A Robust Watermarking Scheme with High Security and Low Computational Complexity

Liangjia Li[1], Yuling Luo[1,2(✉)], Junxiu Liu[1], Senhui Qiu[1,3], and Lanhang Li[1]

[1] School of Electronic Engineering, Guangxi Normal University, Guilin 541004, China
yuling0616@gxnu.edu.cn
[2] Guangxi Key Lab of Multi-source Information Mining and Security, Guangxi Normal University, Guilin 541004, China
[3] Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing, Guilin 541004, China

Abstract. Implementing a watermarking algorithm with high security and low computational complexity is a challenge, especially at a limited distortion level. A novel watermarking scheme is proposed in this paper, which is based on Tent-Logistic-Cosine Map (TLCM) and Direct Current (DC) coefficient modification. Firstly, the watermark is encrypted by a matrix obtained from TLCM. Then, the cover image is divided into non-overlapping 4×4 sub-blocks and some blocks are selected randomly. Thereafter, the DC coefficients of selected blocks are calculated directly in the spatial domain without performing two-dimensional discrete cosine transform. Finally, using the proposed watermark embedding procedure, DC coefficients of selected blocks are updated according to the encrypted watermark bits. Results show that the proposed watermarking algorithm has high security and low computational complexity at a limited distortion.

Keywords: Watermark · TLCM · DC coefficient · Spatial domain

1 Introduction

Digital data is continuously transmitted and shared owing to the recent advancements in Internet technologies, which makes the copyright infringement issue serious. To resolve this problem, digital watermarking schemes [1–6] and image encryption schemes [7–10] are presented. In this paper, the watermarking scheme is investigated as it is considered to be an effective copyright protection method [11]. Watermarking technology is used to embed digital information into digital content. Then, the copyright can be proved via the extracted digital information from the digital content by related computing operations [4]. There are two methods to insert the watermark: spatial domain insertion and transform domain insertion [12]. Specifically, the former is that the pixel values of cover

N. Park et al. (Eds.): SecureComm 2020, LNICST 336, pp. 439–454, 2020.
https://doi.org/10.1007/978-3-030-63095-9_28

image are changed directly to embed a watermark, which has lower computation but the ability of resisting to geometric and image processing attacks is relatively weaker [13]. The latter is that the transform coefficients of the cover image are used to embed the watermark. The latter has better robustness but its computation complexity is higher than the former [14]. Therefore, many watermarking schemes are based on the transform domain. For example, Discrete Cosine Transform (DCT) is commonly used in watermarking schemes [15–17]. However, it is a recent research hotspot to design a watermarking algorithm that can simultaneously satisfy the advantages of two watermark embedding methods [18]. For example, in [1], a new watermarking method based on Direct Current (DC) coefficients is designed. Firstly, the luminance Y of 512×512 colour image is partitioned into non-overlapping 8×8 blocks. Then, the DC coefficients of all blocks calculated in spatial domain are used to embed 64×64 binary watermark. In [2], the watermarking technology is also based on pixel domain. The binary watermark with size of 64×64 is encrypted by a chaotic sequence which is generated via iterating generalized Logistic map. Then the grey cover image is partitioned into non-overlapping 8×8 blocks and the encrypted watermark is embedded into the DC coefficients of all blocks.

Security is also the main consideration for designing watermarking schemes [19,20]. Therefore, one-dimensional (1D) chaotic maps are widely used in digital watermarking schemes to improve security due to their complex dynamical behaviour [21,22]. However, some watermarking schemes have been proved that the embedded watermark can be extracted by an attacker due to the limited key space of the chaotic system [23]. Specifically, in [21], the watermark is scrambled by the chaotic sequence of Logistic map. Then, the 2-level wavelet transform is performed on the cover image and the scrambled watermark is embedded into the approximation coefficients. However, the security of this algorithm is not high because the embedded watermark can be extracted by an attacker. In [22], the embedding positions are determined by combining Logistic map and Arnold cat map, and the initial conditions of chaotic systems are used as secret keys. But the embedded watermark can also be removed. Based on aforementioned discussion, by combining Tent-Logistic-Cosine Map (TLCM) and DC coefficient modification, a novel watermarking algorithm with high security and low computational complexity at a limited distortion level is designed in this paper. The designed scheme is based on previous works [1,2]. The main contributions of this work are as follows: (1) The 512×512 grey cover image is divided into non-overlapping 4×4 sub-blocks, and some blocks are used for embedding watermark, which can improve the imperceptibility. (2) The proposed watermark embedding procedure can further improve the robustness. (3) The binary watermark is encrypted via the proposed watermark encryption scheme, which can achieve higher security. (4) The DC coefficients of selected blocks are computed in pixel domain, which can shorten the execution time. (5) Three state-of-the-art watermark schemes are chosen for a comparative study, and the proposed technology outperforms other algorithms in both imperceptibility and robustness.

The rest of this paper is organized as follows. The basic knowledge of TLCM and mathematical theoretical analysis about 2D-DCT are provided in Sect. 2. The proposed watermark scheme is given in Sect. 3. Experimental results and performance analysis are reported in Sect. 4. Finally, Sect. 5 presents the conclusion.

2 Preliminaries

2.1 Chaotic Systems

TLCM is a 1D chaotic map by combing Tent map, Logistic map and Cosine map [24]. Moreover, it has been demonstrated that TLCM has more complex dynamical behaviour than its seed maps. The control parameter $\mathrm{u} \in [0, 1]$. TLCM is defined by

$$x_{\mathrm{n}+1} = \begin{cases} \cos\left(\pi\left(2\mathrm{u}x_{\mathrm{n}} + 4(1-\mathrm{u})x_{\mathrm{n}}\left(1-x_{\mathrm{n}}\right) - 0.5\right)\right), & \text{if } x_{\mathrm{n}} < 0.5, \\ \cos\left(\pi\left(2\mathrm{u}\left(1-x_{\mathrm{n}}\right) + 4(1-\mathrm{u})x_{\mathrm{n}}\left(1-x_{\mathrm{n}}\right) - 0.5\right)\right), & \text{if } x_{\mathrm{n}} \geq 0.5. \end{cases} \tag{1}$$

2.2 Mathematical Theoretical Analysis

(a) DC coefficient is obtained in pixel domain. DCT is used to transform real numbers into frequency domain. A transformed matrix can be obtained by performing DCT. In transform matrix, the coefficient in the upper left corner is named as DC coefficient, whereas remainders are the Alternating Current (AC) coefficients. Suppose the size of matrix $f(\varphi, \omega)$ is $\mathrm{s} \times \mathrm{t}$, ($\varphi = 0, 1, 2, \ldots,$ s-1, $\omega = 0, 1, 2, \ldots,$ t-1), the 2D-DCT of $f(\varphi, \omega)$ is introduced by

$$\mathcal{F}(\mathrm{u}, \mathrm{v}) = \mathrm{c_u c_v} \sum_{\varphi=0}^{\mathrm{s}-1} \sum_{\omega=0}^{\mathrm{t}-1} f(\varphi, \omega) \cos \frac{\pi(2\varphi+1)\mathrm{u}}{2\mathrm{s}} \cos \frac{\pi(2\omega+1)\mathrm{v}}{2\mathrm{t}}, \tag{2}$$

where $\mathcal{F}(\mathrm{u}, \mathrm{v})$ is DCT coefficient of $f(\varphi, \omega)$, u ($\mathrm{u} = 0, 1, 2, \ldots, \mathrm{s}-1$) is horizontal frequency, v ($\mathrm{v} = 0, 1, 2, \ldots, \mathrm{t}-1$) is vertical frequency, $\mathrm{c_u}$ and $\mathrm{c_v}$ are two compensation factors and they are given by

$$\mathrm{c_u} = \begin{cases} \sqrt{1/\mathrm{s}}, \mathrm{u} = 0, \\ \sqrt{2/\mathrm{s}}, 1 \leq \mathrm{u} < \mathrm{s}-1, \end{cases} \tag{3}$$

and

$$\mathrm{c_v} = \begin{cases} \sqrt{1/\mathrm{t}}, \mathrm{v} = 0, \\ \sqrt{2/\mathrm{t}}, 1 \leq \mathrm{v} < \mathrm{t}-1. \end{cases} \tag{4}$$

The inverse 2D-DCT is given by

$$f(\varphi, \omega) = \mathrm{c_u c_v} \sum_{\varphi=0}^{\mathrm{s}-1} \sum_{\omega=0}^{\mathrm{t}-1} \mathcal{F}(\mathrm{u}, \mathrm{v}) \cos \frac{\pi(2\varphi+1)\mathrm{u}}{2\mathrm{s}} \cos \frac{\pi(2\omega+1)\mathrm{v}}{2\mathrm{t}}. \tag{5}$$

According to Eq. (2), when u = 0 and v = 0, the DC coefficient of 2D-DCT can be obtained directly by

$$\mathcal{F}(0,0) = \frac{1}{\sqrt{\mathrm{st}}} \sum_{\varphi=0}^{\mathrm{s}-1} \sum_{\omega=0}^{\mathrm{t}-1} f(\varphi,\omega). \tag{6}$$

Thus, the DC coefficient $\mathcal{F}(0,0)$ can be obtained directly by calculating the average of all values of the matrix in spatial domain, and the specific result is detailed in [1].

(b) Modifying DC coefficient in spatial domain. Each value in the matrix will be updated after executing inverse 2D-DCT if the DC coefficient is changed. The relation between the changed amount of DC coefficient and each value update in spatial domain is discussed below. According to Eq. (5), the inverse 2D-DCT can be written by

$$f(\varphi,\omega) = \frac{1}{\sqrt{\mathrm{st}}}\mathcal{F}(0,0) + f(\varphi,\omega)^{\mathrm{AC}}, \tag{7}$$

where $f(\varphi,\omega)^{\mathrm{AC}}$ denotes the reconstructed matrix from AC coefficients. If the DC coefficient is altered and the altered amount is recorded as Δ_{m}, the modified DC coefficient $\mathcal{F}(0,0)^{\sim}$ can be obtained by

$$\mathcal{F}(0,0)^{\sim} = \mathcal{F}(0,0) + \Delta_{\mathrm{m}}. \tag{8}$$

Therefore, the recovered matrix $f(\varphi,\omega)^{\sim}$ is written by

$$f(\varphi,\omega)^{\sim} = \frac{1}{\sqrt{\mathrm{st}}}\mathcal{F}(0,0)^{\sim} + f(\varphi,\omega)^{\mathrm{AC}}. \tag{9}$$

According to the Eq. (7) and Eq. (8), Eq. (9) is written as

$$\begin{aligned} f(\varphi,\omega)^{\sim} &= \frac{1}{\sqrt{\mathrm{st}}}\mathcal{F}(0,0)^{\sim} + f(\varphi,\omega)^{\mathrm{AC}} \\ &= \frac{1}{\sqrt{\mathrm{st}}}\left[\mathcal{F}(0,0) + \Delta_{\mathrm{m}}\right] + f(\varphi,\omega)^{\mathrm{AC}} \\ &= \frac{\Delta_{\mathrm{m}}}{\sqrt{\mathrm{st}}} + \frac{1}{\sqrt{\mathrm{st}}}\mathcal{F}(0,0) + f(\varphi,\omega)^{\mathrm{AC}} \\ &= \frac{\Delta_{\mathrm{m}}}{\sqrt{\mathrm{st}}} + f(\varphi,\omega) \end{aligned}. \tag{10}$$

Therefore, if the changed amount of DC coefficient is Δ_{m}, the recovered matrix can be obtained directly by adding $\frac{\Delta_{\mathrm{m}}}{\sqrt{\mathrm{st}}}$ to each value in the original matrix without performing inverse 2D-DCT.

3 The Proposed Watermarking System

3.1 Watermark Encryption Scheme

A binary matrix generated by TLCM is used to encrypt the watermark, which can enhance the watermarking scheme security. The watermark and the

encrypted watermark are shown in Fig. 1. Suppose the size of binary watermark W is m × n, watermark encryption process is as follows. Firstly, the TLCM is iterated for m × n/8 times, and a chaotic sequence $x = (x_1, x_2, \ldots, x_{m\times n/8})$ is obtained. Then, x is quantified by $x' = \text{floor}\left(\text{mod}\left(x \times 10^{14}\right), 256\right)$, where floor(·) denotes rounding down function. Furthermore, the decimal sequence x' is converted into corresponding binary sequence and the length is 1 × m × n, labelled as $x'' = \left(x''_1, x''_2, \ldots, x''_{m\times n}\right)$. Besides, the x'' is reshaped into m × n two-dimensional matrix, and the result is labelled as x''_R which is used for watermark encryption. Finally, the encrypted watermark W_E is obtained by performing $W_E = W \oplus x''_R$, where ⊕ is XOR operation.

Fig. 1. Watermarks: (a) Original watermark; (b) Encrypted watermark.

3.2 Watermark Embedding

In this section, the watermark embedding process is given. Specifically, the M×N gray cover image C is divided into non-overlapping 4×4 blocks. Each sub-block is embedded with one-bit watermark information, so the number of sub-blocks and the number of watermark bits should meet M/4 × N/4 ≥ m × n. The flow chart of the watermarking embedding is shown in Fig. 2 and its detailed embedding process is as follows.

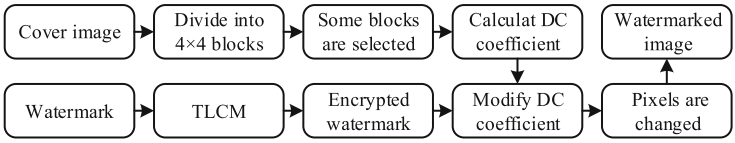

Fig. 2. The flow chart of watermark embedding.

Step 1. The m×n binary watermark W is encrypted by performing the steps of Sect. 3.1. The encrypted watermark is recorded as $W_E(s, t)$, where s = 1,2,. . . ,m, t = 1,2,. . . ,n and (s, t) denotes the coordinates of encrypted watermark bits.

Step 2. The M × N gray cover image C is divided into non-overlapping 4 × 4 sub-blocks $B_{i,j}$, where $i = 1, 2, \ldots, M/4, j = 1, 2, \ldots, N/4$, (i, j) represents the coordinates of sub-blocks.

Step 3. $m \times n$ blocks are randomly selected according to a given key and their positions are recorded.

Step 4. DC coefficient of each selected block is calculated directly in pixel domain, which is expressed by $DC = \left[\sum_{p=1}^{4}\sum_{q=1}^{4} B_{i,j}(p,q)\right]/4$, where (p,q) denotes the coordinates of pixel values in the block.

Step 5. According the encrypted watermark W_E, if $W_E(s,t) = 1$, DC coefficient of selected block is modified by

$$\begin{cases} DC_1 = \text{ floor } \left(\frac{DC}{\alpha}\right)\alpha + \gamma\alpha, \\ DC_2 = \left[\text{ floor } \left(\frac{DC}{\alpha}\right) + 1\right]\alpha + \gamma\alpha, \end{cases} \tag{11}$$

where DC_1 and DC_2 are two different modified DC coefficients, respectively, α is scaling factor, γ is fine-tuning coefficient and $\gamma \in [0,1]$. If $W_E(s,t) = 0$, DC coefficient of selected block is modified by

$$\begin{cases} DC_1 = \left[\text{ floor } \left(\frac{DC}{\alpha}\right) - 1\right]\alpha + (1-\gamma)\alpha, \\ DC_2 = \text{ floor } \left(\frac{DC}{\alpha}\right)\alpha + (1-\gamma)\alpha. \end{cases} \tag{12}$$

Step 6. Select the optimal modified DC coefficient DC_{opt} according to the rules: if $|DC_1 - DC| \le |DC_2 - DC|$, $DC_{opt} = DC_1$, or else, $DC_{opt} = DC_2$.

Step 7. The changed amount of selected block is calculated by $DC_{ch} = DC_{opt} - DC$, where DC_{ch} denotes changed amount of DC coefficient.

Step 8. The DC_{ch} is distributed averagely to all pixels of the block. Then, the block with one-bit watermark information is obtained by $B^w_{i,j} = B_{i,j} + DC_{ch}/4$, where $B^w_{i,j}$ is the watermarked sub-block.

Step 9. Repeating the steps 4–8 until all the selected blocks are embedded with encrypted watermark bits. Finally, the watermarked image C^w is obtained.

3.3 Watermark Extraction

The positions of sub-blocks containing watermark information and the matrix x''_R are required in watermark extraction. The extraction flowchart is shown in Fig. 3 and its specific steps are as follows. Firstly, the watermarked image C^w is divided into non-overlapping 4×4 sub-blocks, and the sub-blocks containing watermark bits $B^w_{i,j}$ are selected according to the recorded positions. Thereafter, calculate DC coefficient of $B^w_{i,j}$ by $DC^w = \left[\sum_{p=1}^{4}\sum_{q=1}^{4} B^W_{i,j}(p,q)\right]/4$, where DC^w denotes the DC coefficient which contains one-bit watermark information. Furthermore, according to the extracted rule, if $\text{mod}\left(\text{round}\left(DC^W\right), \alpha\right) < \alpha/2$, the extracted watermark bit is 1, otherwise the extracted watermark bit is 0, where round$(\cdot)$ rounds the element to the nearest integer. Repeating the step 2 and step 3 until all the watermark bits W^*_E are extracted from C^w. Finally, the embedded watermark W^* is recovered by performing $W^* = W^*_E \oplus x''_R$.

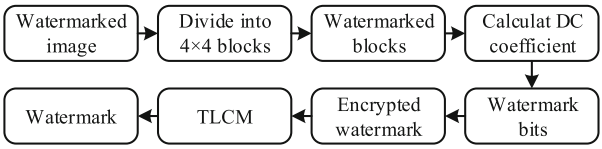

Fig. 3. The flow chart of watermark extraction.

4 Experiment Simulation and Analysis

In this section, the main required performances for a watermarking algorithm, including imperceptibility, robustness, security and computational complexity are analysed. The 64×64 watermark in Fig. 1(a) and eight 512×512 grey cover images in Fig. 4 are used to test. The performance's metrics definitions, simulation results are given in the following subsections.

Fig. 4. Cover images: (a) Lena; (b) Boat; (c) Man; (d) Peppers; (e) F16; (f) Lake; (g) Elaine; (h) House.

4.1 Metrics

Imperceptibility is measured by Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM). SSIM ranges in [0,1]. A higher PSNR and SSIM indicate that the algorithm has a high imperceptibility. According to [14], the imperceptibility is acceptable when PSNR $\geq$ 37dB and SSIM $\geq$ 0.93. The PSNR is defined by

$$\mathrm{PSNR}\left(\mathrm{C}, \mathrm{C}^{\mathrm{w}}\right) = 10 \lg \frac{\mathrm{C}_{\max}^2}{\mathrm{MES}}, \tag{13}$$

where $\mathrm{C}_{\max}$ is the maximum pixel value in C, MES refers to the mean square error between C and C^{w}, which is defined by

$$\mathrm{MES} = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} \left[\mathrm{C}(\mathrm{i}, \mathrm{j}) - \mathrm{C}^{\mathrm{w}}(\mathrm{i}, \mathrm{j})\right]^2, \tag{14}$$

where M × N represents the size of C and C^w. Moreover, SSIM is calculated by

$$\mathrm{SSIM}\left(C, C^w\right) = \frac{\left(\mu_C \mu_{Cw} + d_1\right)\left(\sigma_{CCw} + d_2\right)}{\left(\mu_C^2 + \mu_{Cw}^2 + d_1\right)\left(\sigma_C^2 + \sigma_{Cw}^2 + d_2\right)}, \tag{15}$$

where μ_C and μ_{C^w} are the averages of C and C^W, σ_C^2 and σ_{Cw}^2 are the variances of C and C^W, σ_{CC^w} is the covariance between C and C^w, d_1 and d_2 are two variables.

In addition, Normalized Correlation (NC) and Bit Error Rate (BER) are utilized to measure the robustness of the extracted watermark. The ranges of NC and BER are both in [0,1]. When the NC value equals 1 or the BER value equals 0, the extracted watermark is consistent with the original one. NC is defined by

$$\mathrm{NC}\left(W, W^*\right) = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j) \cdot W^*(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}[W(i,j)]^2} \cdot \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}\left[W^*(i,j)\right]^2}}, \tag{16}$$

where m, n represent the length of W and W^*, respectively. In addition, BER is defined by

$$\mathrm{BER}\left(W, W^*\right) = \frac{\sum_{i=1}^{m}\sum_{i=1}^{n} W(i,j) \oplus W^*(i,j)}{m \times n}. \tag{17}$$

4.2 Imperceptibility and Robustness Analysis

The imperceptibility is a vital performance for watermarking scheme. When the imperceptibility is acceptable, other performances can be discussed further. The watermark is embedded into eight cover images by using the proposed scheme, and Fig. 5 gives the experimental results. Results show that the PSNRs of eight watermarked images are greater than 42 dB and their SSIMs are larger than 0.98. Moreover, both PSNR and SSIM are significantly larger than acceptable values 37 dB and 0.93, respectively, which indicates that the proposed method has excellent imperceptibility.

Figure 6 presents the PSNR comparison for three watermarked images obtained by the proposed algorithm and three state-of-the-art schemes [2–4]. From the Fig. 6, the PSNRs of three watermarked images obtained by this work are higher than other algorithms. Especially compared with [3], the 512 × 512 grey cover image can only contain a 32 × 32 binary watermark in their work, while the 512 × 512 grey cover image can embed with a 64 × 64 binary watermark in this work. The watermark capacity of this work is four times than that of [3], and the PSNR of this work is still higher than [3]. Therefore, it is proved again that the proposed method has excellent imperceptibility.

The robustness is another important feature of watermarking scheme. Therefore, the robustness is further investigated when the invisibility is acceptable. In this work, the robustness is evaluated by using different attacks, including

Cover image	Watermarked image	Extracted watermark	Cover image	Watermarked image	Extracted watermark
					
Lena	PSNR=42.96; SSIM=0.9833	NC=1; BER=0	Boat	PSNR=42.94; SSIM=0.9882	NC=1; BER=0
					
Man	PSNR=42.79; SSIM=0.9868	NC=1; BER=0	Peppers	PSNR=42.96; SSIM=0.9845	NC=1; BER=0
					
F16	PSNR=43.07; SSIM=0.9828	NC=1; BER=0	Lake	PSNR=43.00; SSIM=0.9882	NC=1; BER=0
					
Elaine	PSNR=42.94; SSIM=0.9868	NC=1; BER=0	House	PSNR=43.07; SSIM=0.9872	NC=1; BER=0

Fig. 5. Experimental results.

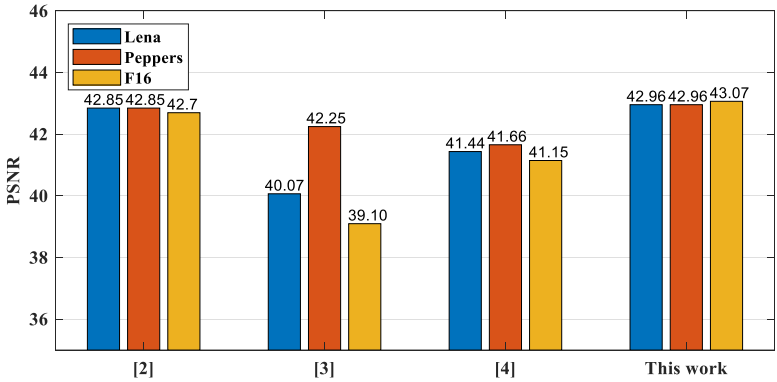

Fig. 6. PSNR comparison.

Gaussian Noise (GN), Speckle Noise (SN), Salt & Peppers Noise (SPN), Average Filter (AF), Wiener Filter (WF), Gaussian Low-pass Filter (GLPF), Median Filter (MF), JPEG compression (JPEG), Rescaling (RE), Cropping (CR), Motion Blur (MB), Sharpening (SH) and Rotation (RO). Figure 7 shows the watermarked image "Lena" under aforementioned attacks. Fig. 8 shows the extracted

watermarks from the watermarked images "Lena" under those attacks by using the proposed algorithm, and their corresponding NC and BER are listed in Table 1. The NC values are greater than 0.9 and BERs are less than 11.89%. Especially for JPEG (QF = 70) and RE (2) attacks, the NCs are equal to 1 and BERs are equal to 0, which indicate that the extracted watermark is consistent with the embedded one. Therefore, there is no obvious perceptual distortion between the extracted watermark and the original one. For other cover images, similar results are also obtained, and their corresponding NC and BER are shown in Fig. 9 and Fig. 10, respectively. The NCs shown in Fig. 9 are basically greater than 0.85 and the BERs shown in Fig. 10 are basically less than 15% for other cover images. Therefore, the proposed scheme has a superior behaviour against various attacks.

Fig. 7. Watermarked image "Lena" suffered different attacks, and a–n represent GN (0.02%), SN (0.1%), SPN (1%), AF (3×3), WF (3×3), GLPF (3×3), MF (3×3), JPEG (QF = 70), RE (0.5), RE (2), CR (10%), MB (4, 7), SH (0.8), RO (5°), respectively.

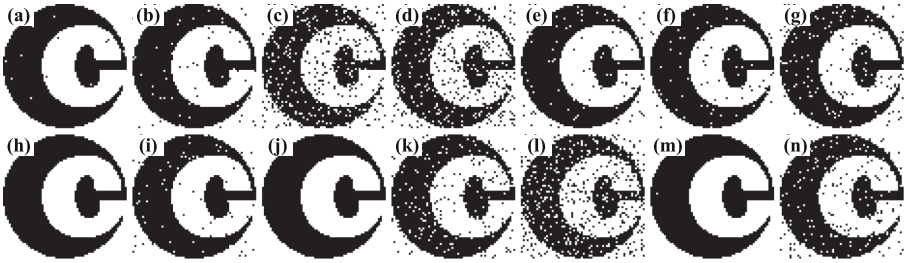

Fig. 8. Extracted watermark from watermarked image "Lena" under different attacks, and a–n represent GN (0.02%), SN (0.1%), SPN (1%), AF (3 × 3), WF (3 × 3), GLPF (3 × 3), MF (3 × 3), JPEG (QF = 70), RE (0.5), RE (2), CR (10%), MB (4, 7), SH (0.8), RO (5°), respectively.

Table 1. NC and BER (%) of watermark extracted from cover image "Lena" under various attacks.

Attack index	Description	NC	BER
a	GN (0.02%)	0.9971	0.29
b	SN (0.1%)	0.9840	1.61
c	SPN (1%)	0.9079	9.23
d	AF (3×3)	0.9040	5.59
e	WF (3×3)	0.9762	2.39
f	MF (3×3)	0.9799	2.03
g	GLPF (3×3)	0.9554	4.49
h	JPEG (QF = 70)	1	0
i	RE (0.5)	0.9823	1.78
j	RE (2)	1	0
k	CR (10%)	0.9437	5.67
l	MB (4, 7)	0.8813	11.89
m	SH (0.8)	0.9998	0.02
n	RO (5°)	0.9474	5.27

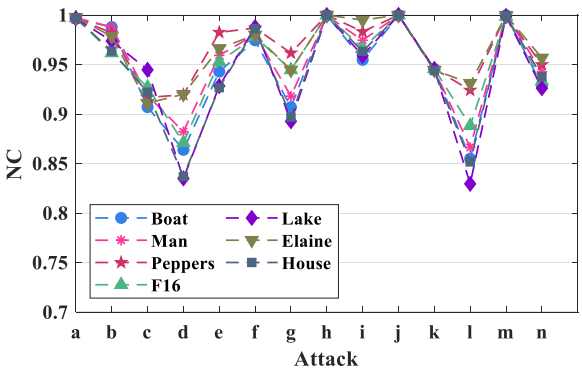

Fig. 9. NCs of extracted watermarks for different watermarked images.

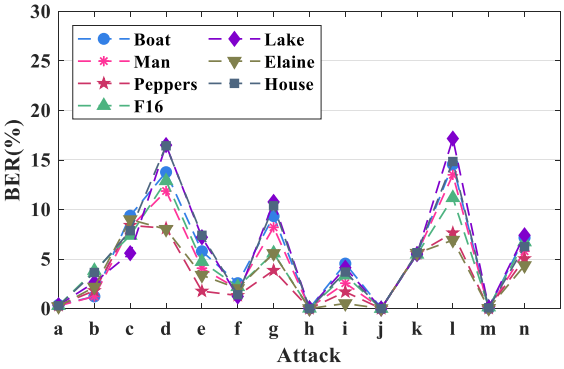

Fig. 10. BERs of extracted watermarks for different watermarked images.

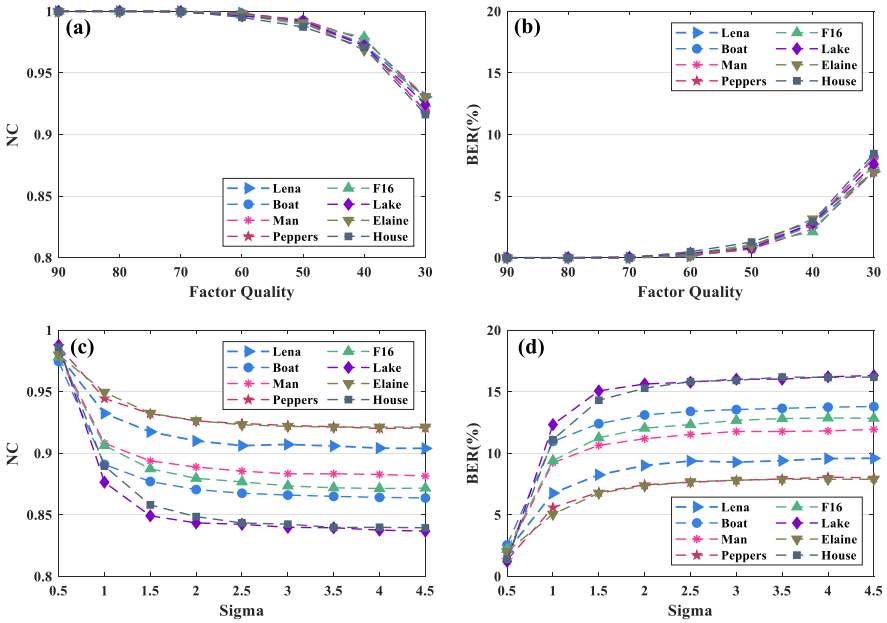

Fig. 11. The NCs and BERs of extracted watermark under JPEG and GLPF attacks with different parameters. (a) NCs under JPEG; (b) BERs under JPEG; (c) NCs under GLPF; (d) BERs under GLPF.

Besides, the robustness is further evaluated by using JPEG and GLPF attacks with dynamic parameters, and Fig. 11 shows the NCs and BERs of extracted watermarks. Figure 11 (a) and (b) represent the JPEG attacks, and the JPEG's quality factor is set from 90 to 30 with a step of −10. As the quality factor decrease, the NCs slowly decrease and the BERs slowly increase. Even the quality factor reaches 30, the NCs are larger than 0.9 and BERs are less than 10%. Moreover, when the quality factor is larger than 70, the NC of extracted

watermark is 1 and BER is 0. Figure 11 (c) and (d) represent the results under the GLPF attack, and the parameter sigma is set from 0.5 to 4.5 with a step of 0.5 under 3×3 filter window size. Results show that the NCs of extracted watermark are greater than 0.84 and BERs are lower than 16% for eight cover images. Thus, the proposed algorithm has great ability to defend against JPEG and GLPF attacks.

What's more, the robustness of this work is compared with two related works to prove the great robustness of this scheme. Table 2 and Table 3 present the BER comparison of this work and two state-of-the-art methods for cover image "Lena" [2,3]. As shown in Table 2, the BERs of extracted watermark are lower than [2] under various attacks. Especially for GN (0.02%) and SH, BER is 14.16% under GN (0.02%) and BER is 32.3% under SH in [2], while BER is 0.29% under GN (0.02%) and BER is 0.02% under SH in this work. The BER comparison with [3] is presented in Table 2. The results show that the BERs in this work are also lower than [3]. Especially for JPEG (QF = 70) and SH, BER is 2.05% under JPEG (QF = 70) and BER is 0.1% under SH in their work, while BER is 0 under JPEG (QF = 70) and BER is 0.02% under SH in this work. Therefore, the proposed algorithm has good performance in both imperceptibility and robustness.

4.3 Security Performance Analysis

Since the embedded watermark is encrypted by the matrix x''_{R}, it is necessary to perform XOR operation between extracted watermark and x''_{R} to get the final correct watermark. In this paper, the binary matrix x''_{R} is generated by iterating the TLCM. Specifically, the initial value x_1 and control parameter u of the TLCM are related to x''_{R}. If the x_1 and u are wrong, a wrong matrix x''_{R} is obtained. Then, the extracted watermark cannot be recovered correctly by

Table 2. BER (%) of [2] and this work for cover image "Lena".

Attack	[2]	This work
GN (0.02%)	14.16	0.29
SPN (1%)	27.19	9.23
MF (3×3)	5.53	4.49
GLPF (3×3)	8.52	2.03
SH	32.30	0.02
JPEG (QF = 70)	0	0
JPEG (QF = 80)	0	0
RO (10°)	7.18	7.18
RO (45°)	19.49	12.65
CR (Centre)	9.91	1.61
CR (Top left corner)	21.09	12.40
CR (Top right corner)	22.31	12.92

Table 3. BER (%) of [3] and this work for cover image "Lena".

Attack	[3]	This work
JPEG (QF = 20)	20.70	9.70
JPEG (QF = 30)	15.82	6.98
JPEG (QF = 50)	7.91	0.98
JPEG (QF = 70)	2.05	0
SPN (1%)	16.50	9.28
SPN (2%)	22.17	15.84
SH	0.10	0.02
RE (2)	0	0

using wrong x''_{R}. In other words, the correct watermark cannot be obtained even the attacker knows the watermark embedding algorithm. Besides, the accuracy of computer is limited, assuming it is 10^{-15}. Thus, the entire key space is 2^{104} in this work, which has reached the required key space 2^{100} [25]. The x_1 and u used in this paper cannot be simultaneously found by force attack. Therefore, the proposed algorithm has high security.

4.4 Computational Complexity Analysis

This section analysis the computational complexity. Table 4 gives the running time comparison of two different methods during embedding and extraction processes. The results indicate that the proposed scheme is faster than the performing true 2D-DCT in terms of both watermark embedding and extraction processes. Specifically, the average total time of watermark embedding and extraction of this work is ∼5 times faster than that of conventional DCT.

Table 4. Times comparison of conventional DCT and this work [unit: second].

Image	Conventional DCT			This work		
	Embedding	Extraction	Total	Embedding	Extraction	Total
Lena	0.2538	0.1590	0.4128	0.0325	0.0441	0.0766
Boat	0.2231	0.1803	0.4034	0.0376	0.0402	0.0778
Man	0.2053	0.1514	0.3567	0.0390	0.0448	0.0838
Peppers	0.2246	0.1582	0.3828	0.0331	0.0403	0.0734
F16	0.2096	0.1492	0.3588	0.0316	0.0443	0.0759
Lake	0.2261	0.1483	0.3744	0.0332	0.0394	0.0726
Elaine	0.2252	0.1502	0.3754	0.0359	0.0440	0.0799
House	0.2156	0.1817	0.3973	0.0362	0.0407	0.0769
Average	0.2230	0.1598	0.3827	0.0349	0.0422	0.0771

5 Conclusion

In this work, a novel robust watermarking scheme with high security and low computational complexity watermarking scheme is proposed. To achieve high security, the watermark is encrypted by a binary matrix obtained via TLCM before it is embedded into the cover image. In the meantime, the cover image is divided into non-overlapping 4×4 sub-blocks and some blocks are selected to embed with watermark, which can improve the imperceptibility. In watermark embedding process, the DC coefficient is calculated directly in spatial domain to shorten the execution time. Experimental results demonstrate that the proposed watermarking algorithm has high security, low computational complexity, good imperceptibility and great robustness. Future work will investigate the colour watermarking scheme.

Acknowledgments. This research is supported by the National Natural Science Foundation of China under Grants 61801131 and 61661008, the Guangxi Natural Science Foundation under Grants 2017GXNSFAA198180, the funding of Overseas 100 Talents Program of Guangxi Higher Education, 2018 Guangxi One Thousand Young and Middle-Aged College and University Backbone Teachers Cultivation Program, Research Fund of Guangxi Key Lab of Multi-source Information Mining & Security (19-A-03-02), Research Fund of Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing, and the Young and Middle-aged Teachers' Research Ability Improvement Project in Guangxi Universities under Grant 2020KY02030.

References

1. Su, Q., Niu, Y., Wang, Q., Sheng, G.: A blind color image watermarking based on DC component in thespatial domain. Optik **124**(23), 6255–6260 (2013)
2. Parah, S.A., Loan, N.A., Shah, A.A., Sheikh, J.A., Bhat, G.M.: A new secure and robust watermarking technique based on logistic map and modification of DC coefficient. Nonlinear Dyn. **93**(4), 1933–1951 (2018). https://doi.org/10.1007/s11071-018-4299-6
3. Kang, X., Zhao, F., Lin, G., Chen, Y.: A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength. Multimedia Tools Appl. **77**(11), 13197–13224 (2017). https://doi.org/10.1007/s11042-017-4941-1
4. Ko, H.J., Huang, C.T., Horng, G., WANG, S.J.: Robust and blind image watermarking in DCT domain using inter-block coefficient correlation. Inf. Sci. **517**(1), 128–147 (2020)
5. Ali, M., Ahn, C.W.: An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain. Signal Process. **94**(1), 545–556 (2014)
6. Rajani, D., Kumar, P.R.: An optimized blind watermarking scheme based on principal component analysis in redundant discrete wavelet domain. Signal Process. **172**(1), 1–15 (2020)
7. Luo, Y., Lin, J., Liu, J., Wei, D., Cao, L., Zhou, R.: A robust image encryption algorithm based on chua's circuit and compressive sensing. Signal Process. **161**(1), 227–247 (2019)

8. Luo, Y., Cao, L., Qiu, S., Lin, H., Harkin, J., Liu, J.: A chaotic map-control-based and the plain image-related cryptosystem. Nonlinear Dyn. **83**(4), 2293–2310 (2015). https://doi.org/10.1007/s11071-015-2481-7
9. Luo, Y., Tang, S., Liu, J., Cao, L., Qiu, S.: Image encryption scheme by combining the hyper-chaotic system with quantum coding. Optics Lasers Eng. **124**(1), 1–13 (2020)
10. Luo, Y., Ouyang, X., Liu, J., Cao, L.: An image encryption method based on elliptic curve elgamal encryption and chaotic systems. IEEE Access **7**(1), 38507–38522 (2019)
11. Makbol, N.M., Khoo, B.E., Rassem, T.H., Loukhaoukha, K.: A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. Inf. Sci. **417**(1), 381–400 (2017)
12. Zhang, L., Wei, D.: Image watermarking based on matrix decomposition and gyrator transform in invariant integer wavelet domain. Signal Process. **169**(1), 1–18 (2020)
13. Chan, C.K., Cheng, L.: Hiding data in images by simple LSB substitution. Pattern Recogn. **37**(3), 469–474 (2004)
14. Liu, J., Huang, J., Luo, Y., Cao, L., Yang, S.: An optimized image watermarking method based on HD and SVD in DWT domain. IEEE Access **7**(1), 80849–80860 (2019)
15. Hsu, L.Y., Hu, H.T.: Robust blind image watermarking using crisscross inter-block prediction in the DCT domain. J. Visual Commun. Image Representation **46**(1), 33–47 (2017)
16. Parah, S.A., Sheikh, J.A., Loan, N.A., Bhat, G.M.: Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. Digital Signal Process. A Rev. J. **53**(1), 11–24 (2016)
17. Das, C., Panigrahi, S., Sharma, V.K., Mahapatra, K.K.: A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. AEU - Int. J. Electron. Commun. **68**(3), 244–253 (2014)
18. Byun, S.W., Son, H.S., Lee, S.P.: Fast and robust watermarking method based on DCT specific location. IEEE Access **7**(1), 100,706–100,718 (2019)
19. Cayre, F., Fontaine, C., Furon, T.: Watermarking security: theory and practice. IEEE Trans. Signal Process. **53**(10), 3976–3987 (2005)
20. Wang, Y.G., Zhu, G., Kwong, S., Shi, Y.Q.: A study on the security levels of spread-spectrum embedding schemes in the WOA framework. IEEE Trans. Cybern. **48**(8), 2307–2320 (2018)
21. Liu, N., Li, H., Dai, H., Guo, D., Chen, D.: Robust blind image watermarking based on chaotic mixtures. Nonlinear Dyn. **80**(3), 1329–1355 (2015). https://doi.org/10.1007/s11071-015-1946-z
22. Habib, S.M., Ries, S., Max, M.: A blind chaos-based watermarking technique. Secur. Commun. Netw. **7**(4), 800–811 (2014)
23. Chen, L., Chen, J., Zhao, G., Wang, S.: Cryptanalysis and improvement of a chaos-based watermarking scheme. IEEE Access **7**(1), 97549–97565 (2019)
24. Hua, Z., Zhou, Y., Huang, H.: Cosine-transform-based chaotic system for image encryption. Inf. Sci. **480**(1), 403–419 (2019)
25. Murillo-Escobar, M.A., Cruz-Hernández, C., Cardoza-Avendaño, L., Méndez-Ramírez, R.: A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. Nonlinear Dyn. **87**(1), 407–425 (2016). https://doi.org/10.1007/s11071-016-3051-3