

A Blind Watermarking Algorithm

Yu-Wen Chang

Dept. of Electronic Communication Engineering, National Kaohsiung Marine University, Taiwan

Abstract - In this paper, a blind watermarking algorithm is proposed to explore the influence of DCT coefficients in watermarking mechanism. Each two DCT coefficients are selected and compared from the same DCT block. And, the coefficient of the lower frequency region is used as the basis for comparison. Then, the watermark bit will be embedded and extracted with this relation of the coefficients in the same block and the watermark rule. The characteristics of the DCT coefficients in the lower frequency region are not easily changed, thus the relation of the coefficients can be more relatively stable. Moreover, the quality of the retrieved watermark and the robustness of the watermarking will be raised up. And, the proposed method is designed as blind, which the host image and original watermark are not needed in the extracting process.

Key Words: digital watermarking, blind, relation of the coefficients.

1. INTRODUCTION

Digital watermarking technique was first proposed in 1989. The totem or logo used to be the representation of the legal owner is embedded into the media in this scheme based on the character of the digital media can be distorted. With such technology, the identity of the legitimate owner of the multimedia can be claimed in order to achieve the purpose of protecting intellectual property rights.

Because the digital media can be easily downloaded, transmitted or even copied without restriction via web pages or the internet, the copyright and the intellectual property rights are greatly threatened. Moreover, many information security problems such as fake transactions, theft, tampering ... and so on will be yielded. Therefore, digital watermarking technology [1] is more and more important and urgent.

Until now, many digital watermarking technologies have been introduced and have more effective for different applications. A robust lossless data hiding method using the clustering and statistical quantity histogram is showed in [2-3]. However, the retrieved data will be wrong under the lossy compression and random noise. A watermarking scheme using the codebook expansion based on the vector quantization (VQ) is developed in [4-5]. Though these technologies are designed as simple and effective; but the

embedded watermark is not robust. A sharing-based watermarking mechanism is proposed to resist the attack as cropping and collage [6]. However, the large scale tampering of the watermarked image will not be detected. In recent years, the algorithms using the soft computing are derived to optimize the parameters intelligently for trading off the qualities between the host image and the retrieved watermark [7-8]. Nevertheless, these schemes are not designed as blind. A hybrid watermark technique using Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) is showed in [9]. Although two complementary watermarks are hid simultaneously for higher detection response, each watermark could against a specific class of attacks. A watermark method using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) is designed as robust for various attacks [10]. But, the watermark is visual.

Until the correspondence between the communication and the data hiding is introduced, the digital watermarking method is regarded as a communication problem. Therefore, the error correcting codes (ECC) are used to enhance the robustness of the watermark [11-14]. Besides, some schemes are designed to protect the color image [15-16]. These methods utilized the block-edge-pattern or the error correcting coding. However, the redundancy quantities would be increased after the ECC technique.

For the robustness reason, most of watermarking techniques [17-20], the watermark will be hid in the frequency domain instead of the spatial domain. Each two DCT coefficients are selected from the different DCT blocks and modified using the embedding rule and the information of the watermark.

In this paper, we would like to explore the results of that each two DCT coefficients are selected and modified from the same DCT block. The coefficient of the lower frequency region is used as the basis for comparison. Since, the characteristics of the DCT coefficients in the lower frequency region are not easily changed, the relation of the coefficients can be relatively stable. Thus, the proposed algorithm can used to raise the quality of the retrieved watermark and to enhance the robustness of the watermarking.

The remainder of this paper is organized as follows. In section 2, the concept of image is briefly presented. The framework and details of the proposed technique are

described in section 3. The section 4 is about the results and the conclusion.

2. THE CONCEPT OF IMAGE

In most cases, the characteristics of the neighboring blocks in the image are similar. Therefore, the values of each two DCT coefficients which are selected from the same position of the different blocks are also similar. The other hand, the watermark is embedded into the frequency domain for the robustness reason. According to the theory of data hiding, the DCT coefficients will be used to compare and modify in order to embed the watermark.

For the quality of the host image, the affect of the modification of the DCT coefficients in the high-frequency region is a little. However, the watermark would be erased easily due to signal processing. Though the watermark is hid in the low-frequency region can avoid attacks. But the quality of the host image would be damaged seriously. Consequently, the watermark had been chosen mostly to embed into the medium-frequency region.

To preserve the quality of the host image, the modification of DCT coefficient should be as small as possible. Thence, the watermark bit will be give up sometimes. In other word, if the difference of each two block is too large, the watermark bit will be thorwing away to maintain a better quality of the watermarked image. However, it will cause the decrease in the quality of the retrieved watermark.

3. THE PROPOSED TECHNIQUE

The proposed watermarking scheme is used to improve the question discussed above section. Each two DCT coefficients are selected from the same block in order to achieve the purpose for watermarking algorithm. The process of the embedding the watermark into the host image is shown in Fig. 1.

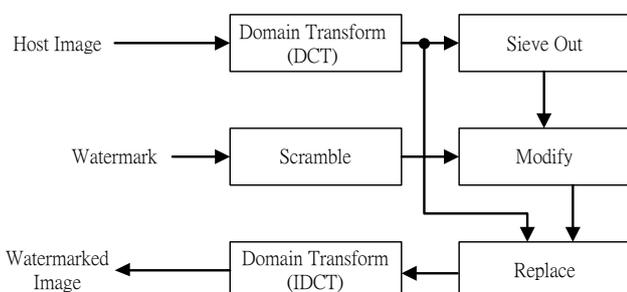


Fig -1: The process of the watermark embedding

Step 1: watermark scrambled

The pixel of the watermark w of size $L \times L$ is scrambled with the chaos mapping function. Let T_k denotes the permutation matrix and w_p means the permuted watermark, respectively.

Step 2: DCT transformed

The host image f of size 256×256 is performed block transform by DCT. Let F denotes the block transform of f is given by $F = \{F(u, v) | 0 \leq u, v \leq 255\}$. And these block are be sequentially labeled as C_l , for $0 \leq l \leq 1023$.

Step 3: coefficients selected and modified

The coefficients are selected from the lower-frequency and the middle frequency regions. Then, to modify these coefficients according the watermark information and rule 1 as follows.

Rule 1 :

(a) If $\text{round}(C_l(j)/Q(j)) \leq \text{round}(C_l(j+8)/Q(j+8))$ and $w_p = 1$, then $C'_l(j+8) = C_l(j+8) + \Delta$

(b) If $\text{round}(C_l(j)/Q(j)) > \text{round}(C_l(j+8)/Q(j+8))$ and $w_p = 1$,

If $(\text{round}(C_l(j)/Q(j)) \times Q(j+8) + \Delta) - C_l(j+8) < \Gamma$, then $C'_l(j+8) = \text{round}(C_l(j)/Q(j)) \times Q(j+8) + \Delta$

else $C'_l(j+8) = C_l(j+8)$

(c) If $\text{round}(C_l(j)/Q(j)) \leq \text{round}(C_l(j+8)/Q(j+8))$ and $w_p = 0$,

If $C_l(j+8) - ((\text{round}(C_l(j)/Q(j)) - 1) \times Q(j+8) - \Delta) < \Gamma$, then $C'_l(j+8) = ((\text{round}(C_l(j)/Q(j)) - 1) \times Q(j+8) - \Delta)$

else $C'_l(j+8) = C_l(j+8)$

(d) If $\text{round}(C_l(j)/Q(j)) > \text{round}(C_l(j+8)/Q(j+8))$ and $w_p = 0$, then $C'_l(j+8) = C_l(j+8) - \Delta$

for $l = 1, 2, \dots, 1023$, $j = 0, 1, \dots, 8$

where $C_l(j)$ (resp. $C_l(j+8)$) denotes the lower frequency (resp. the middle frequency) coefficient; w_p denotes the scrambled watermark bit will be embedded into the block C_l ; $Q(j)$ and $Q(j+8)$ denote the quantifications of corresponding to the quantization table in JPEG standard. The Δ and Γ , indicate the control scaling parameters are used to control the value of the DCT coefficient.

Step 4: replaced the coefficients

The coefficients of the middle frequency is adjusted by step 3 and is restored to the host image.

Step 5: IDCT transformed

Implement the IDCT to obtain a watermarking image g .

The watermarking technique is designed as oblivious. Therefore, the original host image and watermark are all not be needed in the extracting procedure which is given in Fig. 2.

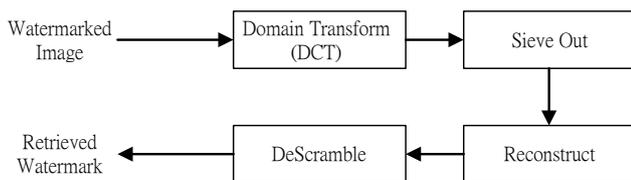


Fig -2: The process of the watermark extracting

Step 1: DCT transformed

Perform the block transform of the watermarked image g of size 256×256 using DCT.

Step 2: coefficients selected and reconstructed

Collect the middle frequency coefficients $B_i(j)$ which are the same as step 3 in the embedding method.

Step 3: permuted watermark recovered

Retrieve the permuted watermark according the rule 2.

Rule 2 :

(a) If $\text{round}(B_i(j)/Q(j)) \leq \text{round}(B_i(j+8)/Q(j+8))$ then $w'_p = 1$

(b) If $\text{round}(B_i(j)/Q(j)) > \text{round}(B_i(j+8)/Q(j+8))$ then $w'_p = 0$

Step 4: watermark de-scrambled

Reverse the permutation operation using chaos map function to obtain the retrieved watermark w_r .

4. SIMULATIONAL RESULTS AND CONCLUSIONS

In this section, the proposed scheme described in section 3 will be demonstrate the robustness. The host images of size 256×256 are 8-bit gray level images and the watermarks is a binary image. And, one watermark and three host images (i.e., Pepper, Lena and F16) are used to test.

In the experimental results, the peak signal noise rate (PSNR) is applied to estimate the quality between the original image and the watermarked image, which denote as f and g , respectively. The formula of PSNR is defined as

$$PSNR = 10 \cdot \log_{10}(255^2 / MSE) \quad (1)$$

where the mean square error (MSE) is described as follows

$$MSE = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (f(x, y) - g(x, y))^2 / N^2 \quad (2)$$

The similarity between the original watermark w and the retrieved watermark w' is measured using the bit error rate (BER).

Table 1 (resp. Table 2) shows the quality of the watermarked images and retrieved watermarks in which different host images are used for the proposed watermarking scheme (resp. the conventional watermarking scheme). From the table 1, it can be found that the qualities (PSNR) of the watermarked image with respect to the host image are more than 32dB in average. And the retrieved watermarks can be recovered.

Table -1: Quality of watermarked images and retrieved watermark in which different host image are used in the proposed algorithm

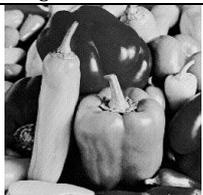
The proposed algorithm				
Watermarked image	MSE	PSNR(dB)	Retrieved watermark	BER(%)
	37.306	32.413		9.27
	37.326	32.411		8.66
	32.039	33.074		9.76

From the table 1 and 2, it is obviously that the qualities of the watermarked images for the proposed algorithm are better about 0.2 to 1.1dB than that of the conventional watermarking algorithm based on the frequency domain.

Further, the retrieved watermarks can be recognized in lower BER.

Therefore, the results of the each two DCT coefficients used to select and modify from the same DCT block are presented in this proposed technique. And, the original image and watermark are not necessitated in the extracting process.

Table -2: Quality of watermarked images and retrieved watermark in which different host image are used in the conventional watermarking algorithm

The conventional watermarking algorithm				
Watermarked image	MSE	PSNR(dB)	Retrieved watermark	BER(%)
	42.324	31.864		9.67
	39.108	32.208		9.5
	41.912	31.907		10.63

REFERENCES

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking. Academic Press, A Harcourt Science and Technology Company, 2002.

[2] L. An, X. Gao, Y. Yuan, and D. Tao, "Robust Lossless Data Hiding using Clustering and Statistical Quantity Histogram," Neurocomputing, 2012, pp. 1-11.

[3] X. Gao, L. An, Y. Yuan, D. Tao, and X. Li, "Lossless Data Embedding using Generalized Statistical Quantity Histogram," IEEE Trans. Circuits Syst. Video Technol. 21, 2011, pp. 1061-1070.

[4] H. C. Wu and C. C. Chang, "A Novel Digital Image Watermarking Scheme Based on the Vector Quantization Technique," Computers and Security, 2005, pp. 460-471.

[5] Z. M. Lu, J. S. Pan, and S. H. Sun, "VQ-Based Digital Image Watermarking Method," IEE Electronic Letters, 2000, pp. 1201-1202.

[6] Y. J. Chang, R. Z. Wang, and J. C. Lin, "A Sharing-Based Fragile Watermarking Method for Authentication and Self-Recovery of Image Tampering," EURASIP Journal

on Advances in Signal Processing, Article ID 846967, 2008.

[7] H. Harrak, T. D. Hien, Y. Nagata, and Z. Nakao, "DCT Watermarking Optimization by Genetic Programming," Advances in Soft Computing, 2006, pp. 347-351.

[8] A. Khan, S. F. Tahir, A. Mahid, and T. S. Choi, "Machine Learning Based Adaptive Watermark Decoding in View of Anticipated Attack," The Journal of the Pattern Recognition Society, 2008, pp. 2594-2610.

[9] Z. J. Lee, S. W. Lin, S. F. Su, and C. Y. Lin, "A hybrid watermarking technique applied to digital images," Applied Soft Computing, 2008, pp. 798-808.

[10] N. Wang and C. H. Kim, "Tamper Detection a Self-Recovery Algorithm of Color Image Based on Robust Embedding of Dual Visual Watermarks using DWT-SVD," 9th International Symposium on Communications and Information Technology, 2009, pp. 157-162.

[11] L. Chen and Z. Yao, "A Novel Watermarking Extraction Based on Error Correction Code and Evidence Theory," Fourth International Conference on Natural Computation, 2008, pp. 613-617.

[12] J. Antonio, M. Noriega, B. M. Kurkoski, M. N. Miyatake, and H. P. Meana, "Image Authentication and Recovery using BCH Error-Correcting Codes," International Journal of Computers, Issue 1, Vol. 5, 2011.

[13] C. Qin, Q. Mao, and X. Zhang, "Image Watermarking Scheme with Unequal Protection Capability Based on Error Correcting Codes," Journal of Multimedia, Vol. 5, No. 5, 2010, pp. 427-433.

[14] I. Usman and S. Khan, "BCH Coding and Intelligent Watermark Embedding: Employing both Frequency and Strength Selection," Applied Soft Computing, 2010, pp. 332-343.

[15] C. H. Chen, Y. L. Tang, and W. S. Hsieh, "Color Image Authentication and Recovery via Adaptive Encoding," 2014 International Symposium on Computer, Consumer and Control, 2014, pp. 272-275.

[16] K. C. Liu, "Color Image Watermarking for Tamper Proofing and Pattern-Based Recovery," IET Image Process., Vol. 6, No. 5, 2012, pp. 445-454.

[17] C. C. Chang, P. Y. Lin, and J. S. Yeh, "Preserving Robustness and Removability for Digital Watermarks using Subsampling and Difference Correlation," Information Sciences, 2009, pp. 2283-2293.

[18] C. M. Kung, J. H. Jeng, and T. K. Truong, "Watermark Technique using Frequency Domain," Proc. of the 14th IEEE International Conference on Digital Signal Processing, July 2002, pp. 729-731.

[19] C. M. Kung, J. H. Jeng, and C. H. Kung, "Watermarking Based on Block Property," 16th IPPR Conference on Computer Vision, Graphics and Image Processing, Aug. 2003, pp. 540-546.

[20] H. C. Chen, Y. W. Chang, and R. C. Hwang, "Watermarking Technique for Multimedia Communication," 2014 3rd International Symposium on Business and Social Sciences, July 2014, pp. 818-826.