World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:4, No:4, 2010

An Algorithm for Secure Visible Logo Embedding and Removing in Compression Domain

Hongyuan Li, Guang Liu, Yuewei Dai, and Zhiquan Wang

***Abstract*—**Digital watermarking is the process of embedding information into a digital signal which can be used in DRM (digital rights managements) system. The visible watermark (often called logo) can indicate the owner of the copyright which can often be seen in the TV program and protects the copyright in an active way. However, most of the schemes do not consider the visible watermark removing process. To solve this problem, a visible watermarking scheme with embedding and removing process is proposed under the control of a secure template. The template generates different version of watermarks which can be seen visually the same for different users. Users with the right key can completely remove the watermark and recover the original image while the unauthorized user is prevented to remove the watermark. Experiment results show that our watermarking algorithm obtains a good visual quality and is hard to be removed by the illegally users. Additionally, the authorized users can completely remove the visible watermark and recover the original image with a good quality.

***Keywords*—**digital watermarking, visible and removable watermark, secure template, JPEG compression

I. Introduction

THE advance of digital technologies and the development of the Internet have made reproduction and distribution of digital multimedia content easier than ever before. To protect the multimedia content, digital watermarking is proposed which embeds the watermark into digital multimedia content so that the watermark can later be extracted or detected. Most of the watermarks are invisible [1,2,3] while a few are visible [4,5,6,7]. A visible watermark is a secondary translucent overlaid on the primary image and appears visible to the user. The main advantage of visible watermarking is that it prevents unauthorized using of copyrighted high quality images.

In visible watermarking, a secondary image is inserted into the host image such that visible watermark is perceptible to a human observer while invisible watermarking the embedded data is not perceptible. Many researches have been done in this area. In [4], Kankanhalli proposed a visible watermarking technique in the discrete cosine transform (DCT) domain. Firstly, the host image and watermark are classifies into 8 × 8 blocks. Then, each block was divided into one of eight classes depending on the sensitivity of the block to distortion. The DCT coefficients of the corresponding blocks of the watermark and the original are added in varying proportions depending on the class to which the image block belongs. They exploited the effect of luminance to make a final correction to the block scaling factors. In [5], Mohanty et al. proposed a dual watermarking algorithm which combines a visible watermark and an invisible watermark in spatial domain. The visible watermark is to show the owner's copyright of the image and the invisible watermark is adopted to find whether the image is tampered. In [6], the user-key-dependent removable visible watermarking system is proposed. The user key structure decides both the embedded subset of watermark and the host information adopted for adaptive embedding. The neighbor-dependent embedder adjusts the marking strength to host features and makes unauthorized removal very difficult. Meng and Chang embedded visible logos to video sequence in the discrete cosine transform (DCT) domain [7] that the stochastic approximation for Braudaway's method is applied.

In this paper, we design a visible and removable watermarking scheme which the embedded visible watermark can be removed from the host image with the right key. The rest of the paper is arranged as follows. In Section 2, the architecture of JPEG based visible and removable watermarking algorithm is proposed. The process of generating the secure template is introduced in Section 3. In Section 4, the experiments are given to show the advantages of the proposed scheme. Finally, some conclusions are drawn, and future work is given in Section 5.

II. Proposed JPEG based Visible and Removable Watermarking Scheme

The architecture of the visible and removable watermarking algorithm is illustrated in Figure 1 which is composed of two parts, visible watermark embedding and watermark removing. The watermark embedding process is done in the server.

Step 1. The original image C and watermark image W is partitioned into 8×8 nonoverlapping blocks, converted to a frequency domain by 8×8 DCT. All the DCT coefficients of watermark and host image are quantized by a quantization table.

Step 2. After the quantization process, the coefficients of

Hongyuan Li, Guang Liu, Yuewei Dai, and Zhiquan Wang are with the Automation Department of Nanjing University of Science and Technology. (corresponding author Hongyuan Li, e-mail: leenuxlee@ gmail.com).

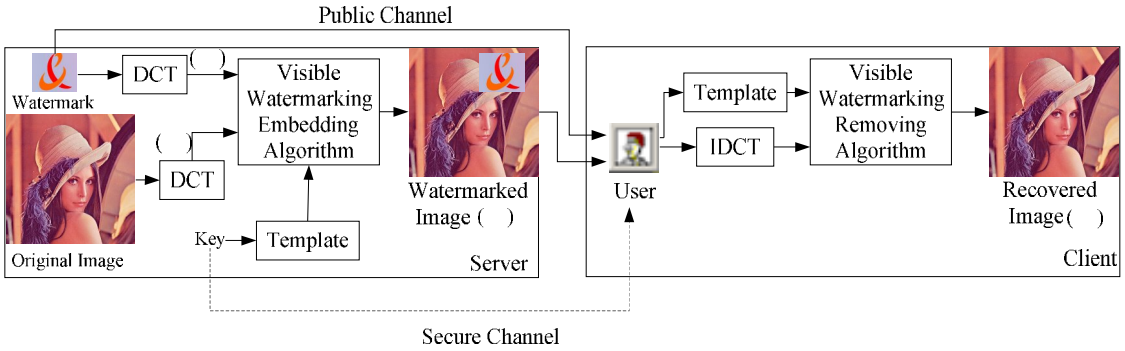


Fig. 1. Architecture of DCT based visible and removable watermarking algorithm

The quantized C and W can be obtained, separately.

Step 3. For different users the different templates are generated by the different keys.

Step 4. In visible watermarking embedding process, the visible watermark is embedded in the host image which is shown in equation (1).

$$C'(i) = \alpha(i)C(i) + S(i)W(i),\ i = 0,1,2,...,n-1. \quad (1)$$

Here, the coefficients $C(i)$ and $W(i)$ are the DCT coefficients of host image and watermarking image after quantization process. $C'(i)$ is the watermarked image. The coefficients $\alpha(i)$ and $S(i)$ are the embedding strength of the host image and watermark. $S(i)$ are selected from the secure template.

After the watermark embedding process, the watermarked images are distributed to the different users in public channel. For different users, the different keys are distributed to users in the secure channel to generate the templates. Then, the template for user is generated under the control of the secret key. With the correct key, the user can generate the same template as the embedding process. Finally, watermark removing process is as follows.

$$C(i) = \frac{C'(i) - S(i)W(i)}{\alpha(i)},\ i = 0,1,2,...,n-1. \quad (2)$$

III. Generation of the Secure Template

From the watermarking algorithm described in Section 2, the process of embedding and removing the watermark is controlled by parameter $\alpha(i)$ and $S(i)$. The generation of parameter $\alpha(i)$ and $S(i)$ in embedding and removing process should be the same so as to keep reversible. In the proposed scheme, $\alpha(i)$ is a constant while $S(i)$ is the variable. The variable $S(i)$ is generated from the secure template. Most of the visible watermark embedding algorithms [7,8,9] do not consider the watermarking removing process. For the security of the visible watermarking, we can make the embedding coefficients of the visible watermark differently with each other so that the user can not remove the watermark from the watermarked image if he removes the watermark directly from the watermarked image. Also, the visual quality of the watermarked image should be considered that the $S(i)$ of the adjacent pixels should have too much interval. Thus, we have to consider the tradeoff between security and visual quality of the proposed scheme.

In Section 2, $S(k)$ is the embedding strength of watermark image. To enhance the security and visual quality, $S(k)$ can be the variable numbers. To find the tradeoff between security and visual quality $S(k)$ is composed of two parts: $S_0(k)$ and $S_1(k)$. $S_0(k)$ is a constant which ensures the visual quality of the visible watermark and $S_1(k)$ is the variable to ensure the security. The algorithm of the secure template generation is as follows.

The Secure Template Generation Algorithm

Step 1. Select a password (*key*).

Step 2. Generate the embedding strength $S(i)$. Here, $S(i)$ is divided into two parts $S_0(i)$ and $S_1(i)$ which we have $S_0(i) \neq S_1(i)$ in most case. $S_0(i)$ is a constant which is adjusted by the original image. The value of $S_1(i)$ which is randomly generated varies in a interval.

Step 3. Function $Template(i, key, p)$ are the binary sequences which are generated randomized. Under the control of the *key* , the $Template(k, key, p)$ are generated by the equation (3).

$$\text{Template}(i, key, p) \in \{0,1\}\ i = 0,1,2,...,n-1. \quad (3)$$

Here, *key* is the password of the template. The proportion of $S_0(i)$ to $S_1(i)$ is determined by the constant p ($0 \le p \le 1$) satisfying $\Pr(S_0(i)) = p$ and $\Pr(S_1(i)) = 1 - p$.

Step 4. Select the watermarking embedding strength template $S(i)$. The final watermarking embedding strength $S(i)$ is obtained by three factors: the embedding strength $S_0(i)$, $S_1(i)$ (in step2) and the binary sequences $Template(i, key, p)$ (in step 3). The generating of the final watermarking embedding strength template $S(i)$ can be obtained by equation (4).

$$S(i) = \begin{cases} S_0(i), & \text{Template}(i, key, p) = 0 \\ S_1(i), & \text{Template}(i, key, p) = 1 \end{cases} \quad i = 0,1,2,...,n-1. \quad (4)$$

The flowchart of generating the watermarking embedding strength template is shown in Figure 2. It consists two embedding strength $S_0(i)$ and $S_1(i)$. For every embedding position k, we choose $S_0(i)$ or $S_1(i)$ as the final embedding strength $S(i)$. In this figure, the white ball ($S_0(i)$) and black ball ($S_1(i)$) are used to represent the two embedding strengths. The binary sequences are generated which have the total length of n. The binary sequences are generated by the key. With the different keys, the binary sequences Template(i, p, q) are quite different from each other. In position k, whether to choose $S_0(i)$ or $S_1(i)$ as $S(i)$ depends on the Template(k, key, p). For every k, if Template$(k, key, p) = 0$, we choose the white ball ($S_0(i)$) as $S(i)$, and if Template$(i, key, p) = 1$, we choose the white ball ($S_1(i)$) as $S(i)$. At last, the embedding strength of visible watermark $S(i)$ is finished.

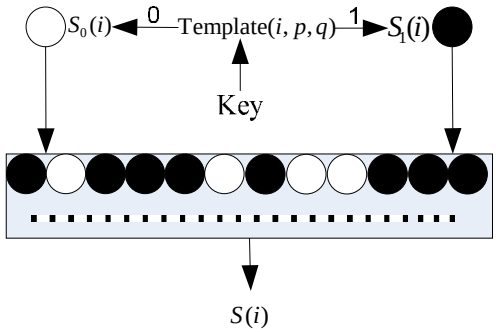


Fig. 2 The Flowchart of Generating the Watermark Strength Coefficients

IV. Simulation Results

(a) (b)

Fig. 3 Test Image: (a)Watermark (b) Original Image

We tested the proposed algorithm on a number of images (shown in Fig. 3). The watermark image is a 33×85 8-bit image. The original image is a 512×512 24-bit image. The original image and the watermark image firstly are transformed from RGB to YUV color space. The watermark embedding process is based on the Y component. At the input to the encoder, original image and watermark image samples are grouped into 8×8 blocks. After the process of discrete cosine transform (DCT), each of the 64 DCT coefficients is uniformly quantized in conjunction with a Quantization Table. Then, all of the quantized coefficients are ordered into the "zig-zag" sequence. After the "zig-zag", the watermark in added to the original image. The watermarking removing process is reverse as the process of watermarking embedding.

A. Analysis of Visual Quality and Security.

In the proposed scheme, the embedding strength of the visible watermark is modulated by the template. That is to say, to remove the visible logo, the user should recover the template thoroughly. From the cryptographic viewpoint, brute-force attack [10] is a solution to break a cryptosystem. In the proposed scheme, the watermark image is 33×85 size. Every pixel has two states $S_0(i)$ and $S_1(i)$. Thus, the brute-force space is 2^{5610} which is secure enough to resist the brute-force attack.

In Section 3, the watermarking strength $S_0(i)$ and $S_1(i)$ are defined but not given in detail. In our visible and removable algorithm, we set $S_0(i)$ different from $S_1(i)$ in most case. $S_0(i)$ and $S_1(i)$ can be got by the following equation (5).

$$\begin{cases} S_0(i) = a \\ S_1(i) \in [c, d] \end{cases}, \quad k = 0,1,2,...n-1. \tag{5}$$

Here, a, c and d are three constants. a adjusts the energy of original image. c and d are chosen by the demand of security.

We tested different a, c and d and the results are as follows (See in Fig. 3)

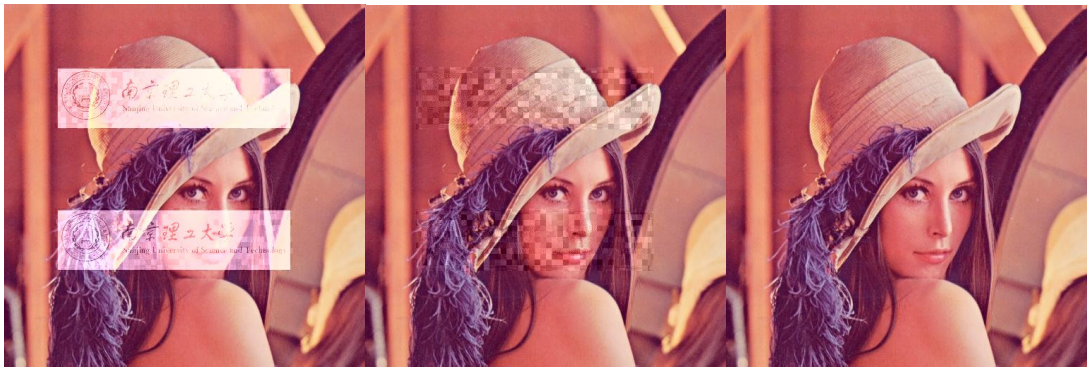
As can be seen from Seen from Fig. 4 5 and 6, there is much distortion when the visible watermark is removed with the wrong key. Users with the right key can completely remove the visible logo from the watermarked image. Additionally, the distortion becomes more serious when parameters a, c and d increases. To avoid pixel overflow, $a = 0.5$, $c = 0.6$ and $d = 0.8$ is preferred.

B. Effect on JPEG compression.

In most cases, multimedia content is stored and transmitted in compressed form to conserve bandwidth. In this paper, the visible watermark is embedded into the host image in the process of the JPEG encoding. This operation will cause the JPEG file size increases. Thus, the proposed scheme which effects on JPEG compression should be consider and is defined as

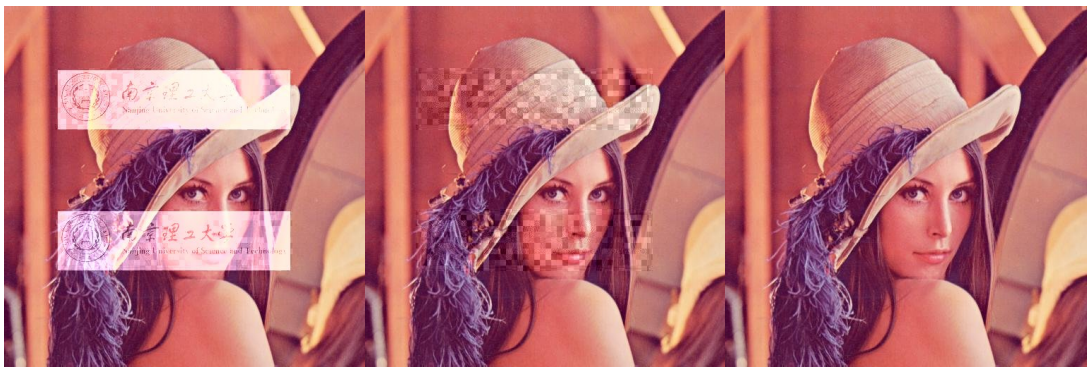
(a) (b) (c)

Fig. 4 Results for $a = 0.2$, $c = 0.3$ and $d = 0.5$: (a) Watermarked Image (Psnr: 17.4), (b) Remove without Right Key (Psnr: 27.3), (c) Remove with Right Key (Psnr:58.7)



(a) (b) (c)

Fig. 5 Results for $a = 0.5$, $c = 0.6$ and $d = 0.8$: (a) Watermarked Image (Psnr: 15.2), (b) Remove without Right Key (Psnr: 22.4), (c) Remove with Right Key (Psnr:56.8)



(a) (b) (c)

Fig. 6 Results for $a = 0.7$, $c = 0.7$ and $d = 0.9$: (a) Watermarked Image (Psnr: 12.3), (b) Remove without Right Key (Psnr: 20.3), (c) Remove with Right Key (Psnr:55.7)

$$EJC = \frac{\text{Image}_{embed} - \text{Image}_{ori}}{\text{Image}_{ori}} \times 100\% . \quad (6)$$

Here, Image_{embed} is the size of the watermarked copy and Image_{ori} is the size of the original image.

4 images are tested and Fig. 7 gives the average result of the impact on compression rate. As can be seen, the scheme impact on the compression rate a lot when the compression factor (Q) is smaller than 50. The *EJC* decreases while Q increases. There is little effect on JPEG compression of the scheme when the compression factor is larger than 75 (default compression factor). Based on the simulation results, the effect on the JPEG compression is acceptable when the visual quality is high (Q>55).

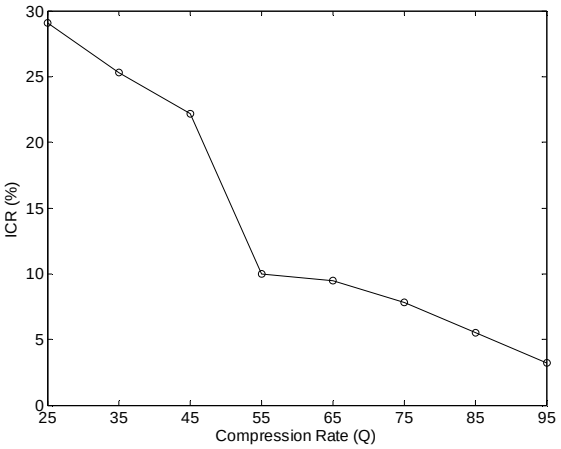


Fig. 7 The effect on the JPEG Compression

V. Conclusion

In this paper, a secure visible and removable watermarking scheme has been proposed. To enhance the security, a mathematical template has been developed which can randomize the coefficients of the watermarking embedding strength. Experiments show that watermarked image is visibility and transparency. Users with the write key can remove the watermark and obtain a high quality of the recovered image. With the wrong key, users can only remove part of the visible logo and obtain a low quality of the image by illegally removing. In the future work, we can explore the HVS model into our algorithm to obtain better visual quality and better security.

Acknowledgment

This study was supported by the China Post Doctor Foundation of China (Grant No. 20070421017), NSF of Jiangsu, Post Doctor Foundation of Jiangsu province and Excellent Doctoral Dissertation Innovation Foundation of Nanjing University of Science and Technology

References

[1] I. Cox, J. Kilian, F. Leighton, F. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, Vol. 6, No. 12, Dec. 1997, pp.1673-1687.

[2] Barni, M., "Improved wave-Based Watermarking through Pixel-Wise Marking." IEEE Transactions On Image Processing, 2001. 10(5): p. 783-791.

[3] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," in Proc. IEEE Int. Symp. Circuits and Systems, Vol. 2, BANGKOK, THAILAND, MAY 2003, PP. 912–915.

[4] M.S. Kankanhalli, R. Lil, and R. Ramakrishnan, "Adaptive Visible Watermarking of Images," Proc. IEEE Int'l Conf. Multimedia Computing and Systems, IEEE CS Press, 1999, pp. 68-73.

[5] S.P. Mohanty, K.R. Ramakrishnan, and M.S. Kankanhalli, A dual watermarking technique for image, Proc.7th ACM Int. Multimedia Conf. 2(1999) 9–51.

[6] Yongjian Hu, Sam Kwong, Jiwu Huang. "An Algorithm for Removable Visible Watermarking." Ieee Transaction on Circuits and Systems for Video Technology, Vol. 16, No.1, January 2006.

[7] Meng and S. –F Chang, "Embedding Visible Video Watermarks in the Compressed Domain," IN PROC. ICIP, OCT. 4–7, 1998, VOL. 1, PP. 474–477.

[8] Min-Jen Tsai, Chih-Wen Lin. "The Collaboration of Noise Reduction and Human Vision System Models for a Visible Watermarking Algorithm." Image Processing, 2007. ICIP 2007. IEEE International Conference on. Volume: 3, On page(s): III - 273-III – 276, 2007.

[9] P.-M. Chen, "A Visible Watermarking Mechanism Using A Statistic Approach," IN PROC. 5TH INT. CONF. SIGNAL PROCESSING, 2000, VOL. 2, PP. 910–913.

[10] B. M. Macq And J. J. Quisquater. "Cryptology for Digital TV Broadcasting." PROCEEDINGS OF THE IEEE, 83(6): 944-957, 1995.