Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 526174, 10 pages
http://dx.doi.org/10.1155/2015/526174

Research Article

Cryptanalysis and Improvement of the Robust and Blind Watermarking Scheme for Dual Color Image

Hai Nan,[1] Bin Fang,[1] Weibin Yang,[2] Jiye Qian,[1] Ming Li,[3] Yi Liu,[4] and Yushu Zhang[1]

[1]*College of Computer Science, Chongqing University, Chongqing 400044, China*
[2]*College of Automation, Chongqing University, Chongqing 400044, China*
[3]*College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China*
[4]*PetroChina Chongqing Marketing Jiangnan Company, Chongqing 400060, China*

Correspondence should be addressed to Bin Fang; fb@cqu.edu.cn

Received 2 July 2014; Accepted 2 September 2014

Academic Editor: Ezzat G. Bakhoum

With more color images being widely used on the Internet, the research on embedding color watermark image into color host image has been receiving more attention. Recently, Su et al. have proposed a robust and blind watermarking scheme for dual color image, in which the main innovation is the using of two-level DCT. However, it has been demonstrated in this paper that the original scheme in Su's study is not secure and can be attacked by our proposed method. In addition, some errors in the original scheme have been pointed out. Also, an improvement measure is presented to enhance the security of the original watermarking scheme. The proposed method has been confirmed by both theoretical analysis and experimental results.

1. Introduction

With the rapid development of the Internet, a great deal of digital data can be easily accessed, and the copyright of digital content against privacy and malicious manipulation becomes increasingly important. A variety of theories can be used for the security applications [1–3]. Watermarking [4–6] is a widely used technology for ensuring authenticity, copyright violation detection, and proof of ownership or distributorship of the content. The existing watermarking technologies always equip one of the two distinct properties: robustness and fragility. Robustness means that the embedded watermark in the host media cannot be easily modified or removed. Thus the robust watermarking can be used to protect ownership of the digital content [7]. Contrarily, the fragile watermarking is sensitive to any modification of the host media and can be used to authenticate the integrality of the protected content [8].

Watermarking technologies can be classified into two categories: blind detection watermarking technologies and nonblind detection watermarking technologies [9] according to whether it requires the original data when extracting watermark. The blind detection means to extract watermark without the help of the original host image and the original watermark [10, 11], while the nonblind detection requires the original host image or the original watermark [12, 13]. Generally, the blind detection watermarking technologies are less robust than the nonblind detection ones, but they are more realistic in many applications and have been recently receiving more attention.

Su et al. [14] recently proposed a new robust and blind digital watermarking algorithm for dual color images based on the two-level DCT, which aimed to protect the copyright under JPEG compression attack effectively. In the original scheme, the authors embed extra information into the host image by modifying the selected AC coefficients of the result obtained by two-level DCT. The method is effective; nevertheless, it is not secure due to the fact that the embedded watermark can be replaced while the modification of the host image is imperceptible, and therefore the purpose of copyright protection cannot be achieved. In this paper, we propose a novel attack method to replace the watermark embedded in the protected image. Moreover, an improvement measure is presented to enhance the security of the original scheme.

The rest of the paper is organized as follows. Section 2 presents a brief introduction of Su et al.'s scheme. By correcting the errors and analyzing the weakness of the original scheme, the attack method is proposed in Section 3. The improvement measure is described in Section 4. Section 5 concludes this paper.

2. Review of Su et al.'s Scheme

In Su et al.'s scheme [14], the two-level DCT technology is used to achieve higher concentration of energy; therefore the watermark information can be embedded easily. Before watermark embedding, the color watermark should be first preprocessed to change into the binary sequence form. That is, three components red (R), green (G), and blue (B) of the original watermark are separated out and then are DCT transformed, respectively. After compress coding and random permutation, the final binary sequence to be embedded is obtained.

2.1. Watermark Embedding. The host RGB image should be first transformed into YIQ mode using

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.275 & -0.322 \\ 0.211 & -0.523 & 0.312 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix}. \quad (1)$$

Then, the luminance component Y of the block sized 8×8 is processed by two-level DCT. The obtained 4×4 embedding blocks (upper-left corner) are shown in Figure 1, where the bold characters, that is, nine AC coefficients (**C3**, **C4**, **C7**, **C8**, **C11**, **C12**, **C14**, **C15**, and **C16**), denote the selected positions for watermark embedding.

To embed the obtained binary sequence, that is, the preprocessed color watermark, into the selected positions, the selected coefficients should be modified according to

$$C^* = \begin{cases} A_k, & \text{if } x = 0, \operatorname{argmin} |A_k - C|, \\ B_k, & \text{if } x = 1, \operatorname{argmin} |B_k - C|, \end{cases} \quad (2)$$

where x denotes the watermark bit, C^* is the modified coefficient after embedding x in coefficient C, k is the bit number of the watermark, $A_k = \lfloor |C|/T \rfloor \times k + T/4$, $B_k = \lfloor |C|/T \rfloor \times k + 3\times T/4$, $\lfloor \cdot \rfloor$ denotes the least nearest integer, and $|\cdot|$ is the absolute value operation. T is chosen to determine the embedding strength and the difference between C^* and C, in the worst condition, is $T/2$.

After modifying the coefficients, the inverse two-level DCT transform and inverse YIQ color transform should be performed to restore the original state of the host image. Thus, the watermark bits are embedded into the frequency domain of the host image based on two-level DCT.

2.2. Watermark Extraction. To extract the watermark from a watermarked host image, one should first acquire the luminance information through YIQ color transform and, then, use two-level DCT to get the modified coefficients C^{**}.

$C1$	$C2$	**C3**	**C4**
$C5$	$C6$	**C7**	**C8**
$C9$	$C10$	**C11**	**C12**
$C13$	**C14**	**C15**	**C16**

Figure 1: The selected positions for embedding watermark in each image block.

Three segments watermarks $x_{i,k}$, $i = 1, 2, 3$, of the original watermark can be extracted using

$$x_{i,k} = \begin{cases} 0, & \text{if } \operatorname{mod}(C^{**}, T) \le \dfrac{T}{2} \\ 1, & \text{if } \operatorname{mod}(C^{**}, T) > \dfrac{T}{2}. \end{cases} \quad (3)$$

Then, according to the majority principle, the watermark bit x_k can be obtained from $x_{i,k}$. By inverse random permutation, decompression technology, and the inverse coding, the color watermark can be recovered.

3. The Cryptanalysis and Attack

3.1. Mistake in the Original Scheme. In the embedding process of the original scheme, there are some mistakes in (2); for example, suppose $C = 9$ and $T = 4$; then $A_k = 2 \times k + 1$ and $B_k = 2 \times k + 3$; according to (2), if the embedded x is 0, then $\min|A_k - C|$ is 0; here $k = 4$ and $C^* = A_k = C$. Similarly, if 1 is embedded, $k = 3$ and $C^* = B_k = C$. Thus, no matter which value is embedded, the modified coefficient C^* is not affected, and the watermark cannot be extracted exactly.

The appropriate approach is to change A_k and B_k to

$$A_k = k \times T + \frac{T}{4}, \qquad B_k = k \times T + \frac{3 \times T}{4}, \quad (4)$$

where k is an integer. Then, the modified coefficient C^* is obtained from (2). The following steps demonstrate that the largest difference between C and C^* is $T/2$.

Suppose the embedded $x = 0$.

Let $q = \lfloor (C - T/4)/T \rfloor$; then

$$C - \frac{T}{4} = q \times T + r, \quad \text{where } r \in [0, T). \quad (5)$$

According to the range of r, it can be divided into two cases.

Case 1 ($r \in [0, T/2)$). Let $k = q$; we obtain

$$\left|(k - q) \times T - r\right| \in \left[0, \frac{T}{2}\right); \quad (6)$$

that is,

$$\left|k \times T - (q \times T + r)\right| \in \left[0, \frac{T}{2}\right). \tag{7}$$

According to (5),

$$\begin{aligned} &\left|k \times T - \left(C - \frac{T}{4}\right)\right| \in \left[0, \frac{T}{2}\right), \\ &\left|\left(k \times T + \frac{T}{4}\right) - C\right| \in \left[0, \frac{T}{2}\right); \end{aligned} \tag{8}$$

then

$$\left|A_k - C\right| \in \left[0, \frac{T}{2}\right). \tag{9}$$

Case 2 ($r \in [T/2, T)$). Let $k = q + 1$; we obtain

$$\left|(k - q) \times T - r\right| = |T - r| \in \left(0, \frac{T}{2}\right]. \tag{10}$$

According to (6)–(9),

$$\left|A_k - C\right| \in \left(0, \frac{T}{2}\right]. \tag{11}$$

Based on the above two cases, we deduce $|A_k - C| \le T/2$.

Suppose the embedded $x = 1$; similarly, we obtain $|B_k - C| \le T/2$.

3.2. Weakness of the Original Scheme. According to Kerckhoffs' principle [17], when analyzing an encryption algorithm, an assumption is that the cryptanalyst knows exactly the design and working of the cryptosystem. Namely, cryptanalyst knows everything about the cryptosystem except for the secret keys.

In the original scheme, according to (3) and the known coefficient T, the scrambled watermark bits x_k can be extracted from watermarked image. At the same time, according to (2) and the known coefficient T, any arbitrary bits can be embedded into the watermarked image. So, we can erase or change the original watermark embedded in the image; thus the copyright protection would fail. The details of the attack scheme are introduced in the next section.

3.3. Method to Modify the Watermark. Suppose I_O is the original image and I_A is the watermarked image carrying the watermark W_A. The attacker has a different image, called I_B, carrying another watermark W_B. The attacker aims to replace W_A of I_A with W_B to change the copyright of I_O. The two attack steps are as follows.

Step 1. Follow the watermark extraction process proposed in Section 2 and obtain the permuted watermark bits x_k from image I_B with known T in (3).

Step 2. Embed the permuted watermark bits x_k into image I_A using (2).

Then, the watermark W_A embedded in the original image is replaced with W_B, which is possessed by the attacker.

The fidelity of the attacked image is analyzed below. Let C denote the two-level DCT coefficient of I_O and C_A^* and C_B^* denote the corresponding coefficients of I_A and I_B, respectively. Based on the statements in Section 3.1, $|C_A^* - C| \le T/2$, $|C_B^* - C_A^*| \le T/2$, and then $|C_B^* - C| \le T$, which means the difference of the coefficients between the original image and the attacked image increases, and, in the worst condition, the difference will be double. Since the modification occurred in the high-frequency coefficients of the two-level DCT, the PSNR (peak signal-to-noise ratio) value of the modified image is acceptable, and the invisibility of the watermark can be ensured. The experiments in the next section also verify this proposal.

3.4. Experiments. PSNR is defined in (12), which may be used to evaluate perceptual distortion of the proposed scheme:

$$\mathrm{PSNR} = \frac{\sum_{i=1}^{3} \mathrm{PSNR}_i}{3}, \tag{12}$$

where $i = \{1, 2, 3\}$, respectively, denotes the R, G, B components, and PSNR_i presents the PSNR value of i component:

$$\mathrm{PSNR}_i = 10\lg \frac{M \times N \times \max\left\{\left[H(x, y, i)\right]^2\right\}}{\sum_{x=1}^{M} \sum_{y=1}^{N} \left[H(x, y, i) - H'(x, y, i)\right]^2}, \tag{13}$$

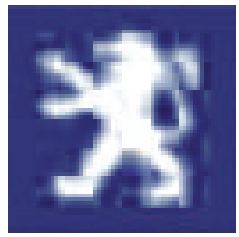
where $H(x, y, i)$ and $H'(x, y, i)$ are the pixel values location at (x, y) of i component of the original host image and the watermarked image. Generally, the larger the PSNR value is, the more invisible the watermark is.

Figure 2(a) shows the original watermarked image of size 512×512. The original watermark of size 64×64 embedded in Figure 2(a) is given in Figure 2(b). The attacker's image whose size is the same as that of the original image is shown in Figure 2(c). Figure 2(d) displays the watermark embedded in the attacker's image using the original scheme with different secret key, the size of which is also $64 * 64$. Figure 2(e) which seems to be the same as Figure 2(a) is the attacked image using the proposed method, and the PSNR value is near to that of Figure 2(a). Figure 2(f) shows the extracted watermark from Figure 2(e). Since Figure 2(f) is totally different from the original watermark that is shown in Figure 2(b), the copyright protection of the original image is invalid.

4. Improvement Measure

The main drawback of Su et al.'s scheme [14] is that one can easily obtain and replace the scrambled watermark from the host image by the known T. Moreover, the scheme is not dependent on the plain image, which would increase the possibility of attacks. In order to overcome the above drawbacks and to improve security, a secret key must be introduced into the coefficients modification step. We propose the improvement measure here.

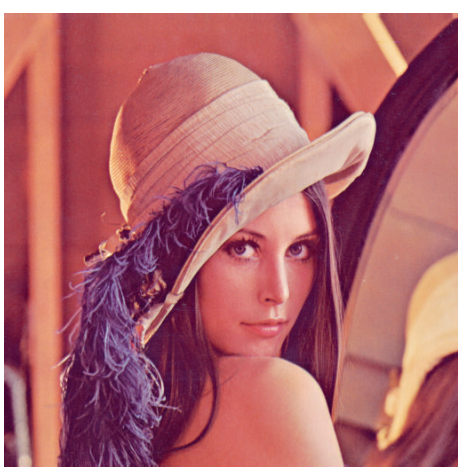
(a) PSNR: 46.3667



(b)

(c) PSNR: 46.5436

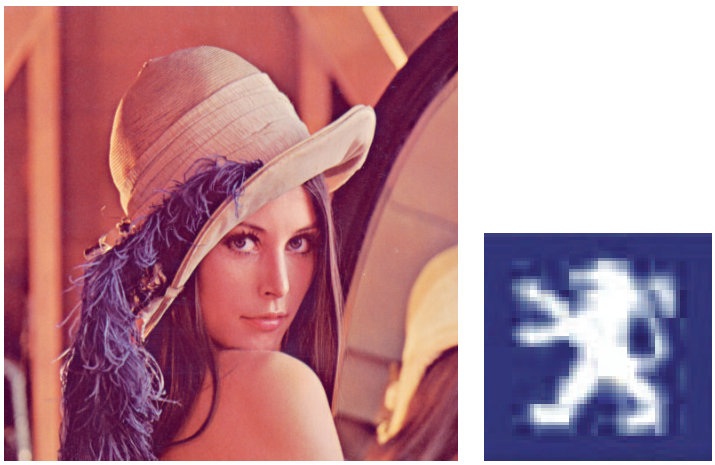
(d)



(e) PSNR: 44.9439

(f)

Figure 2: Attack of the original scheme. (a) The original watermarked image and (b) original watermark; (c) the attacker's watermarked image and (d) the watermark in (c); (e) the attacked image of (a); (f) the extracted watermark from (e).



(a) PSNR: 46.2967 (b)

(c) PSNR: 46.5384 (d)

(e) PSNR: 42.7352 (f)

Figure 3: Attack of the improved scheme. (a) The original watermarked image and (b) original watermark; (c) the attacker's watermarked image and (d) the watermark in (c); (e) the attacked image of (a); (f) the extracted watermark from (e).

Table 1: Performance comparison between the different methods in terms of JPEG compression (CR, compression ratio).

	CR (%)	10	20	30	40	50	60
Reference [15]	PSNR (dB)	35.4	34.8	NA	NA	NA	NA
	NC	1.00	0.29	NA	NA	NA	NA
Reference [16]	PSNR (dB)	35.4	34.8	32.6	31.1	NA	NA
	NC	0.99	0.50	0.12	0.07	NA	NA
Original	PSNR (dB)	33.6428	32.2108	31.8814	31.2290	30.8597	30.4745
	NC	1.0000	1.0000	1.0000	0.9996	0.9792	0.9769
Improved	PSNR (dB)	33.6429	32.2107	31.8816	31.2288	30.8597	30.4744
	NC	1.0000	1.0000	1.0000	0.9995	0.9792	0.9768

4.1. Watermark Embedding

Step 1. The host RGB image should be transformed into YIQ mode using (1) in Section 2.

Step 2. The luminance component Y of the block sized 8×8 is processed by two-level DCT. The obtained 4×4 embedding blocks (upper-left corner) are shown in Figure 1, where the bold characters, that is, nine AC coefficients (**C3**, **C4**, **C7**, **C8**, **C11**, **C12**, **C14**, **C15**, and **C16**), denote the selected positions for watermark embedding.

Step 3. Set the initial parameter α and initial value q_0, which can be considered as the watermarking key, to iterate the chaotic system (14) N_W times, where N_W is the size of scrambled watermark bits:

$$\begin{aligned} &q_{i+1} = \alpha q_i \left(1 - q_i\right), \\ &i = 0, 1, \ldots, N_W - 1, \quad q_i \in (0, 1). \end{aligned} \tag{14}$$

With parameter $\alpha \in (3.5699456, 4]$, the system (14) is in chaotic state [18].

Step 4. Let x be the watermark bit and q be the corresponding pseudorandom numbers obtained from (14). For every x, obtain the integral number Z according to

$$Z = \text{floor}\left(q \times 10^{14}\right) \bmod 7 + 1, \tag{15}$$

where floor(a) returns the largest integer smaller than a and Z is a series of integers ranging from 1 to 7. Then, the remnant AC coefficients ($C1$, $C2$, $C5$, $C6$, $C9$, $C10$, and $C13$) in each block based on two-level DCT are selected according to the values of Z to obtain the C'.

The selected coefficient C' is dependent on the plain host image, so different host image generates different coefficient C', and any modification on the watermarked image will affect the coefficient C' and then will affect the watermark consequently (the explanations are given below), even if the watermark is obtained before.

Step 5. Obtain a bit x' from the selected AC coefficient C' using

$$x' = \begin{cases} 0, & \text{if mod}\left(C', T\right) \le \dfrac{T}{2}, \\ 1, & \text{if mod}\left(C', T\right) > \dfrac{T}{2}. \end{cases} \tag{16}$$

Step 6. The coefficient C^* after watermark embedding can be obtained by the rule stated in

$$C^* = \begin{cases} A_k, & \text{if } x \oplus x' = 0, \text{argmin}\left|A_k - C\right| \\ B_k, & \text{if } x \oplus x' = 1, \text{argmin}\left|B_k - C\right|, \end{cases} \tag{17}$$

where $A_k = k \times T + T/4$, $B_k = k \times T + 3 \times T/4$, k is an integer, and $|a|$ is the absolute value of a. Based on (7), C^* can be easily computed and the difference between C^* and C is very small. In the worst condition, the largest difference between C and C^* is $T/2$.

Step 7. After modifying the coefficients, the inverse two-level DCT transform and inverse YIQ color transform should be performed to restore the original state of the host image. Thus, the watermark bits are embedded into the frequency domain of the host image based on two-level DCT.

4.2. Watermark Extraction

Step 1. Process the watermarked image I_W by the way of Steps 1–5 in the watermark embedding process to get a series of x' using (16).

Step 2. Extract the watermark according to the DCT coefficients based on the following rules. In (18), C^{**} is the DCT coefficient at the low-frequency position of watermarked image and $x_{i,k}$, $i = 1, 2, 3$, are three segments watermarks of the original watermark:

$$x_{i,k} = \begin{cases} x', & \text{if mod}\left(C^{**}, T\right) \le \dfrac{T}{2} \\ \overline{x'}, & \text{if mod}\left(C^{**}, T\right) > \dfrac{T}{2}, \end{cases} \tag{18}$$

where $\overline{x'}$ is the flipped x'.

Table 2: Evaluation of the robustness of the watermarking scheme.

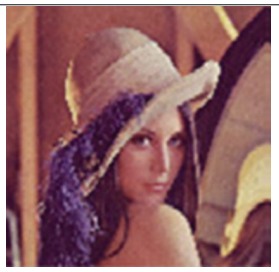
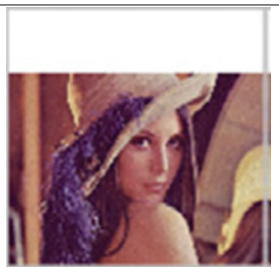
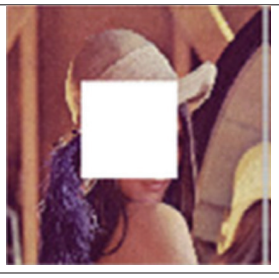
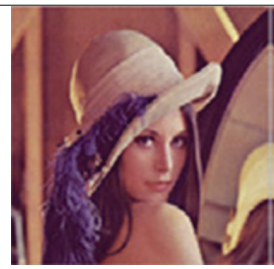
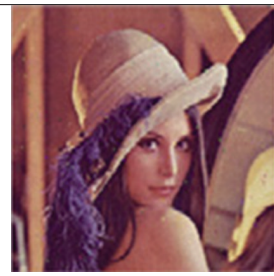
Attacks	Improved scheme				Original scheme	
	Attacked image	PSNR (dB)	Extracted watermark	NC	PSNR (dB)	NC
Brightness + 2		33.1662		0.9999	33.1664	1.0000
Sharpening		33.4241		0.983	33.424	0.9831
Mosaic 3 ∗ 3		30.2472		0.9518	30.247	0.9519
Median filtering		28.8052		0.9093	28.8053	0.9095
Cropping 1		11.5489		0.9999	11.5491	0.9999
Cropping 2		14.0279		0.937	14.0276	0.9369

Table 2: Continued.

Attacks	Improved scheme				Original scheme	
	Attacked image	PSNR (dB)	Extracted watermark	NC	PSNR (dB)	NC
Rotating + 5°		14.683		0.7691	14.681	0.7687
Low pass filtering		28.4824		0.9991	28.4825	0.9991
Adding noise 4%		28.083		0.9971	28.0835	0.9971
JPEG 50%		30.8597		0.9791	30.8597	0.9792

Then, according to the majority principle, the watermark bit x_k can be obtained from $x_{i,k}$. By inverse random permutation, decompression technology, and the inverse coding, the color watermark can be recovered.

4.3. Experiments. Since the selected coefficient from the seven remnant AC coefficients ($C1$, $C2$, $C5$, $C6$, $C9$, $C10$, and $C13$) in each block based on two-level DCT is uncertain, the attacker cannot deduce x' without the secret key mentioned in the above section; therefore the embedded watermark cannot be replaced using the proposed attack method.

In addition, the modifications of the host image during the watermark embedding procedure of the improved scheme are essentially the same as those of the original scheme; that is, only nine AC coefficients (**C3**, **C4**, **C7**, **C8**, **C11**, **C12**, **C14**, **C15**, and **C16**) in each block are selected to embed the watermark, and the largest difference between the coefficients before and after modification is $T/2$. Therefore, the performance of the improved scheme is unchanged. Figure 3 shows an example of the attack to the improved scheme. It can be seen that the PSNRs of Figures 3(a)–3(d) are similar to those of Figures 2(a)–2(d), respectively. Figure 3(e) is the attacked image using the improved method. Figure 3(f) shows the extracted watermark from Figure 3(e). Since the two keys, that is, the initial value q_0 and α of the chaotic map (14), are different between the original watermarked image and the attacker's watermarked image, the extracted watermark from the attacked image is confused, and the copyright protection of the original image will be successful.

In order to measure the robustness of the watermark, we use the normalized correlation (NC) between the original

watermark W and the extracted watermark W', which is shown as follows:

$$\mathrm{NC} = \sum_{i=1}^{3}\sum_{x=1}^{P}\sum_{y=1}^{Q}\left(W(x,y,i)\times W'(x,y,i)\right) \times\left(\sqrt{\sum_{i=1}^{3}\sum_{x=1}^{P}\sum_{y=1}^{Q}\left[W(x,y,i)\right]^2}\right. \times\left.\sqrt{\sum_{i=1}^{3}\sum_{x=1}^{P}\sum_{y=1}^{Q}\left[W'(x,y,i)\right]^2}\right)^{-1}. \quad (19)$$

JPEG compression attack is one of the common attacks that must be verified in watermarking algorithm. In this experiment, the different watermarked images are lossy-compressed with different compression factors ranging from 10 to 100. To prove the robustness of the improved scheme in terms of JPEG compression, we compare our scheme with the earlier works [15, 16] that are based on one-level DCT and also with the original scheme of Su et al. The performance comparison is given in Table 1. Note that "NA" means the corresponding experimental datum is unavailable. As shown in Table 1, the watermark embedded by the proposed scheme can be almost fully extracted from the watermarked image when the compression ratio is 60%. However, under the same conditions, the watermarks embedded by [15, 16] cannot survive after attacked by JPEG compression with compression ratios 20% and 30%, respectively. It demonstrates that the improved and the original scheme have almost the same strong robustness against JPEG compression.

In addition to quantitative measurement, Table 2 gives the evaluation of the robustness of the watermarking scheme in terms of NC [19], in which the watermark is extracted from the watermarked image (as shown in Figure 3(a)) which is under different attacks such as JPEG compression, filtering, and noise addition. The experimental results show that the robustness of the improved watermark scheme keeps consistent with that of the original scheme.

5. Conclusions

This paper attacks Su et al.'s scheme applied for protecting the copyright of digital images. The watermark embedded in the protected image using the original scheme can be replaced by the attacker with another watermark for the purpose of copyright changing, while the modification of the original image is imperceptible. To overcome this defect, the chaotic map is introduced, and the performance of the improvement measure is the same as before. Analysis and experiment show that the proposed method is secure and effective.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the National Key Basic Research Program of China (973 Program 2013CB329103 of 2013CB329100), the National Natural Science Foundations of China (NSFC-61173129), the Specialized Research Fund for the Doctoral Program of Higher Education of China (no. 20120191110026), the Fundamental Research Funds for the Central University (CDJXS11182240 and CDJXS11180004), China Postdoctoral Science Foundation (2014M550456), and Chongqing Postdoctoral Special Funding Project (Xm2014087).

References

[1] S. H. Huddleston and D. E. Brown, "Using discrete event simulation to evaluate time series forecasting methods for security applications," in *Proceedings of the Winter Simulation Conference (WSC '13)*, pp. 2772–2783, Washington, DC, USA, December 2013.

[2] M. Li, "Fractal time series—a tutorial review," *Mathematical Problems in Engineering*, vol. 2010, Article ID 157264, 26 pages, 2010.

[3] M. Li, W.-S. Chen, and L. Han, "Correlation matching method for the weak stationarity test of LRD traffic," *Telecommunication Systems*, vol. 43, no. 3-4, pp. 181–195, 2010.

[4] F. Y. Shih and S. Y. T. Wu, "Combinational image watermaking in the spatial and frequency domains," *Pattern Recognition*, vol. 36, no. 4, pp. 969–975, 2002.

[5] X. Tong, Y. Liu, M. Zhang, and Y. Chen, "A novel chaos-based fragile watermarking for image tampering detection and self-recovery," *Signal Processing: Image Communication*, vol. 28, no. 3, pp. 301–308, 2013.

[6] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 187–193, 2010.

[7] H. S. Malvar and D. A. Florêncio, "Improved spread spectrum: a new modulation technique for robust watermarking," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 898–905, 2003.

[8] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1593–1601, 2001.

[9] H. Luo, F.-X. Yu, Z.-L. Huang, and Z.-M. Lu, "Blind image watermarking based on discrete fractional random transform and subsampling," *Optik*, vol. 122, no. 4, pp. 311–316, 2011.

[10] X. Y. Luo, D. S. Wang, P. Wang, and F. L. Liu, "A review on blind detection for image steganography," *Signal Processing*, vol. 88, no. 9, pp. 2138–2157, 2008.

[11] C. G. Thorat and B. D. Jadhav, "A blind digital watermark technique for color image based on integer wavelet transform and SIFT," *Procedia Computer Science*, vol. 2, pp. 236–241, 2010.

[12] T. K. Tsui, X.-P. Zhang, and D. Androutsos, "Color image watermarking using multidimensional fourier transforms," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 16–28, 2008.

[13] S. Liao, "Dual color images watermarking algorithm based on symmetric balanced multiwavelet," in *Proceedings of the International Symposium on Intelligent Information Technology*

Application Workshop (IITA '08), pp. 439–442, Shanghai, China, December 2008.

[14] Q. Su, Y. Niu, X. Liu, and T. Yao, "A novel blind digital watermarking algorithm for embedding color image into color image," *Optik*, vol. 124, no. 18, pp. 3254–3259, 2013.

[15] S. D. Lin and C.-F. Chen, "A robust dct-based watermarking for copyright protection," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 415–421, 2000.

[16] S. D. Lin, S. C. Shie, and C. F. Chen, "A DCT-based image watermarking with threshold embedding," *International Journal of Computers and Applications*, vol. 25, no. 2, pp. 130–135, 2003.

[17] A. Kerckhoffs, "La cryptographie militaire," *Journal Des Sciences Militaires*, vol. 4, pp. 161–191, 1883.

[18] K. T. Alligood, T. D. Sauer, and J. A. Yorke, *Chaos*, Springer, Berlin, Germany, 1997.

[19] T.-C. Hsu, W.-S. Hsieh, J. Y. Chiang, and T.-S. Su, "New watermark-removal method based on Eigen-image energy," *IET Information Security*, vol. 5, no. 1, pp. 43–50, 2011.