Color Image Watermarking Using Wavelet Transform Based on HVS Channel

G. Rosline Nesa Kumari, Syama Sundar Jeeru, and S. Maruthuperumal

Godavari Institute of Engineering & Technology, Rajahmundry, India
{rosemaruthu,jeerusyam,maruthumail}@gmail.com

Abstract. Digital image watermarking is a copyright protection technology expected at asserting intellectual property rights of digital images by embedding a copyright identifier in the contents of the image, without disturbing its quality. In this paper, a new robust and secure color watermarking scheme based on Discrete Wavelet domain is proposed. The RGB color space is converted into HSV color space and the H component is decomposition with 'Haar' which is simple, symmetric and orthogonal wavelet. The proposed embedding process, the scrambled watermark is embedded in the modification of the extraordinary value of LL band and LH band of H component to the watermarking scheme which excellent preserves the quality. The supplementary improvement of the proposed technique is taking advantage of HVS which can adaptively regulate the watermark embedding strength. Experimental results show that the method not only has better transparency, but also has good robustness such as noise, compression, filtering, cropping.

1 Introduction

In modern year's Copyright protection and authentication of digital data using watermarking is a powerful issue of research. The basic principle of digital watermarking technique [5] is to embed an amount of secret information in the functional part of the cover data. This data may be an image, an audio or video. Since mid 1990s this technique has attracted much attention from academic and industrial sector. After the pioneering contribution by I. J. Cox [5], digital watermarking techniques have been widely developed as an effective tool against piracy, illegal alteration of contents or improper use of image. Digital watermarking is a method that inserts some information into a multimedia object and generates a watermarked multimedia object [6, 7]. The object may be an image, audio, video or text. Watermarking has many different applications [8, 9, 10, 11, 12], such as ownership evidence, fingerprinting, authentication and integrity verification, content labeling and protection, and usage control.

Watermarking techniques can be divided into spatial [13], [14], and frequency [15], [16], [17] based methods. Watermarking algorithms that rely on spatial domains, hide the watermark by modifying the pixel values of the host image. In transform domain technique [1,2,3,4], the host image is first converted into frequency domain by transformation method such as the discrete cosine transform (DCT), discrete

S.C. Satapathy et al. (eds.), *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of CSI - Volume I*, Advances in Intelligent Systems and Computing 248,
DOI: 10.1007/978-3-319-03107-1_7, © Springer International Publishing Switzerland 2014

Fourier transform (DFT) or discreet wavelet transform (DWT) ,etc. then, transform domain coefficients are modified by the watermark. Watermarking the process of embedding data into multimedia element can primarily for copyright protection. Because of its growing popularity, the Discrete Wavelet Transform (DWT) is commonly used in the proposed watermarking scheme increase, area increases so power consumption [18].

Human Visual System (HVS) plays important role in watermarking of images to maintain the perceptual similarity between original and watermarked image. HVS has been characterized with several phenomena that permit to adjust the pixel values to yield perception. These phenomena are luminance sensitivity, frequency sensitivity and texture sensitivity. Human visual model is based on the characteristics such as edges and textures, which are incorporated to determine the gain factor in watermarking. The distortion visibility is very low if the back ground contains texture. In a high texture block, energy is more distributed among the pixels. Therefore, the block having a stronger texture can have a high embedding gain factor. The paper also utilizes Torus automorphism (TA) permutation [19,20,21] to scramble the watermark before embedding and to reassemble it after extraction. This helps increase robustness to intentional attacks while preserving blindness. The paper also proposes an extended version of this technique to increase the robustness against intentional attacks even further. The algorithm is discussed in the rest of the paper.

This paper describes the efficient and robust color watermarking schemes in an attempt to improve watermark robustness to attacks. The proposed scheme embeds a scrambled watermark image by using Torus automorphism into a 2nd level wavelet color image of H components. Select a LL and LH subband having high energy and then embed scrambled the watermark. The proposed method is directly embedded into cover image using a transform before embedding. Experimental results demonstrate that there is high degree of perceptual similarity between original image and watermarked image. Further, the proposed method resists different types of attacks. The rest of the paper is organized as follows. Section 2 briefly reviews about DWT and Torus automorphism Section 3 describes the proposed color watermarking method and in section 4, the experimental results are discussed. Finally, some conclusions are drawn in section 5.

2 Discrete Wavelet Transformation

The Discrete Wavelet Transform (DWT) [22] is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Discrete Wavelet decomposition of image produces the multi-resolution representation of image. A multi-resolution representation provides a simple hierarchical framework for interpreting the image information. At different resolutions, the details of an image generally characterize different physical structures of the image. At a coarse resolution, these details correspond to the larger structures which provide the image context. The following section briefly reviews about Two Dimensional Wavelet Transformation. The original image I is thus represented by set of sub images at several scales;{{Ld,Dnl}ll , , ,n , , , ..., d}, which is multi-scale representation with depth d of the image I. The image is represented by two dimensional signal functions; wavelet transform decomposes the image into four frequency bands, namely, the LL_1, HL_1, LH_1 and HH_1 bands. H and L denote the highpass and lowpass filters respectively. The approximated image LL is obtained by lowpass filtering in both row and column directions. The detailed images LH, HL and HH contain the high frequency components. To obtain the next coarse level of wavelet coefficients, the sub- band LL_1 alone is further decomposed and critically sampled. Similarly LL_2 will be used to obtain further decomposition. By decomposing the approximated image at each level into four sub images forms the pyramidal image tree. This results in two-level wavelet decomposition of image as shown in the Figure 1. Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality. The fact that the DWT is a multi-scale analysis can be used to the watermarking algorithm's benefit.

Fig. 1. Layout of individual bands at second level of DWT decomposition

2.1 Torus Automorphism Permutation

To increase the robustness of the embedded watermark against intentional attacks, the proposed method use Torus automorphism (TA) permutation [19,20,21] to disarrange the watermark bits equally and randomly before embedding and reconstruct it after extraction. This scheme offers cryptographic protection against intentional attacks since the keys utilized in TA permutation (for scrambling the watermark) are also necessary in inverse TA permutation (for reconstructing the watermark after extraction). The watermark is scrambled using the following equation before it is embedded into the host image:

$$\begin{pmatrix} i^* \\ j^* \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} * \begin{pmatrix} i \\ j \end{pmatrix} \bmod \quad (1)$$

Equation (1) indicates that each bit of the watermark at location (i, j) will be moved to a new location (i*, j*). Parameter m is obtained from the size m*n of the watermark while parameter k is arbitrarily chosen by the user. Parameters m and k are secret keys needed for both the scrambling and reconstruction of the watermark. Even with TA permutation, the proposed algorithm is still blind.

3 Proposed Scheme

This paper proposed a novel strategy for DWT domain robust invisible embedding and extraction through a unique approach for creation of a compound color image to serve as the effective watermark. One of the most important features that make the recognition of images possible by humans is color. Color is a property that depends on the reflection of light to the eye and the processing of that information in the brain. Usually colors are defined in three dimensional color spaces These could be RGB (Red, Green, and Blue), HSV (Hue, Saturation, and Value) or HSB (Hue, Saturation, and Brightness). The last two are dependent on the human perception of hue, saturation, and brightness [22]. Color represents the distribution of colors within the entire image. This distribution includes the amounts of each color, but not the locations of colors. The entire process of the proposed method is represented in the Figure 2.

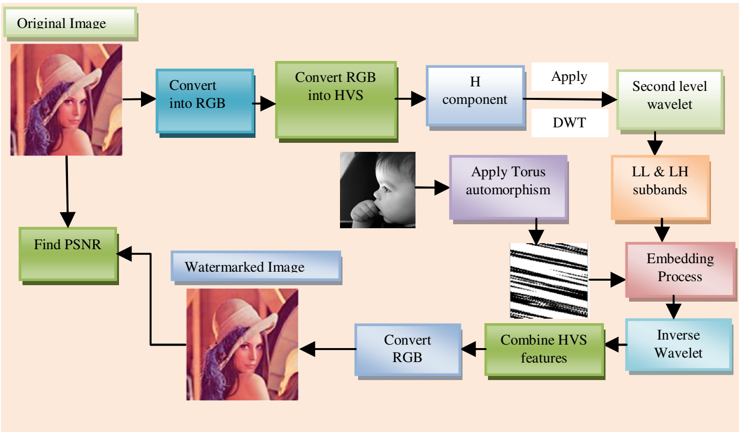

Fig. 2. Overview of Proposed Color Watermarking Scheme

3.1 Embedding Watermark Procedure

The embedding algorithm uses color image as cover and gray-scale image as watermark. The color image is decomposed into Red, Green and Blue channels. RGB color model converted into HVS plane, the proposed method is considered H channel to insert the watermark image. The 2-level DWT is applied on the Hue channel of color image, which produces the frequency subband coefficients. From these LL_2 and LH_2 subband coefficients is selected for inserting watermark. Before embedding the watermark into selected subbands, the watermark image is scrambled by using Torus automorphism, as explained in section 2.1. The scramble watermark image is split into two shares, the first share insert into LH_2 subband coefficients and second share insert into LL_2 subband coefficients. Calculate the average value of LL_2 and LH_2, and compare each and every pixel value with average value of LL_2 and LH_2. If the value is less than average value, select the pixel to insert the watermark bit in the 6^{th} LSB. Continue this procedure until the watermark bit inserted into the wavelet image. Apply inverse wavelet to obtain H component and combine HVS channels, then convert HVS into RGB to get watermarked image.

3.2 Extracting Watermark Procedure

Extraction procedure is a nature blind extraction which uses only watermarked color image as input. The watermarked color image is decomposed into Red, Green and Blue channels. RGB watermarked color model converted into Hue, Saturation, and Value channels. The DWT is applied on the Hue channel of watermarked color image, which produces the frequency subband coefficients. On this subband apply DWT to obtain the second level decomposition. The watermark is extracted from LL_2 and LH_2, subband coefficient. The retrieved watermark can be used to determine the ownership by comparing the retrieved watermark with the assigned one. As in the definition, the goals of the reversible water- marking are to protect the copyrights and can recover the original image.

4 Experimental Results and Analysis

Eight 256×256 sized cover images Lena, Tiffany, Lake, F16, Baboon, Boat, Barbara, and Goodhill are considered in the proposed method, as shown in Figure 3. A binary image “Boy” of size 64×64 is used as the watermark image as shown in Figure 4. The outcome expose that there are no detectably visual degradations on the watermarked image presented in Figure 5 with a PSNR of 43.The proposed method solemnized that there are no visual degradations on the reverenced watermarked images. For all the different original test images, the watermark is successfully extracted with unit NCC.

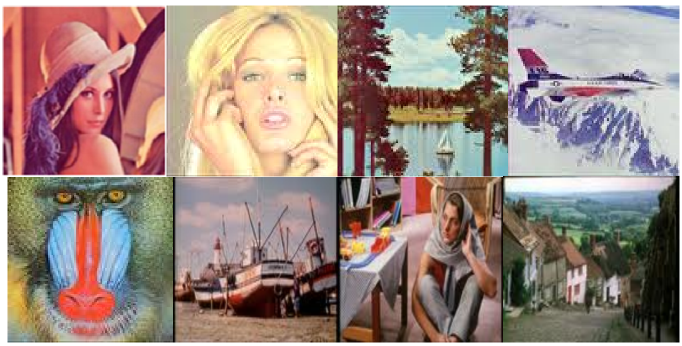

Fig. 3. Cover images Lena, Tiffany, Lake, F16, Baboon, Boat, Barbara, Goodhill

Fig. 4. Watermark images (a) Boy

We propose a new universal objective image quality index (IQI), which is easy to calculate and applicable to various image processing applications. Instead of using traditional error summation methods, the proposed index is designed by modeling any image distortion as a combination of three factors: loss of correlation, luminance distortion, and contrast distortion. Although the new index is mathematically defined and no human visual system model is explicitly employed, experiments on various image distortion types show that it exhibits surprising consistency with subjective quality measurement. It performs significantly better than the widely used distortion metric mean squared error. The structural similarity (SSIM) index is a method for measuring the similarity between two images. The SSIM index is a full reference metric, in other words, the measuring of image quality based on an initial uncompressed or distortion-free image as reference. IQI and SSIM values of the proposed method is nearer to 1, this indicating the cover images and watermarked images are identical as shown in Table 1.

To provide verification of the capability of proposed method, test the proposed scheme watermarked images with Cropping (5%, 10%,15%) , (Gaussian Blur 1px, 2px, 3px), Noise(10%, 15%, 20%), Rotate (20,40,60). The Table 2 exposes the watermark recognition results of the different attack of the Barbara image. From the results, the proposed method is expert to absolutely detect the watermark in the watermarked images. Therefore, the proposed method can represent the conclusion that the proposed method can detect perfectly the watermark from the watermarked images and it is well built robustness to the geometric and non-geometric attacks.

Table 1. Values of various parameters for proposed method

Original images	Proposed approach			
	PSNR(dB)	IQI	SSIM	NCC
Lena	43.24	0.98	0.99	0.97
Tiffany	42.57	0.99	0.97	0.98
Lake	43.98	0.97	0.98	0.99
F16	42.45	0.98	0.99	0.98
Baboon	42.10	0.97	0.97	0.97
Boat	43.07	0.99	0.98	0.998
Barbara	42.76	0.98	0.99	0.98
Goodhill	42.72	0.99	0.97	0.97

Fig. 5. Watermarked images Lena, Tiffany, Lake, F16, Baboon, Boat, Barbara, Goodhill

Table 2. Attacks for proposed method

Attacks	PSNR	NCC
Cropping 5%	34.45	0.80
Cropping 10%	32.76	0.76
Cropping 15%	27.35	0.63
Gaussian Blur 1px	30.65	0.71
Gaussian Blur 2px	28.71	0.67
Gaussian Blur 3px	24.39	0.57
Noise 10%	31.39	0.73
Noise 15%	28.65	0.67
Noise 20%	26.10	0.61
Rotate 20	30.18	0.70
Rotate 40	26.38	0.61
Rotate 60	22.16	0.51

5 Conclusions

In this paper, a Color image watermarking using Wavelet Transform based on HVS Channel has been proposed. This proposed method applies DWT in the HVS channel and embed scrambled watermark into the DWT coefficient. The frequency domain technique are good for applications where exact watermark need to be extracted and channel do not consists any noise. In the proposed color digital watermarking method, the actual bits are scattered in the image in such a way that they cannot be identified by unauthorized persons and show resilience against attempts to remove the hidden data. The proposed method tested the method for several standard test images. The quantitative measure of the extracted watermark for both gray scale and color images shows the flexibility against different attacks.

References

1. Cheng, L.M., Cheng, L.L., Chan, C.K., Ng, K.W.: Digital watermarking based on frequency random position insertion. presented at Control, Automation, Robotics and Vision Conference, vol. 2, pp. 977–982 (2004)
2. Chun-Shien, L., Shih-Kun, H., Chwen-Jye, S., Hong-Yuan Mark, L.: Cocktail watermarking for digital image protection. IEEE Transactions on Multimedia 2, 209–224 (2000)
3. Lu, W., Lu, H., Chung, F.-L.: Robust digital image watermarking based on subsampling. Applied Mathematics and Computation 181, 886–893 (2006)
4. Reddy, A.A., Chatterji, B.N.: A new wavelet based logo-watermarking scheme. Pattern Recognition Letters 26, 1019–1027 (2005)
5. Cox, I.J., Killian, J., Leighton, F.T., Shamoon, T.: Secure Spread Spectrum Watermarking for Multimedia. IEEE Trans. on Image Processing 6(12) (December 1997)
6. Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J., Su, J.: Attacks on digital watermarks: classification, estimation-based attacks and benchmarks. IEEE Commun. Mag. 39(9), 118–126 (2001)
7. Sequeira, A., Kundur, D.: Communications and information theory in watermarking: a survey. In: Proceedings of SPIE Multimedia Systems and Application IV, vol. 4518, pp. 216–227 (2001)
8. Mintzer, F., Braudaway, G., Yeung, M.: Effective and ineffective digital watermarks. In: IEEE International Conference on Image Processing (ICIP 1997), vol. 3, pp. 9–12 (1997)
9. Memon, N., Wong, P.W.: Protecting digital media content. Commun. ACM 41(7), 35–43 (1998)
10. Barnett, R.: Digital watermarking: application, techniques, and challenges. IEE Electron Commun. Eng. J., 173–183 (1999)
11. Bender, W., Butera, W., Gruhl, D., Hwang, R., Paiz, F.J., Pogreb, S.: Applications for data hiding. IBM Syst. J. 39(3-4), 547–568 (2000)
12. Zhao, J., Koch, E., Luo, C.: In business today and tomorrow. Commun. ACM 41(7), 67–72 (1998)
13. Huang, P.S., Chiang, C.S., Chang, C.P., Tu, T.M.: Robust spatial watermarking technique for colour images via direct saturation adjustment. In: IEE Proceedings. of Vision, Image and Signal Processing, vol. 152(5), pp. 561–574 (2005)
14. Verma, B., Jain, S., Agarwal, D.P., Phadikar, A.: A New color image watermarking scheme. INFOCOMP Journal of Computer Science 5(3), 37–42 (2006)
15. Xie, L., Arce, G.: Joint wavelet compression and authentication watermarking. In: IEEE International Conference on Image Processing, vol. 2, pp. 427–431 (1998)
16. Reddy, A.A., Chatterji, B.N.: A new wavelet based logo- watermarking scheme. Pattern Recognition Letters 26(7), 1019–1027 (2005)
17. Raval, M.S., Rege, P.P.: Discrete wavelet transform based multiple watermarking scheme. In: Int. Conference on Convergent Technologies for Asia-Pacific Region, vol. 3, pp. 935–938 (2003)
18. Anumol, T.J., Karthigaikumar, P.: DWT based Invisible Image Watermarking Algorithm for Color Images. In: IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, pp. 76–79 (2011)
19. Voyatzis, G., Pitas, I.: Applications of Toral Automorphisms in Image Watermarking. In: Proceedings of the Image Processing International Conference (1996)

20. Chang, C., Hsiao, J., Chiang, C.: An Image Copyright Protection Scheme Based on Torus Automorphism. In: Proceedings of the 1st International Symposium on Cyber Worlds, pp. 217–224 (2002)
21. Engedy, M., Munaga, V., Saxena, A.: A Robust Wavelet Based Digital Watermarking Scheme Using Chaotic Mixing. In: Proceedings of the 1st International Conference on Digital Information Management, pp. 36–40 (2006)
22. Hsieh, S.-L., Tsai, I.-J., Huang, B.-Y., Jian, J.-J.: Protecting Copyrights of Color Images using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform. Journal of Multimedia 3(4), 42–49 (2008)
23. Husaini, A.Z., Nizamuddin, M.: Challenges and approach for a robust image water marking algorithm. International Journal of Electronics Engineering 2(1), 229–233 (2010)