Image Watermarking Using Psychovisual Threshold over the Edge

Nur Abu, Ferda Ernawan, Nanna Suryana, Shahrin Sahib

Image Watermarking Using Psychovisual Threshold Over the Edge

Nur Azman Abu, Ferda Ernawan, Nanna Suryana and Shahrin Sahib

Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka
Hang Tuah Jaya, Melaka 76100, Malaysia
nura@utem.edu.my,ferda1902@gmail.com, nsuryana@utem.edu.my and
shahrinsahib@utem.edu.my

Abstract. Currently the digital multimedia data can easily be copied. Digital image watermarking is an alternative approach to authentication and copyright protection of digital image content. An alternative embedding watermark based on human eye properties can be used to effectively hide the watermark image. This paper introduces the embedding watermark scheme along the edge based on the concept of psychovisual threshold. This paper will investigate the sensitivity of minor changes in DCT coefficients against JPEG quantization tables. Based on the concept of psychovisual threshold, there are still deep holes in JPEG quantization values to embed a watermark. This paper locates and utilizes them to embed a watermark. The proposed scheme has been tested against various non-malicious attacks. The experiment results show the watermark is robust against JPEG image compression, noise attacks and low pass filtering.

Keywords: Image watermarking, JPEG image compression, edge detection.

1. Introduction

Currently, an efficient access internet makes it easy to duplicate digital image contents. In addition, current mobile devices view and transfer compressed images heavily [1]-[4]. Image watermarking is one of the popular techniques to manage and protect the copyright digital image content. Most of the image watermarking techniques exploits the characteristic of Human Visual System (HVS) in effectively embedding a robust watermark [5]-[7]. HVS is less sensitive to noise in highly textured area [8] and significantly changing region of an image. Human visual properties can be utilized in embedding process by insert more bits of watermark image for each block which has complex textures or edges on an image. The watermark with significant coefficients is more robust if it resides near round edges and texture areas of the image [9]. This paper proposes an embedding watermark scheme along the edge of the host image. This scheme enables the watermark to be more robust against non-malicious attacks.

The organization of this paper is given as follows. The next section will give a brief description on the concept of pshycovisual threshold for image watermarking. Section 3 presents an experimental design of the image watermarking. The experi-

ment results of the propose watermark scheme are presented in Section 4. Section 5 concludes this paper.

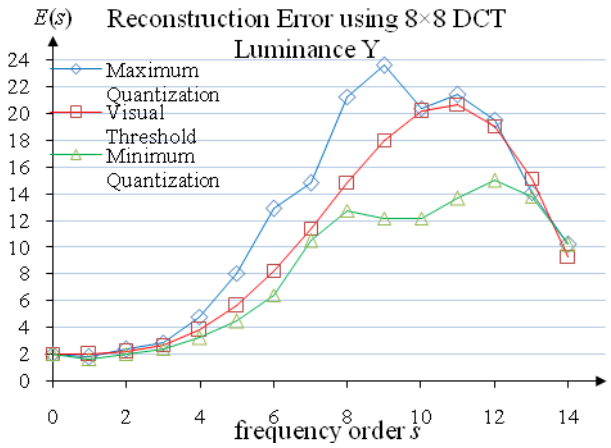

Fig. 1. Average reconstruction error of an increment on DCT coefficient on the luminance for 40 natural images

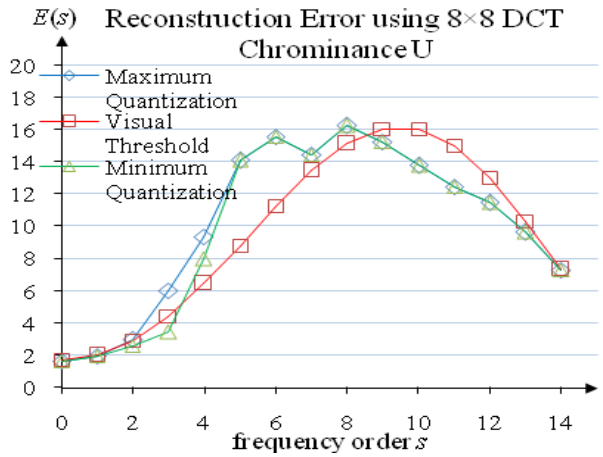

Fig. 2. Average reconstruction error of an increment on DCT coefficient on the chrominance for 40 natural color images

2. Psychovisual Threshold Based on Reconstruction Error

A psychovisual threshold has been generated from a quantitative experimental method. The image is divided into the 8×8 size blocks pixels and then transformed by 2-dimensional DCT. The resulting transformed coefficients are incremented one by one on each frequency order. The DCT coefficients are incremented up to a maximum order of JPEG quantization table values. The effect of incrementing DCT coefficients are measured based on the image reconstruction error from the original image. The average reconstruction error from incrementing DCT coefficients for 40 natural im-

ages is shown in Fig. 1 and Fig. 2. The green line represents average image reconstruction error based on minimum quantization value of each order while the blue line represents average image reconstruction error based on maximum quantization table. The effect of incremented DCT coefficient as the frequency just noticeable difference of image reconstruction is investigated. The average image reconstruction error scores for each frequency order from order zero until order fourteen shall produce a transitional curve. In order to produce a psychovisual error threshold, the average reconstruction error is set by smoothing the curve line of image reconstruction errors as presented the red line. According to Fig. 1 and Fig. 2, there are gaps and loopholes in the popular JPEG quantization table. The gap is identified as the difference between minimum error reconstruction based on JPEG quantization table and an ideal error threshold reconstruction. We choose the gaps in the lower order because the watermark overthere is more robust against JPEG compression. The locations of loopholes in the popular JPEG quantization tables based on error threshold level are shown in Fig. 3.

16	14	13	15	19	28	37	55
14	13	15	19	28	37	55	64
13	15	19	28	37	55	64	83
15	19	28	37	55	64	83	103
19	28	37	55	64	83	103	117
28	37	55	64	83	103	117	117
37	55	64	83	103	117	117	111
55	64	83	103	117	117	111	90

18	18	23	34	45	61	71	92
18	23	34	45	61	71	92	92
23	34	45	61	71	92	92	104
34	45	61	71	92	92	104	115
45	61	71	92	92	104	115	119
61	71	92	92	104	115	119	112
71	92	92	104	115	119	112	106
92	92	104	115	119	112	106	100

Fig. 3. The locations if embedding watermark within 8×8 DCT coefficient for luminance (left) and chrominance (right) of new quantization tables Q_{VL} and Q_{VR} based on the psychvisual threshold.

The watermark is expected to survive better in these deep holes against JPEG standard quantization tables Q_{CL} and Q_{CR} for luminance and chrominance respectively. These gaps can be computed as follows:

$$Q_{GL} = Q_{VL} - Q_{CL} \tag{1}$$

$$Q_{GR} = Q_{VR} - Q_{CR} \tag{2}$$

The location of embedding watermark image is in 8×8 DCT coefficient as depicted and blacken cell in Fig. 3. Each block is embedded watermark image randomly in blacken cells along the edge within the host image.

3. Experimental Design

An experimental sample uses a 'Lena' image 24-bit with size 512×512 pixel as a host image. The binary watermark image *W* "UTeM logo" has image size 32 × 32 pixels as shown in Fig. 4.

Fig. 4. Original watermark image consists of 32×32 pixels

The edge of a host image is computed using Canny edge detection to determine the edge location [11]. A sample Lena image is divided into blocks, each block consists of 8×8 image pixels. The host image is embedded a one-bit watermark for each edge image. The Random Numbers Generator (RNG) is an important computation in term of embedding process to generate the random numbers based on a secret key. The secret key is employed to encrypt and decrypt the watermark during watermark insertion and extraction. This paper implements mersenne twister method to generate random numbers for the embedding watermark scheme.

3.1 Watermark Weight

The watermark that will be embedded into the host image is subjected to JPEG quantization table values. The quantization value that will be used as watermarks of embedding process is given as follows:

$$W_{QL} = \{18, 17, 16\} \text{ and } W_{QCR} = \{21, 26, 26\} \tag{3}$$

where the watermark weight depends upon the random numbers from a private key.

$$a = \begin{cases} 0.5 & \text{if } RNG(i,1) = 1 \text{ and } RNG(i,2) = 1 \\ 1 & \text{if } RNG(i,1) = 1 \text{ and } RNG(i,2) = 0 \\ 0.5 & \text{if } RNG(i,1) = 0 \text{ and } RNG(i,2) = 1 \\ 1 & \text{if } RNG(i,1) = 0 \text{ and } RNG(i,2) = 0 \end{cases} \tag{4}$$

The calculation of the watermark quantity is given as follows:

$$Q(i) = RNG(i) \cdot a \cdot W_Q \tag{5}$$

Consider a given 8×8 image block, if the watermark W is 1, the watermark image is multiplied by "+1" and added to the host image whereas the watermark W is 0, it is multiply by "−1" or subtracted from the host image. Each set occurs in the each pixel along the edge. This paper proposes an effective watermark embedding along the image edge randomly without degrading the visual image quality perceptually. If the watermarked image is disturbed along the boundary of an object in the image means that the watermark will be degraded. Consequently, the host image lost its value whenever the visual aesthetic of the image was degraded.

3.2 Watermark Insertion

The most popular embedding watermark in frequency domain is in the most significant coefficient region [12]. It is a trade-off between robustness and imperceptibility. In this paper the watermark is embedded in the loopholes based on JPEG quantization tables. The embedding watermark is added along the edge of an object in the image. At the same time, a random process based on a key is used in the embedding a watermark or not along a given edge. The number of bits from watermark image to be

embedded depends upon the numbers of edge image on each image block. The watermark weight will make sure that the watermark is perceptually invisible. This watermark procedure is as follows;

a. Take the host image block as an input (the size of an image block is 8×8 pixels).
b. Detect the edge image using Canny edge detection to the input image block.
c. Transform the image block by 2-D DCT if there are more than ten edges in image block.
d. Generate a unique random number based on a private key.
e. Determine the location for the watermark based on random numbers. The random numbers also used to generate the watermark weight which is one or half JPEG quantization value.
f. Embed the watermark into the loopholes when the block image has more than ten edges. Embedding value −1 or +1 when the watermark is 0 or 1 respectively.

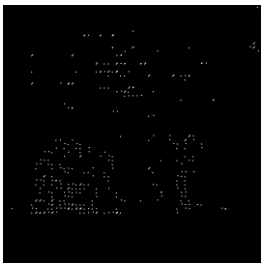

Fig. 5. An enhance absolute difference between the original image and the watermarked image

3.3 Watermark Extraction

The blind detection will be applied to extract the watermark image. This technique does not require an original host image for watermark detection. The watermark image can be obtained by using inner product approach. The watermark is extracted from the host image along the edge image [13]. The watermark image is dispersed randomly along the edge. The watermark is detected by computing correlation between the watermarked image and the watermark code. The difference between watermarked image and original image is enhanced and shown in Fig. 5. The extraction of watermark involves a secret key to generate pseudo random numbers. This extraction is the inverse process of watermark embedding. The extracted watermark algorithms which includes the following steps:

a. Take the watermarked image block as an input (the size of image block is 8×8 pixels).
b. Detect of the edge image using Canny edge detection.
c. Transform the image block by 2-D DCT if there are more than ten edge image in image block.
d. Generate pseudo random numbers based on private key, these random numbers are used to find the location of watermarked image block.
e. Extracted watermark using inner product algorithm. In order to extract the extracted sequence of the $X^*\{x^*(i), (1 < i < N)\}$ where $x^*(i) \geq 1$ means that the watermark is 1 and $x^*(i) \leq 0$ means that the watermark is 0. The correlation coeffi-

cient in the below is used to decide if the watermark image exists in the image as follows:

$$\rho = X \cdot X^* \tag{6}$$

where $X \cdot X^*$ is the inner product of X and extracted sequence of the X^*. If the correlation coefficient between watermarked image X and extracted sequence X^* is larger than a threshold, we determine that watermark exists.

3.4 Image Watermarking Evaluation

In order to evaluate the concealing of the watermark, the standard Peak Signal to Noise Ratio (PSNR) is calculated to measure the quality of extracted watermark image. The comparison between the recovered watermark and the original watermark is quantitatively analysed by using Normalized Cross-Correlation (NC) [13], which is defined as follows:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j).W'(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)^2 \sum_{i=1}^{M}\sum_{j=1}^{N} W'(i,j)^2}} \tag{7}$$

where the $W(i, j)$ is the original watermark image and $W'(i, j)$ is the recovered watermark image. $M \times N$ is the watermark image size and the value of NC is between 0 and 1. The higher value of NC means that the recovery watermark image is closer towards the original watermark image and more robust. In order to evaluate the performance of this watermarking scheme, the watermarked image undergoes various non-malicious attacks such as JPEG image compression, gaussian white noise, salt and pepper noise and gaussian low pass filter.

4. Experimental Results

This section examines the robustness of the image watermarking scheme against non-malicious attacks. Several experiments are tested to evaluate its performance of watermarked image and the results are shown in Table 1.

Table 1. Various Attacks for Watermarked Image.

Various attacks	NC	PSNR
JPEG compression	0.8435	35.4610
Gaussian white noise 0.01	0.7183	20.2163
Salt & pepper noise 0.02	0.8003	22.1565
Gaussian low pass filter 3×3	0.9572	42.5371

The results of watermarked images and the corresponding extracted watermark after various non-malicious attacks are shown in Fig. 6 and Fig. 7.

(a) (b) (c) (d)

Fig. 6. The results of watermarked image from (a) JPEG image compression, (b) Gaussian white noise 0.01, (c) Salt and pepper 0.02 and (d) 3×3 Gaussian low pass filter

(a) (b) (c) (d)

Fig. 7. The extracted watermark image after from (a) JPEG image compression, (b) Gaussian white noise 0.01, (c) Salt and pepper 0.02 and (d) 3×3 Gaussian low pass filter

Human visual system and its sensitivity are utilized in the design of this embedding watermarking scheme. The advantages of this watermarking scheme are the watermark image is perceptually invisible to the human eye and robust to non-malicious attacks. The destroying the image edge will remove the watermark. It also means that the quality of the host image will be damaged considerably.

The experimental results indicate that the watermark is resistance against non-malicious attacks. The recovered watermark changes slightly in comparison with original watermark and there is no significant change in visual perception between host image and watermarked image. Table I shows the comparison NC and PSNR of the proposed watermark against Gaussian low pass filter, JPEG compression, salt and pepper noise. The watermark scheme has a great resistance to salt and pepper noise. The results indicate that the proposed scheme is robust against the JPEG image com-

pression. The extracted watermark image can be damaged but the visual perception of watermark still can be seen by human eye.

5. Conclusion

Digital image watermarking becomes an important technique for management and copyright protection. An effective secure embedding watermark based on human visual system properties is explored. The quantitative experiment of psychovisual error threshold level on natural images has been done. According to visual threshold model, there are gaps within the standard JPEG quantization tables. The embedding watermark image on loopholes based on JPEG quantization tables has been investigated. The watermark image is embedded along the edge based on psychovisual threshold visually invisible to human eye. The watermark is robust to non-malicious attacks. The experimental results show the extracted watermark image survives against JPEG image compression. In addition, the image watermarking scheme has strong resistance against added noise and low pass filtering.

6. Acknowledgment

The authors would like to express a very special thank to Ministry of Higher Education (MOHE), Malaysia for providing financial support for this research project via Fundamental Research Grant Scheme (FRGS/2012/FTMK/SG05/03/1/F00141).

References

1 Ernawan, F., Abu, N.A., Rahmalan, H.: Tchebichef Moment Transform on Image Dithering for Mobile Applications. In: Proceeding of the SPIE, vol. 8334, pp. 83340D-5. SPIE Press (2012)

2 Rahmalan, H., Ernawan, F., Abu, N.A.: Tchebichef Moment Transform for Colour Image Dithering. In: 4th International Conference on Intelligent and Advanced Systems (ICIAS 2012), pp. 866-871. IEEE Press, (2012)

3 Ernawan, F., Noersasongko, E., Abu, N.A.: An Efficient 2×2 Tchebichef Moments for Mobile Image Compression. In: International Symposium on Intelligent Signal Processing and Communication System (ISPACS 2011), pp. 001-005. IEEE Press, (2011)

4 Abu, N.A., Lang, W.S., Suryana, N., Mukundan, R.: An Efficient Compact Tchebichef Moment for Image Compression. In: 10th International Conference on Information Science, Signal Processing and their applications (ISSPA2010), pp. 448-451. IEEE Press, (2010)

5 Liu, K.C.: Human Visual System based Watermarking for Color Images. In: International Conference on Information Assurance and Security (IAS 2009), vol. 2, pp. 623-626. IEEE Press, (2009)

6 Niu, Y., Kyan, M., Krishnan, S., Zhang, Q.: A Combined Just Noticeable Distortion Model-Guided Image Watermarking, Signal, Image and Video Processing, vol. 5, no. 4, 2011, pp. 517-526. IEEE Press, (2011)

7 Jayant, N.J., Johnston, J., Safranek, R.: Signal Compression Based on Models of the Human Perception, Proc. IEEE, vol. 81, pp. 1385–1422. IEEE Press, (1993)

8 Yang, Y., Sun, X., Yang, H., Lie, C.T., Xiao, R.: A Contrast-Sensitive Reversible Visible Image Watermarking Technique, IEEE Transaction on Circuit and Systems for Video Technology, vol. 19, no. 5, pp. 656-667 (2009)

9 Bedi, S.S., Tomar, G.S., Verma, S.: Robust Watermarking of Image in the Transform Domain using Edge Detection. In: 11th International Conference on Computer Modelling and Simulation, pp. 233-238. IEEE Press, (2009)

10 Abu, N.A., Lang, W.S., Sahib, S.: Image Projection over the Edge. In: International Conference on Computer and Network Technology (ICCNT 2010), pp. 344-348. IEEE Press, (2010)
11 John Canny.: A Computational Approach to Edge Detection, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. PAMI-8, no. 6, 1986, pp. 679–698 (1986)
12 Tseng, H.W., Hsieh, C.P.: A Robust Watermarking Scheme for Digital Images Using Self Reference, Advances in Communication Systems and Electrical Engineering, pp. 479-495. Springer, Heidelberg (2008)
13 You, X., Du, L., Cheung, Y., Chen, Q.: A Blind Watermarking Scheme Using New Nontensor Product Wavelet Filter Banks, IEEE Transaction on Image Processing, vol. 19, no. 12, pp. 3271-3284 (2010)