Computer Communication & Collaboration (Vol. 2, Issue 4, 2014)
ISSN 2292-1028(Print) 2292-1036(Online)
Submitted on Aug. 13, 2014
DOIC: 2292-1036-2014-04-002-38

Transparent Data Hiding for True Color Images

Majid Masoumi

Department of Electrical Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran

E-mail: masoumiii@yahoo.com (Corresponding Author)

Mahsa Rezaei

Department of Electrical Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran

E-mail: mahsa.rezaei@yahoo.com

Abstract: Recently digital watermarking turns into one of the hottest research topics in the multimedia signal processing community for its ownership confirmation purposes. In this paper a transparent data hiding for image authentication which is compatible with HVS is presented. For satisfying the security of the proposed scheme three private keys are considered. In order to meet transparency issue, the luminance layer of image is chosen for undergoing the first level of wavelet transform. So, using PRNGs the watermark is scattered into the mid-frequency sub-bands of host image. Eventually, Simulation results show the high transparency of the proposed system, while gratify the robustness against lots of attacks.

Keywords: Data hiding, Image processing, Transparency

1. Introduction

Nowadays by obsolesce of analog media, digital media can be stored, duplicated, and dispersed easily with no lost of fidelity. It is clear that documents in digital form present a lot of advantages, but they also create problems, for parties who desire to prevent unauthorized reproduction and distribution of valuable digital medium like copyrighted, commercial, sensitive, secret document. On the other hand, the simplicity of exchanging digital content over the Internet has created copyright violation issues. Copyrighted material can be easily exchanged over peer-to-peer networks, and this has caused major concerns to those content providers who produce these digital contents [1-2].

Encryptions technologies can be used to prevent unauthorized access to the digital document, protect the content during the transmission of the file, but once it is received and decrypted, the document is no longer protected. As a complement to encryption and/or copy protection, digital watermarking has been proposed as “last line of defense” against document misuse in recent years [3].

Digital watermarking technique [1] refers to the process of embedding the given watermark information such as possessory name, symbol, signature etc, into the protective information like photographs, digital music, and digital video and picking the given watermark information from the

protective information, which is not perceived by human perceptual system. Fig.1 shows the fundamental process of digital watermarking technique. Ref. [4,5] gives sufficient detail about watermarking requirements.

There are two essential requirements for image watermarking. One is transparency, namely the changes in the quality of host image after watermarking should not be distinguishable by Human Visual System (HVS).

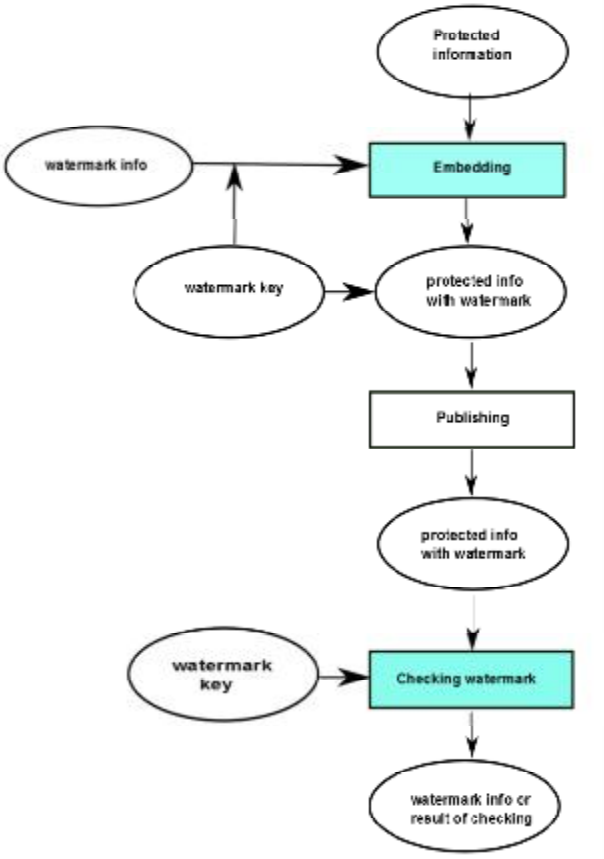


Figure 1. Fundamental process of digital watermarking

2. Watermarking Embedding Process

The detailed steps of the proposed watermark embedding process are illustrated as follows:

Step 1. Torus automorphism permutation: in order to increase the security and robustness of watermark, the watermark logo should be disordered before embedding. Torus Automorphism (TA) is an effective method to scatter a watermark uniformly and randomly [7]. The watermark used in the proposed scheme is permuted based on the following equation before inserting into the host image.

$$\begin{pmatrix} i^* \\ j^* \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & g \end{pmatrix} \times \begin{pmatrix} i \\ j \end{pmatrix} \bmod n \qquad (1)$$

Where (i^*, j^*) represents new coordinate of pixel (i, j) and a and b are the key parameters which

are determined by the user. Moreover, $g = ab + 1$ and n is the size of second dimension of message. Applying the concept of TA for scrambling the binary watermark before it is hidden into the host image offers cryptographic protection against intentional reconstruction of watermark [8]. This is because the keys utilized in the TA permutation procedure are also necessary in the inverse TA permutation in watermark extraction procedure. So by arbitrary choosing of $a = 12$ and $b = 313$ two private keys for satisfying security are provided. Consequently, without the keys, the attacker cannot determine the original permutation of watermark bits and detection process is impossible.

(a) (b)

Figure 2. (a) Original watermark (b) Permuted watermark

Step 2. YUV color conversion: RGB color space is highly correlated and is not suitable for watermarking applications. However, by decreasing the correlation among RGB channels, they can be exploited for watermarking. So in the suggested scheme, the watermark information is inserted into the luminance layer of image. The luminance information Y of the color image is obtained by applying the YUV color transformation, as shown in Eq. (2). The two reasons for embedding watermark in Y (luminance) rather than U or V (chrominance) are: (i) HVS is less sensitive to changes in luminance layer than to the other two chrominance components, and (ii) the JPEG and MPEG standards typically use higher density for Y in contrast with two other components.

$$\begin{pmatrix} Y \\ U \\ V \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ -0.148 & -0.289 & 0.437 \\ 0.615 & -0.515 & -0.100 \end{pmatrix} \times \begin{pmatrix} R \\ G \\ B \end{pmatrix} \qquad (2)$$

As Figure 3 shows, by exploiting Eq (2) over RGB image, the Lena image is converted to YUV separated channels.

Y U V

Figure 3. Converted RGB image to YUV color space

It should be noted that the proposed method is performed on diverse color spaces which their chrominance and luminance layers are separated like L*a*b and HSL. As Fig. 4 shows YUV color space results in better transparency in comparison with two other low correlated color spaces. Additionally Fig. 3 and Fig. 5 provide a visual comparison between different layers of diverse color spaces.

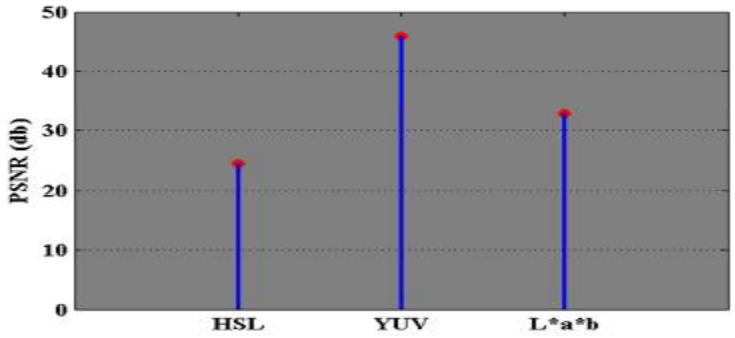


Figure 4. Evaluation of the proposed method under among different color spaces based on PSNR

Figure 5. Representation of various color components;
(a) L*a*b(first row) (b) HSL(second row)

Step 3. DWT transformation: Discrete Wavelet Transform (DWT) is a kind of signal decomposition that converts images from spatial domain to frequency domain. In this paper, we have utilized *Haar* discrete wavelet transform which splits a signal into four sub-bands i.e. LL (low frequency sub-band), HL (horizontal mid-frequency sub-band), LH (vertical mid-frequency sub-band) and HH (high frequency sub-band) with the following equations [9-10]:

$$\begin{aligned} LL &= [(f(i,j)*(f(-i)f(-j)))(2n,2m)]_{(n,m)\in z^2} \\ LH &= [(f(i,j)*(f(-i)y(-j)))(2n,2m)]_{(n,m)\in z^2} \\ HL &= [(f(i,j)*(y(-i)f(-j)))(2n,2m)]_{(n,m)\in z^2} \\ HH &= [(f(i,j)*(y(-i)y(-j)))(2n,2m)]_{(n,m)\in z^2} \end{aligned} \quad (3)$$

Where $f(i,j)$ is image function of size $n \times m$ which belong to integer numbers . Also, $f(t)$ is a low-pass scaling function, and $y(t)$ is the associated band-pass wavelet function.

Among all sub-bands, high frequency sub-band represent the detail and edge components in an image which are less sensitive to human eye, but they are more easily attacked by common signal processing like compression. Conversely, the low frequency sub-band is more robust but embedding the watermark information in this band endangers the quality of image which can be perceived by HVS. To get a trade-off between transparency and robustness, we select the mid-frequency sub-bands to hide the watermark.

Step 4: Watermark insertion: In order to insert the watermark, Pseudo Random Numbers based on Mersenne-Twister algorithm [11] are created by using a private key and with a long period of $(2^{19937} - 1)/2$ which occupy less memory space. Whereas we have used a specific seed to produce the PRN, the third private key of the proposed scheme is formed in this step. By using the following equation the permuted watermark is scattered into the mid-frequency wavelet coefficients.

$$\begin{aligned} &for\ i = 1, 2, \ldots, l\ \ do \\ &CO' = CO + \frac{d \times PRN}{10} \qquad if\ \ i = 1 \\ &CO' = CO \qquad\qquad\qquad Otherwise \\ &sum \end{aligned} \quad (4)$$

Where i represents bit of watermark, l is the length of message, CO , CO' is the mid-frequency wavelet coefficient and watermarked wavelet coefficient, respectively. Additionally, PRN is the Pseudo Random Number and d shows the modulation index. It should be noted that bit of watermark is assigned to one with respect to permuted image.

Step 5. Inverse DWT: by performing the inverse Discrete Wavelet Transformation the watermarked wavelet coefficients and consequently the watermarked image are achieved.

Step 6. Inverse YUV color conversion: The final step of the proposed embedding algorithm is to convert the YUV color space of the watermarked image back to the original RGB color space.

3. Watermarking Detection Process

Outside of the last step of watermark information extraction, the stages of the proposed algorithm for both

extracting and inserting the message are similar to each other. The procedure for watermark detection is simple and does not require any assistance of the original host image which means blind retrieval. Note that three key parameters are needed in the watermark extraction procedure: firstly, the parameters of Torus permutation function which are required for rebuilding the watermark pattern and secondly the utilized key in creating the Mersenne-Twister sequence. The steps for watermark retrieval are briefly listed as follows.

Step 1. Extract the luminance layer of the watermarked image based on the YUV color components.

Step 2. Performing the first level of wavelet in order to extract the horizontal and vertical mid-frequency sub-bands.

Step 3. In this step, correlation coefficient between the original mid-frequency sub-bands and the extracted mid-frequency sub-bands are calculated. Therefore if the correlation coefficient satisfies a threshold the watermark will be detectable. The following algorithm shows this process:

$$\begin{aligned} &for\ i = 1,2,...,l\ \ do \\ &i = 1 \qquad if\ \ corr(CO, CO') > \ th \\ &i = 0 \qquad otherwise \\ &sum \end{aligned} \tag{5}$$

CO, CO' are the original and extracted mid-frequency coefficients, respectively. Also, in order to gratify the robustness of the suggested scheme against attacks the ***th*** (threshold), ***tentatively*** is considered as 0.0099 for modulation index of 2. The value of correlation is computed based on the following equation [12]:

$$Corr(w,w') = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(w(i,j)-v).(w'(i,j)-v')}{\sqrt{\left(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(w(i,j)-v)^2\right).\left(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(w'(i,j)-v')^2\right)}} \tag{6}$$

where v and v' are the mean of $w(i, j)$ and $w'(i, j)$ respectively.

Step 4: Rearrange the extracted watermark bits into right order by Torus automorphism permutation. Then the watermark pattern is rebuilt.

4. Simulation Results

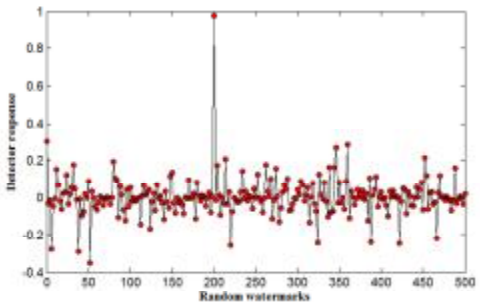
The proposed scheme has been executed on Lena color image. The test image is with size 512×512 pixels. The watermark pattern used in the experiments is a binary image with size 32×32 pixels and it is given as Fig. 2(a). To provide objective judgment of the extracting fidelity, similarity value between the original watermark W and the extracted watermark W^*, is calculated and it is defined as Eq. (7). In addition, the visual quality of watermarked images is evaluated by the peak signal to noise ratio (PSNR) criterion defined as Eq. (8) [13].

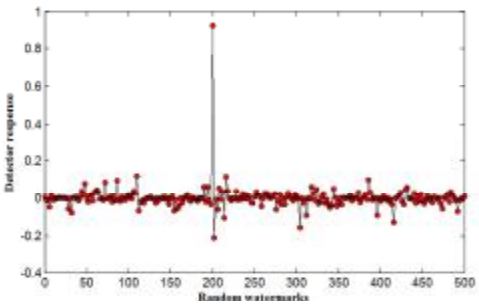
$$NC = \frac{\sum_{i=1}^{32}\sum_{j=1}^{32} w(i,j)\times w^{*}(i,j)}{\sum_{i=1}^{32}\sum_{j=1}^{32}[w(i,j)]^{2}} \qquad (7)$$

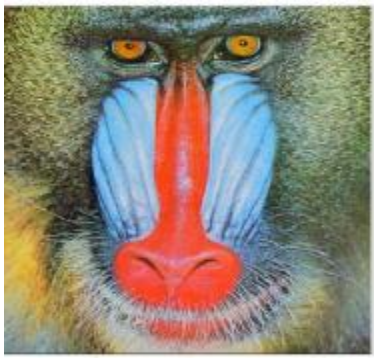
$$PSNR = 10\log_{10}\frac{E_{\max}^{2}\times I_{w}\times I_{h}}{\sum(I_{i,j}-I_{i,j}^{*})^{2}} \qquad (8)$$

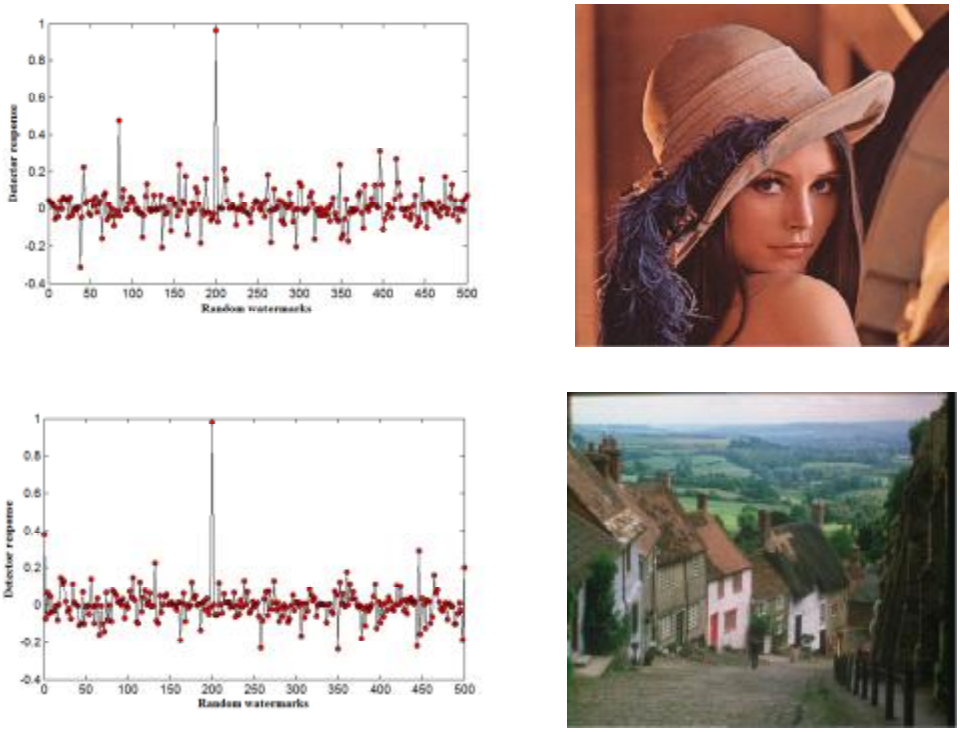
In Eq. (7), I_w and I_h are the width and height of the watermarked image, respectively. $I_{i,j}$ is the original image pixel value at coordinate (i j) and $I_{x,y}^{*}$ is the altered image pixel value at coordinate (i, j). $E_{\max}$ is the largest energy of the image pixels (i.e., $E_{\max}$ =255).

As Fig. 4(a) depicts the watermarked image has good compatibility with HVS. Furthermore by calculating Eq. (7) a PSNR of 45.59 dB is achieved which demonstrate the proposed scheme satisfies a very good transparency. Also Fig. 4(b) shows the detector response for 500 possible watermark generated by 500 different keys; and the embedded watermark generated by the owner corresponds to the key equal to 200.









(b) (a)

Figure 6. (a) Watermark image; (b) Detector response of (a)

The success in acquiring high transparency contains two reasons (i) watermark is hidden in edges and texture of image (ii) by extracting the luminance component of the host image and embedding the watermark in this area, human eyes is not able to sense the modification of the host image.

4.1 Evaluation of robustness & transparency

In order in to survey the robustness and transparency of the proposed scheme with other approaches, our method is compared with three previously presented algorithms. In [14] Feng et al. proposed a combined DWT-DCT algorithm for image watermarking. They insert the watermark into mid-frequency coefficients of DCT which were acquired by performing DCT transform on first level of wavelet LL sub-band. Hong-liang et al. [15] delivered approximately the same work however this method embeds the watermark into mid-frequency components of DCT which were achieved by performing DCT transform on third level of wavelet LL sub-band. Also these schemes have different algorithm for watermark embedding process. Another DWT-DCT based image watermarking was proposed in [16]. In this scheme the mid-band coefficient of second level of wavelet are earned at first. Then this sub-band undergoes the DCT transform to insert the watermark information into mid-band DCT coefficients.

Although these schemes delivered good robustness against attacks, they had degradation in transparency and quality of watermarked image. As Table I shows the proposed method has better transparency in comparison with other methods meanwhile deliver significant robustness against different kinds of attacks.

Table 1. Performance comparison among the presented algorithm and previously suggested algorithms

Attack/Transparency	Feng [14]	Al-Haj [16]	Huai-bin[15]	Proposed
PSNR (dB)	37.71	37.29	37.29	45.59
No attack	0.9906	0.9951	1	1
AWGN (10%)	0.9558	0.9473	0.9684	0.9644
Salt & Pepper noise (10%)	N/A	0.8193	0.9856	0.9959
Cropping (25%)	0.9495	0.9551	0.9712	0.9918
Wiener filtering	N/A	N/A	N/A	0.7027
JPEG compression (75%)	0.9880	0.9902	0.9963	0.9634
Resizing (50%)	0.9798	0.8350	0.5176	0.6110

Where the first row of the table I shows the quality of image based on Peak Signal to Noise Ratio after extraction step. Moreover, other rows depict the robustness factor of different approaches based on Normalized Correlation. In this comparison a categories of attacks like different kinds of noises, cropping, filtering, compression and resizing are investigated over our method and other approaches. As Table I illustrates our method have better performance both in quality and attack invariance aspects in comparison with the other approaches.

5. Conclusion

An imperceptible and blind image watermarking was introduced in this paper. In the proposed method 3 private keys are applied to meet the security of the scheme. The watermark is embedded into a digital image by modifying the mid-frequency coefficients in DWT frequency domain. With the proposed scheme，so, the embedded watermark can successfully survive after attacked by image processing operations. Moreover, the watermark embedding and extracting processes are very simple and the watermark is self-extractable. Simulation results show that the proposed scheme outperforms the earlier works.

Acknowledgments: We would like to appreciate the anonymous reviewers for their nice comments.

References

[1]. Ghosh, P. et al. (2012), “A Novel Digital Watermarking Technique for Video Copyright Protection” , *J. Computer Science & Information Technology (CS & IT)*, 6(2): 601–609.

[2]. Masoumi, M., Amiri, S. (2012), “A High Capacity Digital Watermarking Scheme for Copyright Protection of Video Data based on YCbCr Color Channels Invariant to Geometric and Non-Geometric Attacks” , *Int. J. Computer Applications*, 51(13):13-22.

[3]. Katzenbeisser, S., Petitcolas, F. (1999), *Information hiding techniques for steganography and digital watermarking*, Artech House Books.

[4]. Liu J., He X. (2005), “A Review Study on Digital Watermarking”, *1st Int. Conf on Information and Communication Technologies*, pp. 337 – 341.

[5]. Cox I.J, Miller M.L., and J.A. Bloom (2001), "*Digital Watermarking*.", 1st edition, San Francisco: Morgan Kaufmann Publisher.

[6]. Vleeschouwer C.D., Delaigle J.F., Macq B. (2002), "Invisibility and application functionalities in perceptual watermarking an overview", in *Proc. of the IEEE*, pp. 64–77.

[7]. Chang C.C., Hsiao J.Y., Chiang C.L. (2002), "An image copyright protection scheme based on torus automorphism", *Proc. of the 1st Int. Symposium on Cyber Worlds*, pp. 217–224.

[8]. Engedy M., Munaga V.N.K., Saxena A. (2006), "A robust wavelet based digital watermarking scheme using chaotic mixing", *Proc. of the 1st Int. Conf. on Digital Information Management*, pp. 36–40.

[9]. Masoumi M., Amiri S, (2012)"A Blind Video Watermarking Scheme Based on 3D Discrete Wavelet Transform," *International Journal of Innovation, Management and Technology (IJIMT))*, 3(4): 487-490.

[10]. Masoumi M., Amiri S. (2014), "Content protection in video data based on robust digital watermarking resistant to intentional and unintentional attacks.", *Int. Arab J. Information Technology*, 10(3): 204-212.

[11]. Matsumoto M., and Nishimura T., (1998), "Mersenne Twister, A 623-dimensionally equilistributed uniform pseudorandom number generator," *ACM Trans. Modeling and Comput. Simul*, 8(1): 3–30.

[12]. Zhang F., Yang, G. Liu1 X., and Zhang X. (2006), "Image watermarking algorithm based on the code division multiple access technique," *Springer- Heidelberg, Knowledge Based Intelligent Information and Engineering Systems*, pp. 204–211.

[13]. Xiuguang L. , Xiaoyuan Y. (2011), "A Blind Watermarking Algorithm Resisting to Geometric Transforms Based on SVD", *Wuhan University J. Natural Sciences*, 16(6): 487-492.

[14]. Feng L. P., Zheng L. B., Cao P. (2010), "A DWT-DCT Based Blind Watermarking Algorithm for Copyright Protection", *Computer Science and Information Technology, IEEE*, 7(3): 455-458.

[15]. Huai-bin W., Hong-liang Y., Chun-dong W., Shao-ming W. (2010), "A New Watermarking Algorithm Based on DCT and DWT Fusion", *Int. Conf. on Electrical and Control Engineering*. DOI: 10.1109/iCECE.2010.640

[16]. Al-Haj A. (2007), "Combined DWT-DCT Digital Image Watermarking", *Journal of Computer Science*, 3(9): 740-746.