Hindawi Publishing Corporation
Abstract and Applied Analysis
Volume 2013, Article ID 384067, 8 pages
http://dx.doi.org/10.1155/2013/384067

Research Article

Chaotic Image Encryption Algorithm Based on Circulant Operation

Xiaoling Huang,[1] Guodong Ye,[1,2] and Kwok-Wo Wong[2]

[1] *College of Science, Guangdong Ocean University, Zhanjiang 524088, China*
[2] *Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong*

Correspondence should be addressed to Xiaoling Huang; xyxhuang@hotmail.com

Received 19 May 2013; Revised 19 June 2013; Accepted 19 June 2013

Academic Editor: Luca Guerrini

A novel chaotic image encryption scheme based on the time-delay Lorenz system is presented in this paper with the description of Circulant matrix. Making use of the chaotic sequence generated by the time-delay Lorenz system, the pixel permutation is carried out in diagonal and antidiagonal directions according to the first and second components. Then, a pseudorandom chaotic sequence is generated again from time-delay Lorenz system using all components. Modular operation is further employed for diffusion by blocks, in which the control parameter is generated depending on the plain-image. Numerical experiments show that the proposed scheme possesses the properties of a large key space to resist brute-force attack, sensitive dependence on secret keys, uniform distribution of gray values in the cipher-image, and zero correlation between two adjacent cipher-image pixels. Therefore, it can be adopted as an effective and fast image encryption algorithm.

1. Introduction

With the rapid development of the computer network, it becomes more and more convenient to communicate in digital form. However, the transmitted information may be intercepted, copied, and even modified illegally. Aiming at the security and protection of digital images, many image encryption algorithms or technologies such as DNA sequence [1], chaotic map [2], circular bit shift and XOR operations [3], quantum logistic map [4], and Hartley transform [5] have been developed. Among these encryption algorithms, the chaos-based approach has become a hot research topic because of many unique characteristics of the chaotic system itself such as sensitive dependence on initial conditions and system parameters, nonperiodicity, pseudorandom property, and topological transitivity. These properties lead to efficient methods for image encryption.

One-dimensional and two-dimensional chaotic maps are usually employed in chaos-based image encryption algorithms. One-dimensional chaotic maps such as Logistic map, Sine map, and skew tent map have the advantages of simplicity and easy implementation [6]. In particular, Logistic map was widely used for image encryption [7–9]. However, it is not secure enough to use only one-dimensional chaotic map because of its small key space and weak security [7]. Many studies [10–13] were carried out to improve its security. For example, Singh and Sinha combined the Hartley transform and Logistic map in [5], Gao et al. [6] increased the number of parameters to six, and Ye [10] adopted the matrix property of Toeplitz and Hankel. Reference [11] proposed a total shuffling algorithm using Logistic map. In [12], two Logistic maps were employed to enlarge the key space. In other schemes [14, 15], the security has been improved by shuffling the positions and changing the pixel values simultaneously. Li and Yuan [15] reported the weakness of DCT-based encryption algorithm and proposed the full interblock shuffle approach. The authors in [16] studied the hyperchaotic systems with uncertain parameter for image encryption.

A good encryption algorithm must satisfy some requirements such as large key space, sensitive dependence on secret keys, and no correlation between two adjacent pixels [17, 18]. Here we propose an image encryption algorithm based on the time-delay Lorenz system and the unique properties of chaotic systems. It performs the position permutation according to a chaotic sequence and the diffusion stage by blocks. The rest of this paper is arranged as follows. In

Section 2, Circulant matrix and time-delay Lorenz system are introduced. The proposed image encryption algorithm and its mathematical model are described in Section 3. Numerical experiments are reported in Section 4 while the related security analysis is given in Section 5. Finally, some conclusions are drawn in Section 6.

2. Circulant Matrix and Time-Delay Lorenz System

2.1. Circulant Matrix

Definition 1. Suppose that there is an $n \times n$ matrix C_n having the following form:

$$C_n = \begin{pmatrix} c_0 & c_{-1} & \cdots & c_{2-n} & c_{1-n} \\ c_1 & c_0 & c_{-1} & \ddots & c_{2-n} \\ \vdots & c_1 & c_0 & \ddots & \vdots \\ c_{n-2} & \cdots & \ddots & \ddots & c_{-1} \\ c_{n-1} & c_{n-2} & \cdots & c_1 & c_0 \end{pmatrix}. \tag{1}$$

Then C_n is called a Circulant matrix [19] if $c_{-k} = c_{n-k}$ $(1 \le k \le n-1)$.

Definition 2. Suppose that there is an $m \times n$ matrix $G_{m\times n}$ $(m \le n)$ possessing the following form:

$$G_{m\times n} = \begin{pmatrix} g_0 & g_{-1} & \cdots & g_{m-n} & g_{m-1-n} & \cdots & \cdots & g_{1-n} \\ g_1 & g_0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ g_{m-2} & \ddots & \ddots & \ddots & \ddots & \ddots & g_{m-n} & g_{m-1-n} \\ g_{m-1} & g_{m-2} & \cdots & g_1 & g_0 & g_{-1} & \cdots & g_{m-n} \end{pmatrix}. \tag{2}$$

Then $G_{m\times n}$ is called a generalized Circulant matrix if $g_{m-k} = g_{m-k-n}$ $(1 \le k \le m-1)$.

We can also consider $G_{m\times n}$ as a generalized Circulant matrix when $m > n$, considering that G^T has the same form as (2).

2.2. The Time-Delay Lorenz System. The time-delay Lorenz system [20] is a three-dimensional system defined by

$$\begin{aligned} \dot{x} &= m\left(y - x\right) + u_1, \\ \dot{y} &= rx - y - xz + u_2, \\ \dot{z} &= xy - bz\left(t - \tau\right) + u_3, \end{aligned} \tag{3}$$

where τ is an unknown time-varying lag. When $m = 10$, $r = 28$, $b = 83$, $\tau = 1/6$, and $u_1 = u_2 = u_3 = 0$, the time-delay Lorenz system (3) is in the chaotic state [20]; that is, the two chaotic sequences are nonperiodic, nonconvergent, and noncorrelated with two different sets of initial values x_0, y_0, and z_0. More details of the time-delay Lorenz system can be found in [20].

2.3. Random Chaotic Sequence. Given initial values x_0, y_0, and z_0, a set of values $\{x_0, y_0, z_0, x_1, y_1, z_1, \ldots\}$ can be obtained by iterating (3). A parameter p can be added to drop the former p iterated values; that is, we only keep the values $\{x_{p+1}, y_{p+1}, z_{p+1}, x_{p+2}, y_{p+2}, z_{p+2}, \ldots\}$. Collect the first component $\{x_{p+1}, x_{p+2}, \ldots, x_{p+M}\}$ since the plain-image size is $M \times N$. Do the preprocessing for $\{x_{p+1}, x_{p+2}, \ldots, x_{p+M}\}$ by updating the values as $x_{p+i} = \text{abs}(x_{p+i} \times 10^{14}) - \text{floor}(\text{abs}(x_{p+i} \times 10^{14}))$, $i = 1, 2, \cdots, M$.

Sort the updated sequence and we obtain $\{\overline{x}_{p+1}, \overline{x}_{p+2}, \ldots, \overline{x}_{p+M}\}$. By finding the position of $\overline{x}_i$ $(i = p+1, \ldots, p+M)$ in $\{x_{p+1}, x_{p+2}, \ldots, x_{p+M}\}$, a sequence $H = \{h_1, h_2, \ldots, h_M\}$ can be generated. Similarly, do the same process for the second component $\{y_{p+1}, y_{p+2}, \ldots, y_{p+N}\}$, and we can get another sequence $L = \{l_1, l_2, \ldots, l_N\}$.

3. Image Encryption Scheme

In general, the adjacent pixels in the plain-image have high correlation. In order to reduce this correlation and resist known-plaintext attacks, position permutation is considered as the first encryption operation.

3.1. Position Permutation Based on Circulant Matrix. Noting that the generalized Circulant matrix (Definition 2 for rectangular image) can be extended directly, we mainly discuss the case of Circulant matrix (Definition 1 for square image). For a Circulant matrix, its elements satisfy $c_{-k} = c_{n-k}$ $(1 \le k \le n-1)$; that is, all elements in a diagonal or a subdiagonal line are equal. Moreover, the total number of elements along the subdiagonal line c_{-k} and c_{n-k} $(1 \le k \le n-1)$ is n. For example, for a Circulant matrix $A_{3\times3}$ which satisfies $a_0 = 11$, $a_1 = 12$, $a_2 = 13$, $a_{-1} = 13$, $a_{-2} = 12$, the total number of a_{-k} and a_{3-k} $(k = 1, 2)$ is 3, which equals that on the diagonal line:

$$A_{3\times3} = \begin{pmatrix} 11 & 12 & 13 \\ 13 & 11 & 12 \\ 12 & 13 & 11 \end{pmatrix}. \tag{4}$$

Based on the Circulant matrix, we can perform position permutation along the diagonal or antidiagonal lines in the upper and lower triangular matrices. This approach is different from the traditional method of row and column position shuffling. Of course, it will have problems if we apply the chaotic sequences to the diagonal and antidiagonal lines directly because the number of elements on these lines is not equal. This is the main reason why the existing approaches do not perform position shuffling along the diagonal and antidiagonal instead of row and column. Here we can solve this problem using the properties of the Circulant matrix.

(1) Permutation along Diagonal Direction. In the upper part of an image matrix $A_{n\times n}$ (we denote the plain-image as A in this paper), the number of elements on subdiagonal and diagonal lines is n if the elements on the subdiagonal line of a_{-k} $(1 \le k \le n-1)$ are patched by the elements on the subdiagonal line of a_{n-k}. In this case, the position permutation along the diagonal direction can be carried out. This is equivalent

to having position permutation in the n diagonal matrix $B_{n\times(2n-1)}$, of which the elements are

$$B(i,j) = \begin{cases} A(i,j), & \text{if } 1 \le i \le n,\ i \le j \le n, \\ A(2n+1-j, n+1-i), & \text{if } n+1 \le j \le 2n-1, \\ & \quad j-n+1 \le i \le n, \\ 0, & \text{others}. \end{cases} \tag{5}$$

The position shuffled matrix $\overline{C}_{n\times n}$ is governed by (6) when B is permuted along the diagonal direction:

$$\overline{C}(i,j) = \begin{cases} B(i,j), & \text{if } 1 \le i \le n,\ i \le j \le n, \\ B(n-j+1, 2n+1-i), & \text{if } 2 \le i \le n,\ 1 \le j \le i-1. \end{cases} \tag{6}$$

We will go back to the traditional position scrambling approach by columns if the elements of the matrix $B_{n\times(2n-1)}$ are computed by (7) instead of (5):

$$B(i,j) = \begin{cases} A(i,j), & \text{if } 1 \le i \le n,\ i \le j \le n, \\ A(i,j-n), & \text{if } n+1 \le j \le 2n-1, \\ & \quad j-n+1 \le i \le n, \\ 0, & \text{others}. \end{cases} \tag{7}$$

(2) Position Permutation along Antidiagonal Direction. For the case of antidiagonal, the permutation procedures are similar to those for the diagonal case. The difference is that we make use of the lower triangular of matrix $A_{n\times n}$ that is equivalent to performing position scrambling in the n antidiagonal matrix $D_{(2n-1)\times n}$, of which the elements are given by

$$D(i,j) = \begin{cases} A(i,j), & \text{if } 1 \le i \le n,\ n-i+1 \le j \le n, \\ A(j,i-n), & \text{if } 1 \le j \le n-1,\ n+1 \le i \le 2n-j, \\ 0, & \text{others}. \end{cases} \tag{8}$$

Thus, the shuffled image $E_{n\times n}$ is obtained by (9) when D is permuted along the antidiagonal direction:

$$E(i,j) = \begin{cases} D(i,j), & \text{if } 1 \le i \le n,\ n-i+1 \le j \le n, \\ D(n+j,i), & \text{if } 1 \le i \le n-1,\ 1 \le j \le n-i. \end{cases} \tag{9}$$

Similarly, this is equivalent to the traditional position scrambling by rows when we set the matrix $D_{(2n-1)\times n}$ by

$$D(i,j) = \begin{cases} A(i,j), & \text{if} 1 \le i \le n,\ n-i+1 \le j \le n, \\ A(i-n,j), & \text{if} 1 \le j \le n-1,\ n+1 \le i \le 2n-j, \\ 0, & \text{others}. \end{cases} \tag{10}$$

In the decryption process, we just need to rewrite (5), (6), (8), and (9) reversely. In fact, the traditional permutation is a special case of our method. Of course, the method can be extended to image shuffling of any size according to the generalized Circulant matrix (here we do not discuss this in detail; please refer to the Appendix). After being permutated along the diagonal and antidiagonal directions, the process of position permutation is finished. For example, Figure 1(b) is the cipher-image of Rice shown in Figure 1(a) using three rounds of our method. Figure 1(c) is the cipher-image using traditional row and column method, also by three rounds. The figures show that the proposed method has a better shuffling performance.

3.2. Block-Based Diffusion. To make a bit-change in the plain-image result in a big difference in the cipher-image, we adopt block-based diffusion for a fast implementation. The diffusion steps are stated as follows:

Step 1. Read the permuted image to a $M \times N$ matrix E. Then divide E into two equal blocks, that is, $E = [E_1; E_2]$. Each block has size $(M/2) \times N$. We can add a random row to E if M is not an even number.

Step 2. Extract $MN/2$ values from $\{x_{p+1}, y_{p+1}, z_{p+1}, x_{p+2}, y_{p+2}, z_{p+2}, \ldots\}$ to form the set S. Then convert the elements into decimal value in the following way:

$$S_i = \operatorname{mod}\left(\left(\operatorname{abs}(S_i) - \operatorname{floor}(\operatorname{abs}(S_i))\right) \times 10^{14}, 256\right), \quad i = 1, 2, \ldots, \frac{MN}{2}, \tag{11}$$

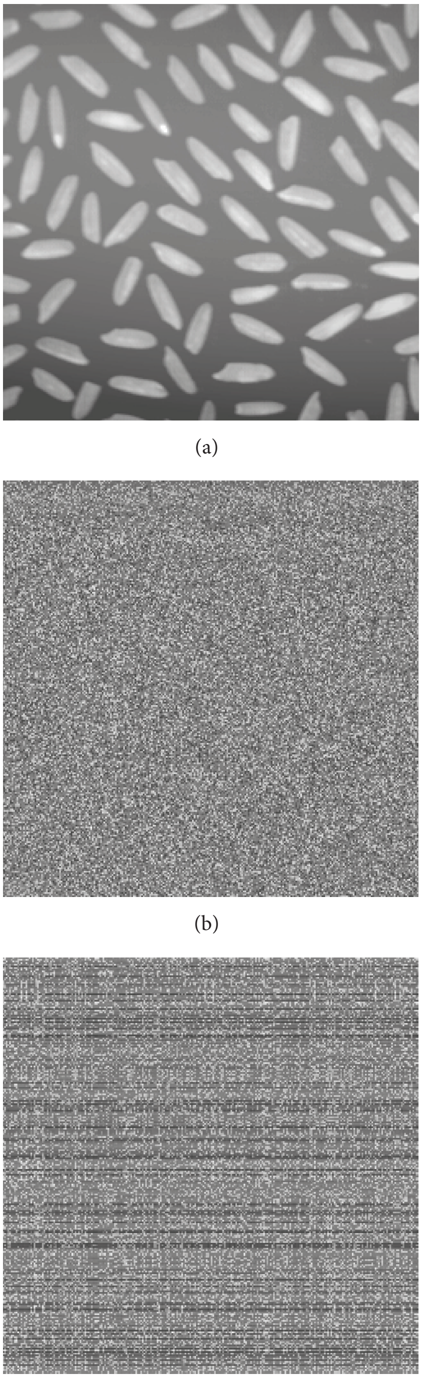
where abs(x) returns the absolute value of x, floor(x) rounds x to the nearest integer less than or equal to x, and mod returns the remainder after division. Rearrange S into a matrix W in the order from left to right and top to bottom.

Step 3. Carry out the following gray-level diffusion [22] and the cipher-image F will eventually be generated as $F = [\overline{E}_1; \overline{E}_2]$:

$$\overline{E}_1 = E_1 \dot{+} t \times W; \qquad \overline{E}_2 = E_2 \dot{+} \overline{E}_1, \tag{12}$$

where $t = \operatorname{mod}(\sum E_2, M/2) + \operatorname{mod}(\sum E_2, N) + \operatorname{mod}(\sum E_2, M/2 + N) + 1$. Here, $\dot{+}$ represents the modular addition under 256. The parameter t is dependent on the plain-image.

3.3. Encryption Procedures. The detail procedures of the proposed image encryption algorithm based on time-delay Lorenz system and Circulant matrix are described as follows.



(a)

(b)

(c)

Figure 1: Encryption: (a) plain-image of Rice, (b) shuffled image using our method, and (c) shuffled image using traditional method.

Step 1. Read the plain-image and put its pixels in a two-dimensional matrix A.

Step 2. Generate two chaotic sequences H and L by iterating the time-delay Lorenz system from the initial condition x_0, y_0, z_0, p.

Step 3. Perform position permutation on A using H and L according to the property of the Circulant matrix. A new permuted matrix E is then formed.

Step 4. Generate the pseudorandom matrix W of size $(M/2)\times N$ from the chaotic system again.

Step 5. Divide the matrix E into two parts, that is, $E = [E_1; E_2]$, and compute the control parameter $t = \mathrm{mod}(\sum E_2, M/2) + \mathrm{mod}(\sum E_2, N) + \mathrm{mod}(\sum E_2, M/2 + N) + 1$.

Step 6. Perform pixel value diffusion according to (12). Then the cipher-image is obtained as $F = [\overline{E}_1, \overline{E}_2]$.

To enhance the security, we can perform more rounds from Step 5 to Step 6, that is, multiple diffusion. In this paper, we take 5 rounds. The decryption process is just the reverse of the encryption one.

4. Numerical Experiments

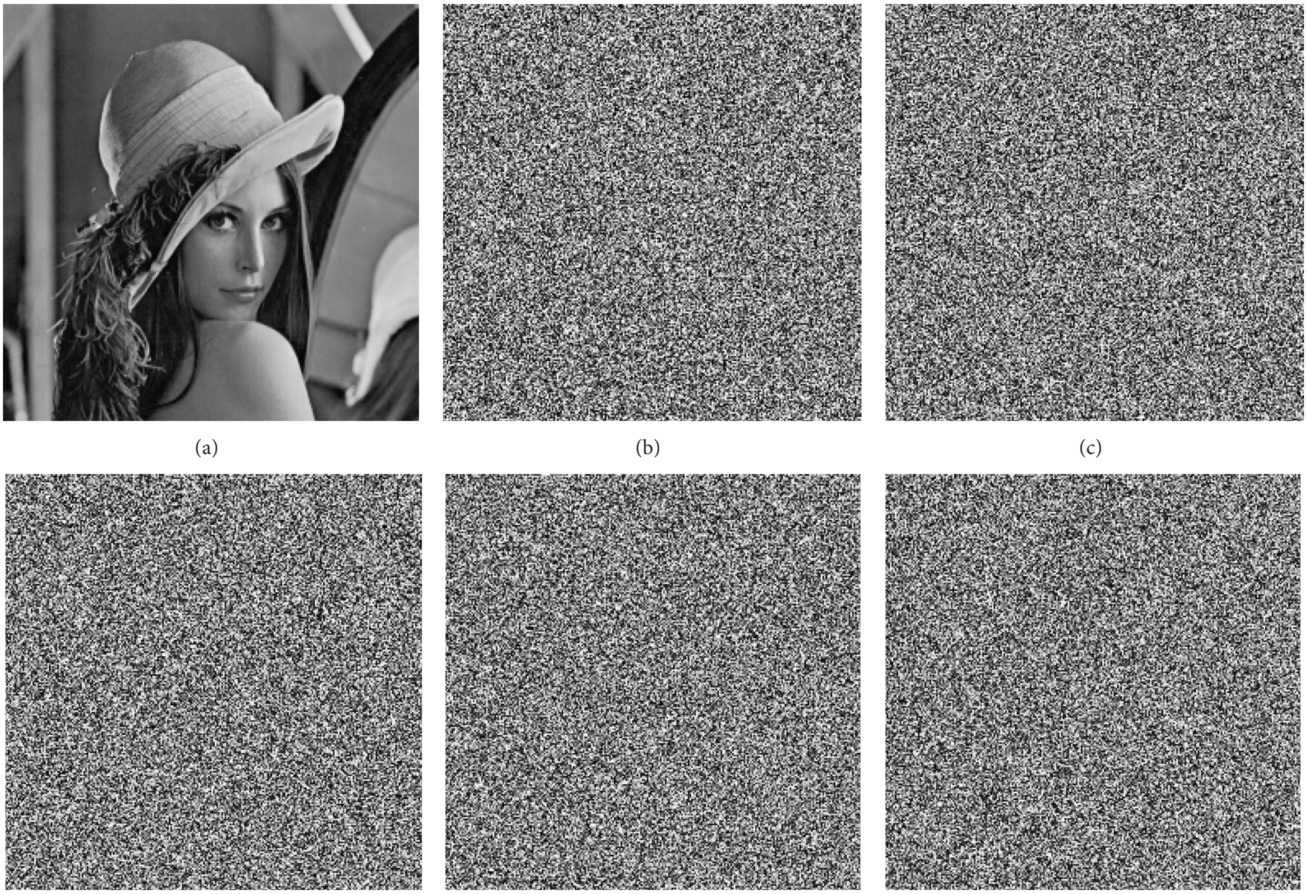
In this section, some experimental results of the proposed image encryption method are presented. The work is accomplished in a computer of Intel(R) Core(TM) i3-2350M, 2.30 GHz CPU, running Windows 7. The plain-image is Lena with size 256 × 256 shown in Figure 2(a). Figure 2(b) is the cipher-image obtained by the proposed method using the initial values $x_0 = -0.175$, $y_0 = 0.216$, $z_0 = -0.811$, and $p = 30$.

5. Security Analysis

(1) Key Space. The key space refers to the total number of distinct keys which can be used in the algorithm. A good encryption algorithm should have a large key space to avoid brute-force attacks. In the proposed algorithm, the size of the key space can reach $p \times 10^{42}$ if the computation precision is 10^{-14}. This value justifies that our encryption algorithm has a sufficiently large key space.

(2) Sensitivity Analysis. High key sensitivity means that a little change in the key will cause a huge change in the decrypted image. In our algorithm, with the original keys $x_0 = -0.175$, $y_0 = 0.216$, $z_0 = -0.811$, and $p = 30$, we encrypt the plain-image Lena to the cipher-image shown in Figure 2(b). The decrypted image using a key with only a tiny difference, that is, $x_0 = -0.17500000000001$, is depicted in Figure 2(c). Figure 2(d) shows the decrypted image with a wrong key of $y_0 = 0.21600000000001$. Figures 2(e) and 2(f) are similar wrong decrypted images. They all indicate that the new algorithm is very sensitive to the key.

(3) Histogram Analysis. The histogram, also called the gray scale distribution, displays and reflects the distribution of pixel values in an image. Figures 3(a) and 3(b) are the plain-image and cipher-image of Cameraman while Figures 3(c) and 3(d) are their histograms, respectively. These diagrams show that an attacker can hardly launch any statistical attack because the gray values are distributed uniformly.



(a) (b) (c) (d) (e) (f)

Figure 2: Encryption and decryption: (a) plain-image of Lena, (b) cipher-image, (c) decrypted image with key $x_0 + 10^{-14}$, (d) decrypted image with key $y_0 + 10^{-14}$, (e) decrypted image with key $z_0 + 10^{-14}$, and (f) decrypted image with key $p = 31$.

(4) Correlation Coefficient Analysis of Two Adjacent Pixels. To evaluate the correlation between two adjacent pixels in the plain and the cipher-images, the following equation is used [6, 11]:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x) D(y)}}, \tag{13}$$

where $\operatorname{cov}(x, y) = (1/N) \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))$, $D(x) = (1/N) \sum_{i=1}^{N} (x_i - E(x))^2$, $E(x) = (1/N) \sum_{i=1}^{N} x_i$.

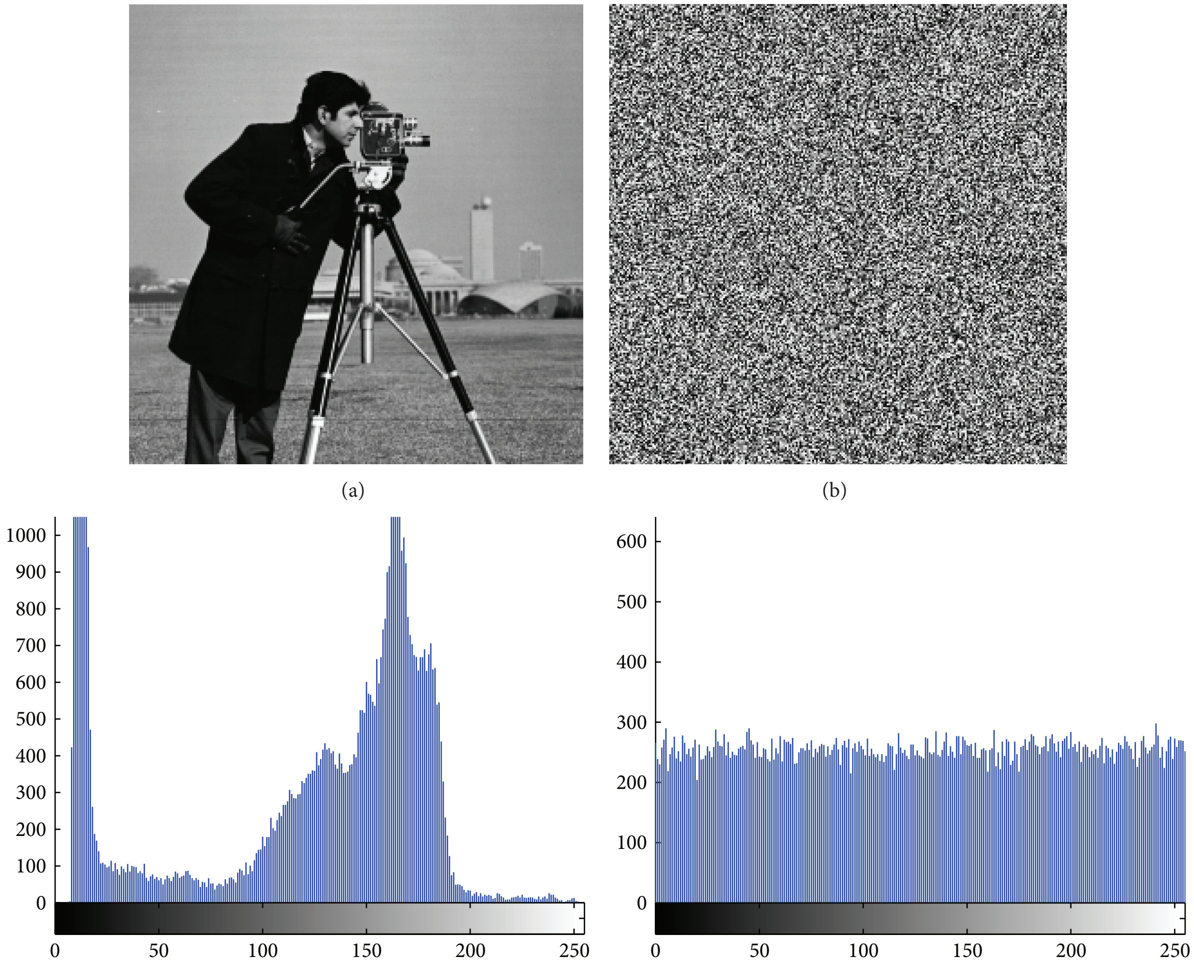
First of all, 2500 pairs of adjacent pixels of the Rice image (Figure 4(a)), in horizontal, vertical, and diagonal directions, are randomly selected. The results are listed in Table 1, in which we find that the correlation coefficients of two adjacent pixels in the cipher-image are almost zero. Figures 4(b) and 4(c) show the gray-level distribution of two horizontally adjacent pixels in the plain-image and the cipher-image, respectively.

(5) Differential Attack. To avoid differential attacks, NPCR and UACI [12, 23, 24] defined by (14) are commonly used to test the influence of a one-pixel change in the plain-image on the resultant cipher-image. For an effective encryption algorithm, the cipher-image should show a significant change even for a tiny change in the plain-image:

$$\begin{gathered} \mathrm{NPCR} = \frac{\sum_{ij} D(i, j)}{M \times N} \times 100\% \\ \mathrm{UACI} = \frac{1}{M \times N} \left[\sum_{i,j} \frac{\left| C_1(i, j) - C_2(i, j) \right|}{255} \right] \times 100\%, \end{gathered} \tag{14}$$

where $M \times N$ is the image size and $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$; namely, if $C_1(i, j) = C_2(i, j)$, then $D(i, j) = 0$; otherwise, $D(i, j) = 1$. Here, C_1 and C_2 are the two cipher-images whose corresponding plain-images are different only in one pixel.

In the proposed method, a small difference in the plain-image can affect the whole cipher-image. The results can be found in Table 2 (here, we randomly choose a pixel at position (201,100)). The percentage of pixel changed in the cipher-image is over 99.5% even with a one-bit difference in the plain-image. The UACI values are over 33.4%, as required for good protection [22, 23, 25]. Thus, the proposed encryption method is able to resist the differential attack.



(c)

(d)

Figure 3: Histogram plots: (a) plain-image, (b) cipher-image, (c) histogram of (a), and (d) histogram of (b).

Table 1: Correlation coefficients.

Model	Plain-image	Cipher-image
Horizontally	0.97799	−0.02068
Diagonally	0.98125	−0.04076
Vertically	0.96017	0.04687

Table 2: NPCR and UACI of two encrypted images with one-bit difference.

Image	Size	UACI	NPCR
Cameraman	256 × 256	0.33589	0.99579
Lena	256 × 256	0.33562	0.99578
Straw	512 × 512	0.33446	0.99594
Gravel	512 × 512	0.33457	0.99594

Table 3: Time test (second).

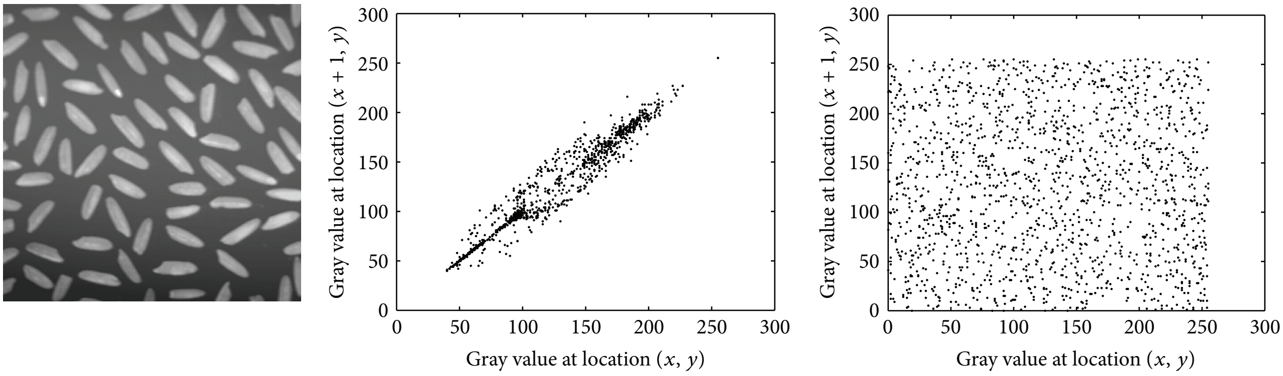
Image size	Reference [10]	Reference [11]	Reference [21]	Our method
256 × 256	0.172	0.156	1.342	0.055
512 × 512	0.702	0.764	5.257	0.195

(6) Speed Analysis. There are already many image encryption algorithms suggested. Here, we compare the speed of our method with [10, 11, 21], which is also composed of two stages of permutation and diffusion. The average time cost is listed in Table 3. The data show that the proposed method is fast and efficient, which is more suitable to encrypt large images.

(7) Information Entropy Analysis. Commonly, we take the information entropy as a tool to measure the strength of a cryptosystem. It is defined by (15) for message s:

$$H(s) = \sum p(s_i) \log \frac{1}{p(s_i)}. \tag{15}$$

Here, $p(s_i)$ represents the probability of occurrence of s_i and log means the base 2 logarithm. The information entropy is 8 for any ideal random sequence. Using the proposed algorithm, we can get the results for different images, as listed in



(a)

(b)

(c)

Figure 4: Correlation of two horizontally adjacent pixels in (a) plain-image, (b) correlation of (a), and (c) correlation of the cipher-image.

Table 4: Information entropy.

Image	Lena	Grass	Cameraman	Straw
Value	7.990	7.992	7.990	7.991

Table 4. They indicate that the cryptosystem can resist the entropy attacks.

(8) Other Comparisons. Compared with the existing methods [2, 22, 26], the proposed one using the time-delay chaotic system can show more natural phenomena when generating the chaotic sequence. Besides, only two blocks are decomposed with a new control parameter t which is determined by the plain-image and so the implementation time is shorter. To make the attack infeasible, any algorithm should have the ability to resist the chosen-plaintext, the chosen-ciphertext, and the known-plaintext attacks. However, in spite of good randomness and high computational efficiency, the keystream remains unchanged in the encryption process of [27], which cannot offer the security requirement [28]. In [26], the UACI is less than 28% while we can reach 33% in our method. All these show good performance by using the proposed scheme.

6. Conclusions

In this paper, a novel image encryption method based on chaotic maps and Circulant operation has been proposed. Position scrambling is employed to remove the high correlation between adjacent pixels in the plain-image. Meanwhile, to avoid statistical attacks, the modular function by blocks is adopted in the diffusion stage. Security analyses on (1) key space and key sensitivity, (2) histogram, (3) correlation between two adjacent pixels, (4) differential attacks, and (5) operating speed have been carried out. All the results are satisfactory which justify the effectiveness of the proposed algorithm for image encryption. Furthermore, the algorithm can be extended to images at any aspect ratio by the generalized Circulant matrix (see Definition 2 and appendix).

Appendix

The Case When m Is Not Equal to n

When m is not equal to n, we can also perform encryption on the image matrix $A_{m\times n}$. Without loss of generality, we assume $m < n$ and (7), (8), (10), and (12) are rewritten to the following forms, respectively:

$$\overline{B}(i,j) = \begin{cases} A(i,j), & 1 \le i \le m, \\ & i \le j \le n, \\ A(m+n+1-j, m+1-i), & 1 \le j-n \le m-1, \\ & j-n+1 \le i \le m, \\ 0, & \text{others}, \end{cases} \tag{A.1}$$

$$C(i,j) = \begin{cases} \overline{B}(i,j), & 1 \le i \le m, \\ & i \le j \le n, \\ \overline{B}(m-j+1, m+n+1-i), & 2 \le i \le m, \\ & 1 \le j \le i-1, \end{cases} \tag{A.2}$$

$$\overline{D}(i,j) = \begin{cases} A(i,j), & 1 \le i \le m, \\ & m-i+1 \le j \le n, \\ A(j-n+m, i-m), & n-m+1 \le j \le n-1, \\ & m+1 \le i \le m+n-j, \\ 0, & \text{others}, \end{cases} \tag{A.3}$$

$$E(i,j) = \begin{cases} \overline{D}(i,j), & 1 \le i \le m, \\ & m-i+1 \le j \le n, \\ \overline{D}(m+j, i+n-m), & 1 \le i \le m-1, \\ & 1 \le j \le m-i. \end{cases} \tag{A.4}$$

Acknowledgments

This project was supported by the National Natural Science Foundation of China (no. 11226091), the grant from CityU (Project no. 7008106), the Science & Technology Program Foundation of Zhanjiang City of China (no. 2011C3109002), and the Natural Science Foundation of Guangdong Ocean University of China (no. 1212334).

References

[1] X. Xue, Q. Zhang, X. Wei, L. Guo, and Q. Wang, "An image fusion encryption algorithm based on DNA sequence and multi-chaotic maps," *Journal of Computational and Theoretical Nanoscience*, vol. 7, no. 2, pp. 397–403, 2010.

[2] M. Amin, O. S. Faragallah, and A. A. Abd El-Latif, "A chaotic block cipher algorithm for image cryptosystems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 11, pp. 3484–3497, 2010.

[3] S.-J. Xu, X.-B. Chen, R. Zhang, Y.-X. Yang, and Y.-C. Guo, "An improved chaotic cryptosystem based on circular bit shift and XOR operations," *Physics Letters A*, vol. 376, no. 10-11, pp. 1003–1010, 2012.

[4] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 4653–4661, 2012.

[5] N. Singh and A. Sinha, "Optical image encryption using Hartley transform and logistic map," *Optics Communications*, vol. 282, no. 6, pp. 1104–1109, 2009.

[6] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," *Chaos, Solitons and Fractals*, vol. 29, no. 2, pp. 393–399, 2006.

[7] S. Li and X. Zheng, "Cryptanalysis of a chaotic image encryption and decryption," *Proceedings of IEEE International Symposium on Circuits and Systems*, vol. 2, pp. 708–711, 2002.

[8] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, no. 1–3, pp. 153–157, 2005.

[9] X. Y. Wang and X. M. Bao, "A novel block cryptosystem based on the coupled chaotic map lattice," *Nonlinear Dynamics*, vol. 72, pp. 707–715, 2013.

[10] G. D. Ye, "A chaotic image cryptosystem based on toeplitz and hankel matrices," *Imaging Science Journal*, vol. 57, no. 5, pp. 266–273, 2009.

[11] T. G. Gao and Z. Q. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons & Fractals*, vol. 38, no. 1, pp. 213–220, 2008.

[12] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.

[13] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," *Physics Letters A*, vol. 366, no. 4-5, pp. 391–396, 2007.

[14] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing Journal*, vol. 12, no. 5, pp. 1457–1466, 2012.

[15] W. Li and Y. Yuan, "A leak and its remedy in JPEG image encryption," *International Journal of Computer Mathematics*, vol. 84, no. 9, pp. 1367–1378, 2007.

[16] X.-F. Li, A. C.-S. Leung, X.-J. Liu, X.-P. Han, and Y.-D. Chu, "Adaptive synchronization of identical chaotic and hyper-chaotic systems with uncertain parameters," *Nonlinear Analysis. Real World Applications*, vol. 11, no. 4, pp. 2215–2223, 2010.

[17] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, John Wiley & Sons, New York, NY, USA, 2nd edition, 1995.

[18] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, no. 16-17, pp. 3895–3903, 2011.

[19] R. H. Chan and M. K. Ng, "Conjugate gradient methods for Toeplitz systems," *SIAM Review*, vol. 38, no. 3, pp. 427–482, 1996.

[20] H. Wang, X. Wang, X.-J. Zhu, and X.-H. Wang, "Linear feedback controller design method for time-delay chaotic systems," *Nonlinear Dynamics*, vol. 70, no. 1, pp. 355–362, 2012.

[21] X. Tong and M. Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically," *Image and Vision Computing*, vol. 26, no. 6, pp. 843–850, 2008.

[22] X. Wang and L. Teng, "An image blocks encryption algorithm based on spatiotemporal chaos," *Nonlinear Dynamics*, vol. 67, no. 1, pp. 365–371, 2012.

[23] F. Sun, Z. Lü, and S. Liu, "A new cryptosystem based on spatial chaotic system," *Optics Communications*, vol. 283, no. 10, pp. 2066–2073, 2010.

[24] Z. Wang, X. Huang, N. Li, and X. N. Song, "Image encryption based on a delayed fractional-order chaotic logistic system," *Chinese Physics B*, vol. 21, Article ID 050506, 2012.

[25] F. Sun, S. Liu, Z. Li, and Z. Lü, "A novel image encryption scheme based on spatial chaos map," *Chaos, Solitons and Fractals*, vol. 38, no. 3, pp. 631–640, 2008.

[26] X.-y. Wang, F. Chen, and T. Wang, "A new compound mode of confusion and diffusion for block encryption of image based on chaos," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 9, pp. 2479–2485, 2010.

[27] X.-y. Wang and Q. Yu, "A block encryption algorithm based on dynamic sequences of multiple chaotic systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 2, pp. 574–581, 2009.

[28] J. He, H. Qian, Y. Zhou, and Z. Li, "Cryptanalysis and improvement of a block cipher based on multiple chaotic systems," *Mathematical Problems in Engineering*, vol. 2010, Article ID 590590, 14 pages, 2010.