieving higher PSNR compare to Mei's Scheme.It's found that the image quality meaausred PSNR of the secured image is greater then 67dB without attack. This indicates that propsed scheme has good visual fidelity. Fig 6(b) indicates that we are achieving good robustness in each and every case for lena image.

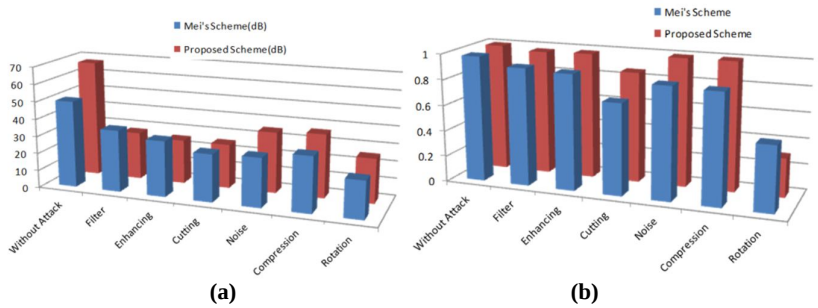

Fig. 6. Performance comparisons of proposed scheme with Mei's Scheme in terms of **(a)** Power Signal to Noise Ratio Versus different attack **(b)** robustness versus different attack

5 Conclusion

Discrete wavelet transform and discrete cosine transform algorithm are use to achieve gray scale image content integrity protection in this paper. Based on the characteristics of the image, embedding secure message, the algorithm has high security. In this paper, we propose a new secure image-hiding scheme based on human visual system in hybrid mixed frequency domain scheme. After decomposing the host image by DWT and DCT, secure message information bits are embedding into the singular values of the selected blocks within each low frequency coefficients sub-band of the host image. The experimental results show that the proposed scheme preserves not only the high perceptual quality, but also is robust against many different types of attacks. The compression security issue indicates good result compare to other security issues.

References

1. P. W. Wong., "A public key watermark for image verification and authentication", Proceedings of the IEEE, International Conference on Image Processing, Chicago, USA, 1998, 455-459
2. C. T. Li., "Digital fragile watermarking scheme for authentication of JPEG images", IEEE Proc.-Vis. Image Signal Process, Vol. 151, No. 6, December 2004

3. Mei Jiansheng, Li Sukang and Tan Xiaomei, “A Digital Watermarking Algorithm Based on DCT and DWT”, Proceedings of the 2009 International Symposium (WISA’09), 978-952-5726-00/01-8/5, © 2009 Academy Publisher, AP-PROC-CS-09CN001, May, 2009, pp.104-107
4. Donghuan Jiang, “Wavelet and partial differential equations image processing applied research”, A doctor's degree thesis, Xidian University, 2007
5. G. C. Langelaar, I. Setyawan and R. L. Lagendijk, “Watermarking digital image and video data”, IEEE Signal Processing Magazine, 2000, vol.5, no.12, pp.20-46
6. J. R. Hernández, M. Amado and F. Pérez González, “DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure”, IEEE Trans.Image Processing, 2000, vol.9, no.1, pp.55-68
7. M. Barni, F. Bartolini and A. Piva, “Improved wavelet-based watermarking through pixel-wise masking”, IEEE Trans.Image Process, 2001, vol.5, no.10, pp.783-791
8. Jing Liu, FeiGao and Hui Zhang, “A blind watermark algorithm in mixed transform domain based on chaotic sequence locating”, Proc. The 3rd International Conference on Innovative Computing Information and Control, Dalian, China, 2008, pp.23-27
9. Shao-min Zhu, Jian-ming Liu, “Adaptive Watermarking Scheme in Hybrid DWT-DCT Transform Based on Human Visual System” , 2008 International Symposium on Knowledge Acquisition and Modeling 978-0-7695-3488-6/08 $25.00 © 2008 IEEE, DOI 0.1109/KAM.2008.78, p668-671
10. A. C. Suthar, C. B. Patel, Dr. Kulkarni G. R., Dr. Shah D. J. “Implementation of Secret Information Hiding over Colour Image using Frequency Domain Technique” Proceedings of the IEEE, December 2011, 978-1-61284-693-4/11/$26.00 ©2011 IEEE,pp.614-618, ISBN:978-1-61284-766-5, IEEE catalog number:CFP1120J-PRT.
11. A. C. Suthar, C. B. Patel, Dr. Kulkarni G. R. “Implementation Of Image Security Issues Using Mixed Frequency Domain Scheme” in International Transactions on Electrical, Electronics and Communication Engineering, ISSN: 2249- 8923, November ‘11 - June ’11, Volume 1, No 5, pp.18-23.