A SEMI-FRAGILE WATERMARKING SCHEME FOR IMAGE TAMPER LOCALIZATION AND RECOVERY

[1] LINTAO LV, [2] HUA FAN, [3] JINFENG WANG, [4] YUXIANG YANG

[123]School of Computer Science and Engineering, Xi'an University of Technology, 710048, PR China

[4]School of Mechanical Instrumental Engineering, Xi'an University of Technology, 710048, PR China

E-mail: [1]lvlintao@xaut.edu.cn , [2]huafan0408@gmail.com, [3]wjf1986114@163.com
, [4]yyxflyinger@gmail.com

ABSTRACT

A novel semi-fragile watermarking scheme for Image tamper localization and recovery is proposed. The Logistic map is used to encrypt the feature extracted from the original image, then the generated watermark is embedded into the middle-frequency DCT coefficients of each block after being ordered in zigzag manner based on invariance properties of DCT coefficients before and after JPEG compressions. As for authentication, firstly, the feature information is extracted after decryption, and compared it with reconstructed feature information, then, the tamper matrix is generated. Finally, recover the invalid blocks by using bicubic interpolation. Experimental results illustrate that the watermarked image has good imperceptibility and can tolerate the common content-preserving image processing. It is also sensitive to malicious manipulations and can localize and recover tampered regions approximately.

Keywords: *Image authentication; Semi-fragile; Tamper localization; Recovery*

1. INTRODUCTION

Due to the wide spread and rapid growth of image processing software, people can replicate and modify digital images easily nowadays. Thus, digital watermarking has been presented to protect the copyright and integrity of image content. In a watermarking system, there are two important properties: robustness and imperceptibility. Usually, a robust watermark is used to protect the copyright, while a fragile or semi-fragile watermark is used to verify the authenticity [1-2]. Semi-fragile watermarking has properties of both fragile watermarking and robust watermarking, which can authenticate the reliability of digital contents [3].

Many semi-fragile watermarking schemes for image authentication have been proposed [4-7]. The common model of a semi-fragile watermark authentication is that the authentication watermark is the features extracted from one given image and then encrypted with sender's private key. To verify the integrity of the transmitted images, the authentication procedure extracts watermark from the received image and then decrypted by sender's public key. Many watermarking-based authentication schemes only determine the integrity of the image contents and locate the modification areas, but lack of the recovery function. However, there are many applications not only require the detection and location, but also require recovery tampered content approximately [8].

2. DIGITAL WATERMARKING GENERATION AND EMBEDDING ALGORITHM

2.1 Chaotic System.

In mathematics and physics, Logistic map is the classical dynamic system which is researched widely in chaos theory. The definition is the following:

$$x_{k+1} = \mu x_k (1 - x_k) \text{, Where } 0 \le \mu \le 4 \quad (1).$$

Experiments show that the system will be completely chaotic when $x_k \in (0,1)$ and $\mu \in (3.57, 4]$. That is to say, the generated sequence with two different initial values is irrelevant. The sequence generated by Logistic map is simple and sensitive to initial conditions.

The initial values of x_0 and μ will be used as a secret key K_1.

2.2 Digital Watermark Generation Algorithm.

The watermark is generated from the LL3 subband of three-level wavelet decomposition of the original image, which is the best description of the original image at low resolution. Assume I is the original gray-level host image, and the number of gray levels is 256.

The steps of watermark generation are described as follows.

Step1: Take three-level DWT on $M \times M$ original image I, obtain the LL3 subband image L, the size of L is $\frac{M}{8} \times \frac{M}{8}$.

Step2: Set the three LSBs of each pixel of the L to zero. According the grey values of each pixel, generate the watermark W.

Step3: Watermark encryption. The extraction of watermark is public; therefore encryption for watermark is necessary. In this paper Logistic map just mentioned above is utilized to generate the pseudo random sequence X. Subsequently the output sequence X is converted to a binary mask sequence M, the length is the same as W. Then XOR operation on watermark W and mask sequence M is performed to obtain the encryption watermark sequence S, $S = W \oplus M$.

2.3 Digital Watermark Embedding Algorithm.

The scheme is based on invariance properties of DCT coefficients before and after JPEG compressions [9]. Experiments demonstrate that the invariant relationships between two coefficients in a block before and after JPEG compression. Therefore, we can use this property to embed watermark. To find a tradeoff between perceptual invisibility and the robustness of watermarking, after order the DCT coefficients in a zigzag manner, we embed the watermark into the middle frequency coefficients from 11 to 20.

According to human visual system [10], the human eye is not sensitive to the change of rich texture and edge, while sensitive to the change of smooth area. Therefore, before the watermark embedded into image, scramble the original image is necessary to ensure the perceptual invisibility of watermarked image. In this scheme, Arnold cat mapping is used to scramble the original image. The steps of watermark embedding are described as follows.

Step1: Scramble the original image I using secret key K_2, generate image I_2.

Step2: Divide the image I_2 into 8×8 non-overlapping blocks and transforming each block using DCT.

Step3: Each DCT-transformed block is quantized using a quantization matrix corresponding to a 50% quality JPEG. Then the coefficients are ordered in a zigzag manner and their values are encoded using a fixed number of bits.

Step4: According to invariance properties of JPEG just mentioned above, embed the watermark sequence S into middle frequency coefficients from 11 to 20. The embed rules as follows.

Assume the total block number of I_3 is n, $n = \frac{M}{8} \times \frac{M}{8}$. The total pixel number of S is n. Obtain the high five bit of each pixel of S, denoted as $s(i, j)_r$, $r \in [4,8]$, $i \in [1, \frac{M}{8}]$, $j \in [1, \frac{M}{8}]$. The middle frequency coefficients denoted as $x_{11}, x_{12}, \ldots, x_{20}$.

If $s(i, j)_8 = 1$ then if $x_{11} < x_{16}$, then modify x_{11} and x_{16}, so as to $x_{11} > x_{16}$.

Else if $s(i, j)_8 = 0$ then if $x_{11} > x_{16}$, then modify x_{11} and x_{16}, so as to $x_{11} < x_{16}$.

If $s(i, j)_7$ =1 then if $x_{12} < x_{17}$, then modify x_{12} and x_{17}, so as to $x_{12} > x_{17}$.

Else if $s(i, j)_7 = 0$ then if $x_{12} > x_{17}$, then modify x_{12} and x_{17}, so as to $x_{12} < x_{17}$.

......

If $s(i, j)_4 = 1$ then if $x_{15} < x_{20}$, then modify x_{15} and x_{20}, so as to $x_{15} > x_{20}$.

Else if $s(i, j)_4 = 0$ then if $x_{15} > x_{20}$, then modify x_{15} and x_{20}, so as to $x_{15} < x_{20}$.

Step 5: Repeat Step 4, until all of the blocks are processed.

Step6: Divide the processed image into 8×8 blocks and transforming each block using IDCT, using secret key K_2 to inverse scramble the image, generate the watermarked image $\overline{I}$.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. DIGITAL WATERMARK EXTRACTION AND AUTHENTICATION ALGORITHM

3.1 Digital Watermark Extraction Algorithm.

Image authentication and restoration are based on the watermark extracted from watermarked image. The steps of watermark extraction are described as follows.

Step1: Scramble the watermarked image $\bar{I}$ using secret key K_2, generate image $\bar{I}_2$.

Step2: Divide the image $\bar{I}_2$ into 8×8 blocks and transforming each block using DCT.

Step3: Obtain the middle frequency coefficients from 11 to 20 of each block after dct coefficients are ordered in a zigzag manner.

Step4: In each block, the watermark bit w_i is extracted as follows:

$$w_8 = \begin{cases} 1, & if\ x_{11} > x_{16} \\ 0, & if\ x_{11} < x_{16} \end{cases}, \quad w_7 = \begin{cases} 1, & if\ x_{12} > x_{17} \\ 0, & if\ x_{12} < x_{17} \end{cases}, .. \quad (2).$$

After all the watermark bits are extracted, the watermark $W1$ is obtained.

3.2 Digital Watermark Authentication Algorithm

Step1: Based on secret key K_1, the mask sequence M is obtained by Logistic map. Then the watermark Wb is computed as:

$$Wb = W1 \oplus M \quad (3)$$

Step2: Based on LL3 subband image of the watermarked image, the extracted watermark Wf is obtained. The process is similar to that of watermark generation.

Step3: Image authentication. Define the tamper matrix Wt as follows:

$$Wt = Wb \oplus Wf \quad (4)$$

After malicious attacks, most watermark error pixels in Wt would cluster in the attacked regions, while after content preserving attacks ,most watermark error points would be spread across Wt. So we delete the isolated error points in the tamper matrix Wt before authentication. An error point is an isolated one if none of its eight neighbor points is an error point. Then we can distinguish malicious attacks from content-preserving attacks through the pattern of the filtered tamper matrix, after all of the isolated error points are deleted from the tamper matrix.

3.3 Image restoration.

Due to practical application in image authentication, not only require to determine whether the image is tampered or not, but also requires to recovery tampered content approximately. The algorithm is also based on this. After the image authentication, a tamper matrix Wt is obtained. In order to restore the original image, replace each invalid blocks by correct area which come from the image enlarge watermark Wb.

There are three methods to enlarge an image: Nearest Neighbor Interpolation, Bilinear Interpolation, and bicubic interpolation. Experiments demonstrate that the third method is the best.

4. EXPERIMENTAL RESULTS

The experiments were implemented on gray-level images with size of 512×512 pixels. The K_1 is set to 0.4123, K_2 is set to 24, and "Haar" was chosen for wavelet transform. Test the watermarked image in transparency, the JPEG compression, Salt-and-pepper noise and malicious attack.

4.1 Quality of watermarked image.

The quality metric is based on PSNR. The original images and the watermarked images are shown in Figure 1. 1(a) is the original images, and 1(b) is the watermarked images. The PSNR are 44.2936dB. It shows that the proposed algorithm has satisfying perceptual invisibility.

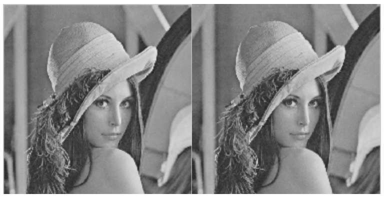
(a) (b)

Figure 1 Original image and watermarked image

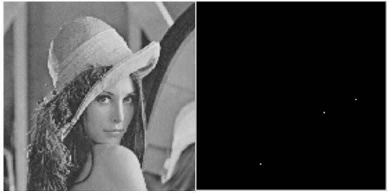
(a) (b)

Figure 2 JPEG compression, quality=90

4.2 JPEG compression.

Lossy compression, such as JPEG, is widely used in image operation, so the authentication algorithm should be robust to image compression operation to distinguish it from malicious tamper. Figure 2 and Figure 3 are the experimental results of JPEG compression. The JPEG compression qualities are 90 and 80 respectively. (a) is compressed watermarked image with different compression qualities, (b) is the authentication result. The authentication results show that the watermarked images have not been tampered. Table 1 shows the comparison of the normalized correlation against JPEG between proposed method and reference [11]. Experiments demonstrate that our method is better.

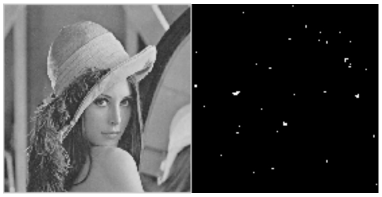

Figure 3 JPEG compression, quality=80

4.3 Adding noise.

Figure 4 and Figure 5 shows the result of adding salt-and-pepper noise to watermarked image. The rates of the noise are 0.005 and 0.02 respectively. (a) is the watermarked image with different rate of noise, (b) is the authentication result. Also the authentication results show that the watermarked images have not been tampered.

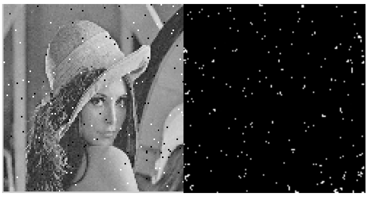

Figure 4 Salt-and-pepper noise, rate=0.005

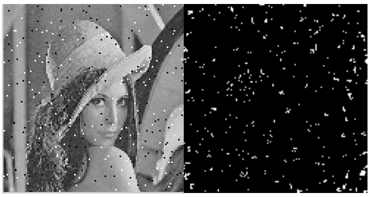

Figure 5 Salt-and-pepper noise, rate=0.02

4.4 Tampering attacks.

We perform malicious attacks on two watermarked images. There are one, two tampered regions in the watermarked images respectively. Figure 6 and Figure 7 show the results of tamper detection and localization. (a) is the watermarked image, (b) is the tampered image, (c) is the authentication result, (d) is the recovered images. The authentication results clearly show that the tampers can be detected, localized accurately and recovered.

Table 1 Comparison of the normalized correlation against JPEG

Quality	QF=50	QF=60	QF=70	QF=80	QF=90
Proposed	0.9993	0.9994	0.9998	1.0000	1.0000
Ref.[11]	0.6874	0.7394	0.8174	0.9070	0.9710

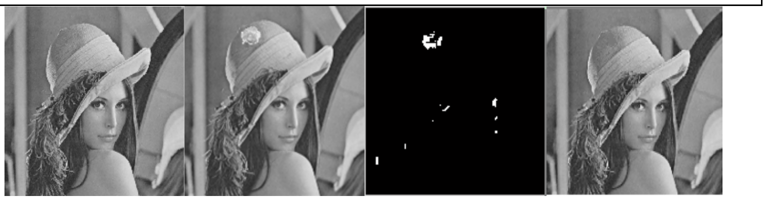

Figure 6 Tampering test of lenna

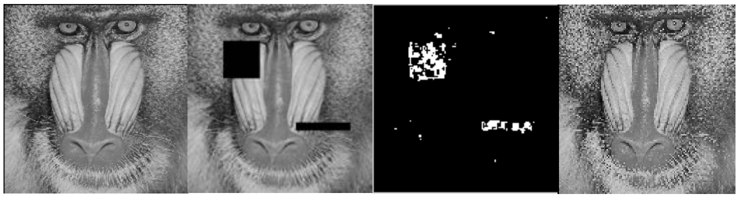

Figure 7 Tampering test of baboon

5. CONCLUSIONS

In this paper, a semi-fragile watermarking scheme for Image tamper localization and recovery is proposed. The watermarked image has good imperceptibility and can tolerate the common content-preserving image processing. Meanwhile, it has a good capability of localizing and recovering the tampered regions. Experimental results show the effectiveness of the proposed scheme.

REFERENCES

[1] R. Petrovic,"Digital Watermarks for Audio Integrity Verification", *Serbia and Montenegro, Nis, September* 2005 28-30

[2] W.H. Chang and L.W. Chang,"Semi-Fragile Watermarking for Image Authentication, Localization, and Recovery Using Tchebichef Moments", *Communications and Information Technologies (ISCIT)*, 2010

[3] Zhou, H., H. Li, et al. "Semi-fragile Watermarking Technique for Image Tamper Localization."*International Conference on Measuring Technology and Mechatronics Automation*, 2009 519-523

[4] M.j. Tsai and C.C Chien,"A Wavelet-Based Semi-Fragile Watermarking with Recovery Mechanism", *IEEE International Symposium on Circuits and Systems*, May 2008pp.3033-3036

[5] D. Zhang and Z. Pan, “A contour-based semi-fragile image watermarking algorithm in DWT domain,” *Proc. ETCS* vol. 3, 2010, pp. 228-231.

[6] K. Maeno, S. Qibin, S.F. Chang and M. Suto “New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization”. *IEEE Trans Multimedia*;8(1) 2006:32–45

[7] X. Wang, “A novel adaptive semi-fragile watermarking scheme based on image content,” *ACTA AUTOMATICA SINICA* vol. 33, no. 4, 2007 pp. 361-366,.

[8] P. Tsai and Y.Chen. Hu ," A Watermarking-Based Authentication with Malicious Detection and Recovery ",*Fifth International Conference on Information, Communications and Signal Processing*,2005

[9] C.Y. Lin and S.F. Chang, "Semi-Fragile Watermarking for Authenticating JPEG Visual Content", *Proc. SPIE*. Security and Watermarking of Multimedia Contents, San Jose, California, January 2000, pp. 140-151.

[10] H.f. Yang and X.M. Sun, "Semi-Fragile Watermarking for Image Authentication and Tamper Detection Using HVS Model", *International Conference on Multimedia and Ubiquitous Engineering* 2007

[11] H.F.Yang and X.M. Sun. “Semi-fragile Watermarking for Image Authentication and Tamper Detection Using HVS Model”. *Proc. of International Conference on Multimedia and Ubiquitous. Seoul.Southkorea*: [s. N.], 2007