An improved chaotic cryptosystem based on circular bit shift and XOR operations

Shu-Jiang Xu\textsuperscript{a,b,c,*}, Xiu-Bo Chen\textsuperscript{a,b}, Ru Zhang\textsuperscript{a}, Yi-Xian Yang\textsuperscript{a}, Yu-Cui Guo\textsuperscript{d}

\textsuperscript{a} Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
\textsuperscript{b} State Key Laboratory of Information Security (Graduate University of Chinese Academy of Sciences), Beijing 100049, China
\textsuperscript{c} Shandong Provincial Key Laboratory of Computer Network, Shandong Computer Science Center, Jinan 250014, China
\textsuperscript{d} School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

\textbf{Abstract}

A type of chaotic encryption scheme by combining circular bit shift with XOR operations was proposed in 2006 based on iterating chaotic maps. Soon after the proposal, it was cryptanalyzed and improved. Unfortunately, there are still two drawbacks in the two improved schemes. To strengthen the performance of the focused type of scheme, a new improved scheme based on Chen’s chaotic system is proposed in this Letter. Simulation results and theoretical analysis show that our improved scheme is immune to information extracting by chosen plaintext attack and has expected cryptographic properties.

\section{1. Introduction}

With the rapid development of information technology and network technology, digital images and other multimedia are more commonly and frequently transmitted in public communication network. Therefore, it is particularly important to protect the image data against illegal purposes. So image encryption technology becomes an important issue of cryptography. Image data have strong correlations among adjacent pixels. Statistical analysis on large amounts of images shows that averagely adjacent 8 to 16 pixels are correlated in horizontal, vertical, and diagonal directions for both natural and computer-graphical images [1]. Moreover, due to some intrinsic features of images, such as bulk data capacity and high redundancy, encryption of images is quite different from that of texts [2]. As a result, conventional cipher algorithms, such as DES, IDEA, etc., are not directly suitable for image encryption. Therefore, many scholars have made an effort to investigate many new image encryption schemes in order to promote communication security recently [1-16]. A novel digital image encryption algorithm is presented by utilizing a new multiple-parameter discrete fractional random transform [3]. In the year 2011, N. Zhou et al. firstly introduced the fractional Mellin transform into the field of image security and proposed an originally novel nonlinear image encryption scheme with large key space and corresponding optoelectronic hybrid structure to overcome the drawbacks of image encryption schemes based linear transforms, such as Fourier transform [4]. Anil Kumar et al. propose an extended substitution-diffusion based image cipher using chaotic standard map [12]. By spatial bit-level permutation and high-dimension chaotic system, a color image encryption is proposed in [13]. Among these algorithms, the chaos-based cryptography has given a new and efficient way to develop fast and secure image encryption algorithms.

Chaos, which has many good properties, such as ergodicity, sensitive dependence on initial conditions and random-like behaviors, is an aperiodic complicated motion modality and nonlinear phenomenon [17]. Most of the properties have granted chaotic cryptosystems as a promising alternative for the conventional cryptographic algorithms [1]. Matthews first proposed the chaos-based encryption scheme in 1989 [6], and Fridrich first adopted chaotic map into image encryption in 1997 [7]. Since then, many chaos-based image encryption algorithms have been designed to realize secure communications [1,8-16].

With a pseudorandom bit sequence generated by iterating chaotic maps, a type of chaotic encryption scheme which was based on circular bit shift and XOR operations was proposed in [15,16]. In this type of algorithm, the plaintext block was permuted by a circular bit shift approach and then encrypted by the XOR operation block by block. However, it was shown that there are some defects with this type of algorithms in [18]: (1) Neither the chaotic trajectories of the logistic map nor those of the delayed chaotic neural networks have a uniform distribution, which leads to insufficient randomness of the chaos-based pseudorandom bit sequence generated from these chaotic trajectories. (2) Low
sensitivity of encryption to plaintexts. (3) Not secure against the differential known-plaintext attack and the chosen plaintext attack. It was pointed out that the type of scheme facilitates leakage of the information and is vulnerable to the chosen plaintext attack [19]. To obtain higher security, an improved scheme was suggested [19], but it was found that the first several bits in quantified sequence generated by chaotic sequence are still not sensitive to the least significant bits of chaotic state and the improved scheme cannot resist chosen plaintext attack [20]. Based on two chaotic maps, an improved scheme of [15,16] was proposed [21], in which the plaintext is first encrypted using the XOR operation block by block, and then it is encrypted using the circular bit shift operation block by block in the inverse order of the first round of encryption. Wang et al. pointed out that the encryption algorithm presented in [15] is vulnerable to chosen plaintext attack because of the plaintext-independent key stream, and suggested a straightforward improved scheme utilizing ciphertext feedback mechanism [22]. Nevertheless, Ben Farah et al. noticed that the improved scheme [22] still was insecure against chosen plaintext attack since the first block of key stream is also plaintext-independent, and proposed an improved algorithm by generating a random stream as the first block of key stream [23]. The improved scheme [22] was also analyzed using key stream attack and improved based on block cryptosystem by Guo et al. [24].

Because the first four steps of Guo’s improved scheme [24] is the same as that of Wang’s scheme [22], the first block of the key stream in Guo’s improved algorithm is also plaintext-independent. Therefore, the improved scheme [24] is unable to withstand chosen plaintext attack according to [23]. For the improved scheme [23], each encrypting process will generate a random key stream as the first block of key, which means that the secret key changes every time the algorithm is used. We think the improved scheme [23] is debatable, since this type of encryption scheme is a block cryptosystem rather than a stream cryptosystem or a one-time pad scheme. If a random key block is generated for several time encryption processes, the improved scheme [23] will be insecure against chosen plaintext attack. Note that the random stream can be used as part of the ciphertext instead of part of the secret key. Furthermore, the pseudorandom bit sequence was generated by the logistic map in these improved schemes [21–24], so the second defect shown in the above paragraph still exists in the schemes. When a plaintext byte is changed, only the ciphertext bytes behind the corresponding ciphertext byte are changed, so the improved schemes [21–24] also have low sensitivity to small changes of the plaintext. As a result, the two measures of differential analysis, NPCR and UACI, are still not reasonable in schemes [21–24]. Following the main idea of this type of chaos-based encryption scheme which combines the circular bit shift operations and XOR operations, an improved scheme of it is proposed in this Letter so as to strengthen its performance.

The rest of this Letter is organized as follows. Section 2 presents the approach to generate a statistical random number sequence by iterating the Chen’s chaotic system (CCS). An improved chaotic image encryption algorithm is introduced briefly in Section 3 based on the CCS. The experimental result is given in Section 4. Section 5 is devoted to security analysis. Finally, Section 6 concludes this Letter.

2. Random number sequence generation

2.1. Chen’s chaotic system

One-dimensional chaotic system which has the advantages of high-level efficiency and is implicit [25], such as Logistic map, is being widely used now. But their weaknesses, such as small key space and weak security, are also known to us obviously [26]. To overcome these drawbacks, a three-dimensional (3D) chaotic system is adopted in this Letter. With more than one initial conditions and control parameters, high-dimensional chaotic systems are most complex and have a big key space which has useful effect on the chaotic cryptosystem.

In 1999, Prof. G. Chen first presented CCS [27]:

\[
\begin{align*}
\dot{x} &= a(y - x), \\
\dot{y} &= (c - a)x - xy + cy, \\
\dot{z} &= xy - bz,
\end{align*}
\]

where \(a, b\) and \(c\) are parameters. Choosing \(a = 35, b = 3, c \in [20, 28, 4]\), the system enters chaotic domain which is shown in Fig. 1. The equations of CCS are quite similar to those of Lorenz system, while the topological properties of the two systems are not equivalent, essentially due to the parameter \(c\) in front of the state variable \(y\), which can lead to abundant dynamic characters of CCS. Therefore, the dynamical property of CCS is more complicated than Lorenz chaotic system. This feature is very useful in secure communications [28]. Eq. (1) will be solved by means of the fourth-order Runge–Kutta method. The time step size \(h\) which can be considered as one of the secret key here is chosen as 0.001.

2.2. Random number sequence

In this section, we will show that a statistical random sequence can be generated by CCS. As a result, the first defect shown in Section 1 can be successfully avoided. Suppose that \(x\) is a double-point value, and the random number is generated as follows:

\[
\text{mod}(\left\lfloor x \times 10^{12} - \left\lfloor x \times 10^{13} \right\rfloor \times 10^{3}, 256),
\]

where \(\text{mod}(x, y)\) returns the remainder after division. \(\lfloor x\rfloor\) rounds the elements of \(x\) to the nearest integers less than or equal to \(x\). Every time the CCS which has three variable values \(x_i, y_i\) and \(z_i\) is iterated, three random numbers can be got. Iterate CCS continuously, a random number sequence \(D = \{D_x \mid x = x_i, y_i, z_i\}\) can be obtained.

For the convenience to test randomness of the generated sequence \(D\), we can convert the decimal number \(D_x\) to binary number and divide it into bits. The obtained binary sequence \(B = \{B_i \mid B_i = 0, 1\}\) can be tested as below. Federal Information Processing Standard 140-2 which was published by the National Institute of Standards and Technology (NIST) defines the security requirements that must be satisfied by a cryptographic module used to protect unclassified information within information technology systems. In the documentation of FIPS PUB 140-2, statistical random number generator tests are defined as follows [29]: A single bit stream of 20,000 consecutive bits of output from RNG shall be subjected to monobit test, poker test, runs test and long runs test. The mono bit test measures whether the number of 0s and 1s produced by the
A sequence of random bits is generated by CCS with key $K = (x_0, y_0, z_0, c)$, where $c$ is a piecewise linear function. The poker test focuses on the randomness of the generated random sequence; the runs test and long runs test results are shown in Table 1. The runs test and long runs test are performed on the generated random binary sequence $B$ by CCS with key $K = (x_0, y_0, z_0, c)$, where $c$ is a piecewise linear function. The poker test focuses on the randomness of the generated random sequence; the runs test and long runs test results are shown in Table 1. The runs test and long runs test are performed on the generated random binary sequence $B$ by CCS with key $K = (x_0, y_0, z_0, c)$, where $c$ is a piecewise linear function.

### Table 1

<table>
<thead>
<tr>
<th>Length of run</th>
<th>Maximal number of consecutive '0'</th>
<th>Maximal number of consecutive '1'</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2463</td>
<td>2455</td>
</tr>
<tr>
<td>2</td>
<td>1251</td>
<td>1235</td>
</tr>
<tr>
<td>3</td>
<td>620</td>
<td>650</td>
</tr>
<tr>
<td>4</td>
<td>313</td>
<td>320</td>
</tr>
<tr>
<td>5</td>
<td>168</td>
<td>170</td>
</tr>
<tr>
<td>6+</td>
<td>155</td>
<td>150</td>
</tr>
<tr>
<td>26+</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### 3. The improved scheme based on circular bit shift and XOR operations

Suppose a plaintext $p_i$ ($i = 0, 1, \ldots, N - 1$) is given. If the plaintext is an image of size $M \times N$, it can be arranged by the order from left to right and top to bottom, and then a plaintext $P = p_0, p_1, \ldots, p_{MN-1}$ can be obtained. Suppose that the secret key $K = K(K_1; K_2) = (x_0^1, y_0^1, z_0^1, c_0^1, x_0^2, y_0^2, z_0^2, c_0^2, c_1)$, where the sub-keys $K_1, K_2$ include one of the control parameters and the initial conditions of the CCS. The proposed scheme shown in Fig. 2 is described below.

**Step 1.** Input the plaintext $P = p_0, p_1, \ldots, p_{N-1}$.

**Step 2.** Circular bit shift operation for the plaintext $P$ which is shown in Fig. 3.

1. Choose the sub-key $K_1 = (x_0^1, y_0^1, z_0^1, c_0^1)$, and then iterate CCS $n_1$ times to avoid the transient effect.

2. Iterate CCS once, and 3 bytes random numbers $d_1, d_2$, and $d_3$ can be gained by Eq. (2). Choose $d = \text{mod}(d_1 \oplus d_2, 8)$ and $e = \text{mod}(d_3, 2)$, where $\oplus$ is the XOR operation. If $e = 1$, permute the plaintext $p_i$ with left circular bit shift $d$ bits; otherwise, permute the plaintext $p_i$ with right circular bit shift $d$ bits.

3. If all the plaintext has already been encrypted, the encrypted plaintext $P' = p_0', p_1', \ldots, p_{N-1}'$ is obtained, and then turn to Step 3. Otherwise, $c = f(p_i')$, where $f$ is a piecewise linear function of $p_i'$.

**Step 3.** Let $M = m_0, m_1, \ldots, m_{N-1} = p'_{N-1}, p'_{N-2}, \ldots, p'_0$, that is to say, $m_j = p'_{N-j-1}$.

**Step 4.** As is shown in Fig. 4, XOR operations with ciphertext feedback for the modified plaintext $M$.

1. Choose the second sub-key $K_2 = (x_0^2, y_0^2, z_0^2, c_0^2, c_1)$, where $c_{1-1}$ is the initial feedback, and then iterate CCS $n_2$ times to avoid the transient effect.

2. Iterate CCS once, and 3 bytes random numbers $d'_1, d'_2$, and $d'_3$ can be gained by Eq. (2). Then encrypt $m_3i, m_{3i+1}, m_{3i+2}$ as follows:

$$c_{3i} = m_{3i} \oplus d'_1 \oplus c_{3i-1},$$

$$c_{3i+1} = m_{3i+1} \oplus d'_2 \oplus c_{3i},$$

$$c_{3i+2} = m_{3i+2} \oplus d'_3 \oplus c_{3i+1},$$

where $\oplus$ is the XOR operation.
(3) If all the modified plaintext has already been encrypted, then the ciphertext \( C \) is obtained, and the encryption process is ended. Otherwise, \( c = f(c_{3i+2}) \), where \( f \) is a piecewise linear function of \( c_{3i+2}: \)

\[
c = \begin{cases} 
\frac{c - q_i}{256}, & c > c_0^2, \\
\frac{c + q_i}{256}, & c \leq c_0^2, 
\end{cases}
\]

where

\[
q_i = \begin{cases} 
\frac{c_{3i+2} + n}{2}, & c_{3i+2} < n, \\
\frac{c_{3i+2}}{2}, & n \leq c_{3i+2} < 256 - n, \\
\frac{c_{3i+2} - n}{2}, & c_{3i+2} \geq 256 - n, 
\end{cases}
\]

and \( n \) is a small constant. Similar to Eq. (4a), Eq. (7a) can be simplified into Eq. (7b) or Eq. (7c):

\[
q_i = \begin{cases} 
\frac{c_{3i+2} + n}{2}, & c_{3i+2} < n, \\
\frac{c_{3i+2}}{2}, & c_{3i+2} \geq n, 
\end{cases}
\]

Let \( i = i + 1 \) and turn to (2).

**Step 5.** Output the ciphertext \( C = c_0, c_1, \ldots, c_{N-1} \).

By Eq. (4a) and Eq. (7a), it can be guaranteed that the perturbation is not only not too small, but also not too much. For this purpose, we suggest \( 1 \leq n \leq 20 \). For simplification, we choose \( n = 10 \) in this Letter. The improved scheme using Eq. (4a) and Eq. (7a), Eq. (4b) and Eq. (7b), Eq. (4c) and Eq. (4c) can be called case 1, case 2 and case 3, respectively. Using Eq. (3) or Eq. (6), a small perturbation is given to one of the control parameters of CCS after iterating CCS every time. It is useful to make the improved scheme not only resist to the chosen plaintext attack, but also very sensitive to the small change of the plaintext.

The decryption process is almost the same as the encryption one. We only need to do XOR operation by \( K_2 \) for the ciphertext first, and then do the inverse shift operation for the obtained text by the inverse order of the XOR operation. Finally, the plaintext can be recovered.

### 4. The experimental results

The experimental results are presented in this section. We take a 256 gray-scale BMP plain-image of size 256 × 256 for example. The two sub-keys are chosen as \( K_1 = (x_1^0, y_1^0, z_1^0, c_1^0) = (−10.058, 0.368, 37.368, 26) \) and \( K_2 = (x_2^0, y_2^0, z_2^0, c_2^0, c_{-1}) = (−10.057, 0.367, 37.369, 26, 127) \). Fig. 5 shows the experimental results. Fig. 5(1) is the plain-image. Figs. 5(2)–(4) are the cipher-images by case 1, case 2 and case 3. As can be seen from Figs. 5(2)–(4), the cipher-images are unknowable and rough-and-tumble, thus the diffusion and confusion properties are confirmed.

The improved algorithms are performed by Visual C++ 6.0 and running in a PC with Intel Core i7 CPU 2.67 GHz 2.67 GHz, 3.00 GB memory, 500 GB hard-disk capacities. The time used in encryption on 256 gray-scale BMP images of size 256 × 256 by the proposed scheme and schemes [21–24] is shown in Table 2. According to Table 2, each case of the improved scheme is faster than all the others [21–24], which indicates that the improved algorithm is fast enough for practical transmission of image files over public communication network. And the encryption speed of our scheme is almost 4 times as quickly as that of [22–24], that is to say, compared with schemes [22–24] which include too many iterations of the chaotic maps, our scheme only takes about one fourth that of [22–24] for encrypting an image.

### 5. Security analysis

To illustrate the performance of our improved scheme, some security analysis on the improved encryption scheme, including key space analysis, information entropy, statistical analysis of two adjacent pixels and differential analysis, etc., which can show the satisfactory security of the proposed scheme, is shown in this section.

#### 5.1. Key space analysis

A good encryption scheme should be sensitive to the secret key, and the key space should be large enough to make brute-force attacks infeasible. From the perspective of cryptography, the size of the key space for any encryption algorithm should be not smaller than \( 2^{100} \approx 10^{30} \) to achieve high level of security [30]. Two groups of secret keys, including the initial values and one of the control parameters of CCS, are adopted in our encryption algorithm. Suppose the precision is \( 10^{-15} \), and the key space size at last is \((10^{15})^4 = 10^{60} \). Table 3 shows key space of the proposed scheme and schemes [21–24]. Compared with the key space of schemes [21–24], the key space of the proposed scheme is large enough to resist all kinds of brute-force attacks.

#### 5.2. Information entropy

The information entropy which is defined to express the degree of uncertainties in the system is defined as:

\[ H = -\sum p_i \log_2 p_i \]
\[ H(m) = - \sum_{i=0}^{2^k-1} P(m_i) \log_2[P(m_i)]. \] (8)

where \( P(m_i) \) is the emergence probability of \( m_i \). If every symbol has an equal probability, i.e., \( m = \{m_0, m_1, \ldots, m_{2^k-1}\} \) and \( P(m_i) = 1/2^k \) \( (i = 0, 1, \ldots, 255) \), then the entropy is \( H(m) = 8 \), which corresponds to a random source. Actually, the practical information entropy is usually less diverse than the ideal one. By two different keys, \( K \) which is adopted in Section 4, and \( K' \), in which only \( c_2^2 = 22 \) is not the same as that in \( K \), the information entropy is respectively shown in Table 4 which is very close to the ideal.

**Table 4**

<table>
<thead>
<tr>
<th>Case</th>
<th>Information entropy with ( K )</th>
<th>Information entropy with ( K' )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>7.9973</td>
<td>7.99732</td>
</tr>
<tr>
<td>Case 2</td>
<td>7.99698</td>
<td>7.99768</td>
</tr>
<tr>
<td>Case 3</td>
<td>7.99695</td>
<td>7.9966</td>
</tr>
</tbody>
</table>

Fig. 5. Encryption experimental results.

Fig. 6. Gray-scale histogram of plain-image and cipher-images.
we can also conclude that the similar information entropy can be obtained by any of the three encryption algorithms.

5.3. Statistical analysis

5.3.1. Gray-scale histograms

Considering the statistical analysis of Lena image and its encrypted images, the gray-scale histograms of them are shown in Fig. 6. From Figs. 6(2)-(4), we can see that the gray-scale distribution of cipher-images have good balance property, which is strong against known plaintext attack.

5.3.2. Correlation analysis of two adjacent pixels

In order to test the correlation between two adjacent pixels in plain image and ciphered image, the following method was carried out [2]. We select 1000 pairs of two adjacent (in horizontal, vertical, and diagonal direction) pixels from an image randomly and calculate the correlation coefficient of each pair using:

\[
\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)),
\]

(9)

\[
r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}},
\]

(10)

where \(x\) and \(y\) are gray-scale values of two adjacent pixels in the image. In numerical computation, the following formulas are used:

\[
E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i,
\]

(11)

\[
D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2.
\]

(12)

Figs. 7–9 respectively show the correlation distribution of two horizontally, vertically and diagonally adjacent pixels in the plain-image and those in the cipher-images by case 1–3, and the correlation coefficients by case 1 are shown in Table 5. It is shown that the correlation coefficients of two horizontally, vertically and diagonally adjacent pixels in the plain-image and those of the cipher-images are all far apart. The measured correlation coefficients of the plain-image are close to 1 while those of the cipher-images are nearly 0. As a result, each case of the chaotic encryption algorithm satisfies zero co-correlation.
5.4. Differential analysis

Two common measures, NPCR and UACI [2], were used to test the influence of a single pixel change on the cipher-image. NPCR means the change rate of the number of pixels of ciphered image while one pixel of plain-image is changed. UACI defines the average intensity of the differences between the plain-image and the cipher-image.

Give two cipher-images, whose corresponding plain-images have only a single pixel difference, mark them as $C_1$ and $C_2$, respectively. Label the gray values of the pixels at grid $(i, j)$ of $C_1$ and $C_2$ by $C_1(i, j)$ and $C_2(i, j)$, respectively. Define a bipolar array $D$ with the same size as image $C_1$ or $C_2$. $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$, if $C_1(i, j) = C_2(i, j)$ then $D(i, j) = 0$; otherwise, $D(i, j) = 1$. NPCR and UACI are defined as:

\[
\text{NPCR} = \frac{\sum_{i,j} |D(i, j)|}{W \times H} \times 100\%,
\]

\[
\text{UACI} = \frac{1}{W \times H} \left[ \sum_{i,j} \left( \frac{|C_1(i, j) - C_2(i, j)|}{255} \right) \right] \times 100\%,
\]

where $W$ and $H$ are the width and height of $C_1$ or $C_2$.

Suppose two 256 gray-scale plain-images, $P_1$ and $P_2$, of size $256 \times 256$ only have a single pixel difference in position $(i, j)$ ($i, j = 0, 1, \ldots, 255$), choose $P_2(i, j) = P_1(i, j) + 1$ when $P_1(i, j) < 255$ or $P_2(i, j) = 254$ when $P_1(i, j) = 255$. With two different keys, $K$ and $K'$, tests have been performed on the improved scheme and schemes [21–24]. The results are shown in Tables 6 and 7, respectively. It is indicated that a swift change in the original image will result in a significant change in the cipher-images by the proposed scheme, so the second defect shown in Section 1 is overcome and the improved algorithm has the ability to resist differential attack. However, there is no obvious change in the ciphertext with a swift change in the original image by each of the schemes [21–24] because the NPCR of schemes [21–24] is very close to 1 and the UACI of them is 0 or very close to 0. According to Tables 6 and 7, we can draw the conclusion as follows: UACI > 0.33% and NPCR < 0.51% by any case of the proposed scheme, and all the three cases have a higher sensitivity to the small change of the plaintext. With the perturbation measure, two rounds of encryption process which follow opposite directions are adopted in the proposed scheme. As a result, each plaintext has an effect on almost all of the others according to the NPCR shown in Tables 6 and 7. Therefore, our improved scheme is secure against chosen plaintext attack and key stream attack. To obtain a better performance against attackers, we suggest randomly choosing one of the three cases for each time encryption.

6. Conclusions

Two drawbacks in the improved schemes of a type of chaotic encryption algorithm based on circular bit shift and XOR operations are pointed out and a new improved scheme is proposed to strengthen the overall performance of the focused type of scheme. CCS instead of logistic map is adopted to generate random number sequence which is shown as statistical random by FIPS 140-2 tests in the improved scheme so as to avoid the first defect shown in Section 1. The plaintext is scrambled using the circular bit
shift operation byte by byte firstly, and then the modified plaintext is substituted using the XOR operation in the inverse order of the permutation. With the purpose of enhancing its security and overcoming the second defect, a small perturbation based on the last obtained one byte encrypted plaintext is given to the parameter $c$ of the CCS after iterating the chaotic map every time. Simulation experiments show that the improved scheme is fast enough to transmit image files over the public communication network and theoretical analysis indicates that the new improved scheme can achieve a high performance. Compared with other improved schemes of this type of chaos-based encryption scheme, our scheme has the advantages of a high encryption speed and a big key space. Moreover, our scheme achieves a very small NPCR as well as a reasonable UACI.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Nos. 61070163, 60973146, 61003284 and 61141007), the Natural Science Foundation of Shandong Province, China (Nos. ZR2009GM036, ZR2011FM023) and the Shandong Province Outstanding Research Award Fund for Young Scientists of China (No. BS2011DX034).

References