Plaintext Related Two-level Secret Key Image Encryption Scheme

Yong Zhang*, Jiali Xia, Peng Cai, Bin Chen
School of Software and Communication Engineering
Jiangxi University of Finance and Economics, Nanchang, P. R. China
*corresponding author, e-mail: zhangyong@jxufe.edu.cn

Abstract
Some chaos-based image encryption schemes using plain-images independent secret code streams have weak encryption security and are vulnerable to chosen plaintext and chosen cipher-text attacks. This paper proposed a two-level secret key image encryption scheme, where the first-level secret key is the private symmetric secret key, and the second-level secret key is derived from both the first-level secret key and the plain image by iterating piecewise linear map and Logistic map. Even though the first-level key is identical, the different plain images will produce different second-level secret keys and different secret code streams. The results show that the proposed has high encryption speed, and also can effectively resist the existing cryptanalytic attacks.

Keywords: chaotic encryption, two-level secret key, image encryption, cryptanalysis

1. Introduction
Chaotic secure communication is one of the most important applications of chaos theory. In the field of chaotic secure communication, there are two types of chaotic encryption systems: one is the analog chaotic secure system based on chaotic synchronization [1-3], the other is the digital encryption system based on chaotic pseudo-random sequence [4-7]. At present, the latter becomes a research hot topic of studying chaotic encryption system, and the proposed encryption scheme also falls into this category.

Recently, G. Alvarez and S. J. Li summarized a large number of problems in the literatures about chaos based encryption systems published before 2005, and put forward some useful suggestions and rules for designing chaos based encryption system to follow [8]. For example, the secret key of encryption system should be clearly defined (Rule 4, [8]): knowing part of secret key information cannot partially decrypt the cipher text (Rule 7, [8]); tiny differences in the secret key or plaintext will result in completely different cipher-text (Rule 6, [8]); the key space should only contain valid secret keys (Rule 5, [8]); cipher-text should have statistical properties similar to white noise (Rule 10, [8]); encryption method is easy to implement and encryption speed is fast enough for real communications (Rule 3, [8]); encryption system can fight against the existing attack methods, particularly against chosen plaintext or chosen cipher-text attacks (Rule 11, [8]), etc.

According to the above rules, the encryption schemes proposed in literatures [9-13] have some drawbacks, among which the most important point is that, the secret code streams in these encryption schemes are independent of plain text, and these schemes cannot effectively resist the attacks of known/chosen plaintext, which violates the Rule 11 in [8]. In literatures [14-18], the researchers analyzed the cryptographic performance of literatures [9-13], and with known/chosen plaintext or other methods obtained all or part of equivalent secret keys of those encryption systems, so demonstrated that the cryptosystems proposed in [9-13] have security issues and cannot be used in real communications. Also, the literature [18] confirmed that the key space of encryption scheme proposed in [13] contains a large number of invalid secret keys, and furthermore, knowing part of secret keys can decrypt the cipher-text to obtain some visual information of original plaintext. Obviously, these shortcomings and deficiencies
should be avoided in the design of chaotic encryption systems, and also indicate that there is a lot of research work to be done in the field of chaotic image encryption.

The aforementioned encryption systems based on chaotic systems [9-13] have security problems, mainly because the secret code streams used only depend on the secret keys, and are independent of plaintext, i.e. when secret keys are determined, the same secret code streams will be used to encrypt arbitrary plaintext. It was pointed out in [19] that if these types of cryptosystems use only confusion without diffusion methods for encryption, the attacker can certainly decrypt them successfully through choosing \( \lfloor \log_{M \cdot N} \lfloor +1 \) plain images, where \( M \) and \( N \) are the height and width of plain image, \( L \) is the number of pixel gray levels, and \( \lfloor \cdot \rfloor \) denotes the smallest integer greater than or equal to \( x \). These shortages were noticed in [20, 21], and methods of producing secret code streams related with plaintext were put forward. In [20], using Tent map and four floating-point forms of initial values (secret keys), together with the whole plain image, the authors produced a length of 128-bit hash code, which then was converted into initial values and parameters of 2D standard map and Logistic map, and iterated these two maps to obtain secret code streams which were employed to confuse and diffuse the plain image to get the cipher image. Thus, the sender needs to transfer secret keys and hash code to the receiver at the same time, so that the receiver can decrypt the cipher image to restore the original plain image. In [21], not the image pixel information but the size of plain image was used as part of secret keys, which makes this cryptosystem vulnerable to time attack method [17]. The common deficiencies of encryption schemes proposed in [20, 21] are that there are different secret keys for different plain images, therefore, the cipher images were transmitted by public open network, each time meanwhile, the corresponding secret keys were transmitted by private secure communication channel, which increases the burden of communication and brings inconveniently to legitimate receiver.

Trying to solve this problem, this paper presents a two-level secret key encryption scheme, which includes two ranks of secret keys, of which the first level secret key (L1SK) is the common used symmetric key by both the sender and the receiver, and the second level secret key (L2SK) is produced by L1SK and the information extracted from plain image, i.e. L2SK depends on both L1SK and plain image. L2SK works as the initial value and parameter of piecewise linear map, through iterating to generate the secret code streams for directly encrypting used, therefore, the secret code streams depend on both L1SK and plain image. The rest of this paper is organized as follows: section 2 describes the used chaotic maps, i.e. piecewise linear map and Logistic map for expressing conveniently; section 3 introduces the encryption/decryption scheme of the proposed two-level secret key encryption system; section 4 illustrates some representative simulation results through numerical experiments of encryption and decryption schemes; section 5 analyzes secure performance of the proposed encryption system in detail, mainly focusing on the characteristics of cipher-text, the key space, encryption speed, and against chosen plaintext or chosen cipher-text attack; section 6 concludes the paper.

2. Used Chaotic Maps

This paper uses three chaotic maps, denoted as Map-A, Map-B and Map-C, respectively, whose formulae are tabulated in Table 1.

<table>
<thead>
<tr>
<th>Map-A</th>
<th>Map-B</th>
<th>Map-C</th>
</tr>
</thead>
<tbody>
<tr>
<td>( F(x) = \begin{cases} \frac{x}{p}, &amp; x \in [0, p] \ \frac{1-x}{1-p}, &amp; x \in (p,1] \end{cases} )</td>
<td>( F(x) = \begin{cases} \frac{x}{p}, &amp; x \in [0, p] \ \frac{x-p}{0.5-p}, &amp; x \in (p,0.5] \ F(1-x, p), &amp; x \in (0.5,1] \end{cases} )</td>
<td>( x(n+1) = \mu \cdot x(n)(1-x(n)) )</td>
</tr>
</tbody>
</table>

Plaintext Related Two-level Secret Key Image Encryption Scheme (Yong Zhang)
In Table 1, \( p \) is the parameter of Map-A and Map-B, and \( \mu \) and \( n \) are the parameter and iteration time of Map-C, respectively. Map-A and Map-B are called continuously piecewise linear map, particularly, when \( p = 0.5 \), Map-A is also called Tent map. Map-B was used in the encryption system proposed in [22], and literatures [23, 24] further confirmed that Map-A and Map-B can produce pseudo-random sequences with good statistical properties even under the condition of finite word-length computing. The well-known Map-C, namely the discrete time Logistic map, was a simple one-dimensional discrete dynamical system presented by R. M. May in 1976 [25], and when \( 3.569945627 < \mu \leq 4.0 \), complicated chaos phenomena which were analyzed in detail in [26] exist in this system, and we set \( \mu = 4.0 \) in this paper.

3. Proposed Encryption Scheme
3.1. Two-level Secret Key Encryption System

The typical digital image encryption scheme with symmetric secret key [7, 27, 28] includes two basic encryption operations: confusion and diffusion, and sometimes many rounds of confusion and diffusion, which can be found in Shannon's masterpiece in 1949 [29]. Confusion operation uses secret code streams to change image pixel positions or pixel values or both, such that the adjacent pixels of the confused image are irrelevant or the confused image has noise-like histogram. However, diffusion operation refers to the change of one plain image pixel location or pixel value causes the avalanche effect of changes of cipher image pixels as many as possible, i.e. the plain images with the change of one pixel location or pixel value will be encrypted into completely different cipher images so as to resist chosen plaintext attack. If the secret code streams used to encrypt the plaintext only depend on the secret key, and do not rely on the plaintext, when the secret key is fixed, encrypting different plaintexts employs exactly the same secret code streams, which as a defect was discussed in [14-18] to find that this type of system cannot resist the chosen plaintext or chosen cipher-text attack well.

Through the above analysis, it can be seen that the secret code streams used for encryption should depend on both the secret key and the plaintext. However we should not directly use part of information extracted from plaintext as part of secret keys. This contradiction can be overcome through the two-level secret key encryption system as shown in Figure 1. This scheme belongs to symmetric key encryption scheme, in which the communication pairs use the same secret key, namely L1SK. Chaos system I with L1SK produces pseudo-random sequences, which, together with the information extracted from plaintext, generates L2SK, and then, chaos system II using L2SK produces the secret code streams for encryption. In this way, the secret code streams depend on not only secret keys (L1SK), but also the information extracted from plaintext. The chaos system I and chaos system II in Figure 1 can be one identical chaotic system, also can choose two different chaotic systems, and the only requirement is that such chaotic systems can produce pseudo-random sequences with good statistical properties by iteration under the condition of finite word length computing. Map-A, Map-B and Map-C are chosen as chaos system I, and Map-B is selected as chaos system II in this paper.

![Figure 1. Two-level secret key encryption system](image_url)
3.2. Encryption Scheme

Based on the scheme in Figure 1, we design the two-level secret key encryption scheme as shown in Figure 2. The secret key of the encryption system, namely L1SK, is denoted by \( \{x_A, p_A, s_A, p_B, x_B\} \), where, \( x_A \) and 0.25+0.50\( p_A \) are the initial value and parameter of Map-A, respectively, and \( x_B \) and 0.50\( p_B \) are the initial value and parameter of Map-B, respectively, and \( x_C \) is the initial value of Map-C with the parameter of \( \mu = 4.0 \).

In Figure 2, \( m \) is the size of plain image, and if the height and width of plain image are denoted as \( M \) and \( N \), then \( m=MN \), which means the image has \( m \) pixels. Suppose the image is of \( L \)-bit grayscale and so each pixel is in the range \([0, 2^L-1]\). Arrange the pixels of plain image in scan order of from left to right and from top to bottom to obtain the one-dimensional array \( I = \{i; i=0,1,2,\ldots,m-1\} \).

![Figure 2. The proposed two-level secret key encryption scheme](image)

The encryption processes as shown in Figure 2 are as follows:

**Step 1.** Use \( x_A \) and 0.25+0.50\( p_A \) as the initial value and parameter of Map-A, respectively, and iterate Map-A to generate a chaotic sequence, denoted by \( S_A: \{x_{A,0}, x_{A,1}, \ldots, x_{A,m-1}\} \) (excluding the beginning of transient points of 200 iterations); use \( x_B \) and 0.50\( p_B \) as the initial value and parameter of Map-B, respectively, and iterate Map-B to produce another chaotic sequence, denoted by \( S_B: \{x_{B,0}, x_{B,1}, \ldots, x_{B,m-1}\} \) (excluding the beginning 200 transient points); use \( x_C \) as the initial value of Map-C, and iterate Map-C to generate the third chaotic sequence, denoted by \( S_C: \{x_{C,0}, x_{C,1}, \ldots, x_{C,m-1}\} \) (excluding the beginning 200 transient points).

**Step 2.** Choose the front \( u (u=16 \) thereinafter) pixels in turn from the sequences \( S_A \) and \( S_B \), respectively, and each forms a new sequence, denoted by \( S_A': \{x_{A,0}, x_{A,1}, \ldots, x_{A,u-1}\} \) and \( S_B': \{x_{B,0}, x_{B,1}, \ldots, x_{B,u-1}\} \), respectively. According to the following Eqs. 1-2, two new integer sequences \( S_A: \{x_{A,0}, x_{A,1}, \ldots, x_{A,u}\} \) and \( S_B: \{x_{B,0}, x_{B,1}, \ldots, x_{B,u}\} \) can be obtained from the above two
Let regarded as “L2SK 1” in Figure 2. Here, when the height \( M \) or width \( N \) of the image is greater than \( 10^5 \), the plain image should be divided into small blocks for facilitating processing.

Based on the coordinates \((s_{u,i}, s_{v,i})\), \( i = 0, 1, \ldots, u-1 \), i.e. \( M \times N \) for the indices of one-dimensional array \( I \), from the plain image \( I \) we select \( u \) pixels, whose values are denoted by \( \{v_{0,0}, v_{1,1}, \ldots, v_{u-1}\} \). We make

\[
[v_{0,0}, v_{1,1}, v_{2,2}, v_{3,3}]^T = VE + E
\]

(3)

\[
[v_{0,0}, v_{1,1}, v_{2,2}, v_{3,3}]^T = E^TV + E^T
\]

(4)

Here, \( V=[V_0, V_1, V_2, V_3] \), \( V=[V_0, V_{16}, V_{32}, V_{48}] \), \( V_{i+1} \), \( i = 0, 1, 2, 3 \), and \( E=[1 \quad 1 \quad 1 \quad 1]^T \). \((s_{u,i}, s_{v,i})\), \( i = 0, 1, \ldots, u-1 \) are regarded as “L2SK 1” in Figure 2.

**Step 3.** With the front \( u \) pixels in the sequence \( S_C \), namely \( \{v_{C,i}, i = 0, 1, \ldots, u-1\} \), by means of the following Eqs. 5-6, the \( u \) pixel values \( \{v_{i}, i = 0, 1, \ldots, u-1\} \) from the plain image will be transformed into the corresponding new values, namely \( \{v_{C,i}, i = 0, 1, \ldots, u-1\} \), without altering the locations of the \( u \) pixels, which will not participate in the following operations of Steps 4-5.

\[
v_{C,0} = v_{u-1} + \left[ (s_{C,0} \times 100 - s_{C,0} \times 10^6) \mod 2^L \right] \mod 2^L
\]

(5)

\[
v_{C,i} = (v_{C,i-1} + [s_{C,i} \times 100 - s_{C,i} \times 10^6] \mod 2^L) \mod 2^L, \quad i = 0, 1, \ldots, u-1
\]

(6)

**Step 4.** With the help of the \( u \)th \(-\) \((m-1)\)th elements of sequences \( S_A \), \( S_B \) and \( S_C \), we calculate the sequences \( x_D(x_{D,i}, i = 0, 1, \ldots, m-u-1) \) and \( p_D(p_{D,i}, i = 0, 1, \ldots, m-u-1) \), respectively, using the following formulae:

\[
x_{D,i} = (s_{D,i} + s_{C,i}) \mod 1, \quad i = 0, 1, \ldots, m-u-1
\]

(7)

\[
p_{D,i} = (s_{D,i} + s_{C,i}) \mod 1, \quad i = 0, 1, \ldots, m-u-1
\]

(8)

Let

\[
x_{E,i}=[v_{i,0}, v_{i,1}, v_{i,2}, v_{i,3}]\{s_{C,i+u}, s_{C,i+u+1}, s_{C,i+u+2}, s_{C,i+u+3}\} \mod 1, \quad i = 0, 1, \ldots, m-u-1
\]

(9)

\[
p_{E,i}=[v_{i,0}, v_{i,1}, v_{i,2}, v_{i,3}]\{s_{C,i+u}, s_{C,i+u+1}, s_{C,i+u+2}, s_{C,i+u+3}\} \mod 1, \quad i = 0, 1, \ldots, m-u-1
\]

(10)

Then, let

\[
x_{E,i} = (x_{D,i} + x_{E,i}) \mod 1, \quad i = 0, 1, \ldots, m-u-1
\]

(11)

\[
p_{E,i} = (p_{D,i} + p_{E,i}) \mod 1, \quad i = 0, 1, \ldots, m-u-1
\]

(12)

The derived sequences \( x_F(x_{F,i}, i = 0, 1, \ldots, m-u-1) \) and \( p_F(p_{F,i}, i = 0, 1, \ldots, m-u-1) \) are called as “L2SK k”, \( k = u+1 \) as shown in Figure 2. Compared to L1SK \( \{x_A, x_B, x_C\} \) with only 5 floating-point numbers, L2SK here has \( 2(m-u) \) float-point numbers.

**Step 5.** Let the \( 2(m-u) \) L2SKs \( x_F \) and \( p_F \) obtained in the previous step as the initial values and parameters of Map-B, respectively, and iterate each Map-B one time to get a new
state value, and then we will get \( m-u \) state values, which constitute a new sequence, denoted by \( x_G; \{x_G,j=0,1,...,m-u-1\} \), from which we will get an integer sequence \( x_H; \{x_H,i=0,1,...,m-u-1\} \) using Eq. 13.

\[
x_{H,i} = \left( \left( x_{G,i} \times 100 - \left[ x_{G,i} \times 100 \right] \right) \times 10^5 \right) \mod 2^L, \quad i=0,1,...,m-u-1
\]  

(13)

The sequence \( x_H \) is the secret code stream used for encrypting the plain image \( I \) (except the \( u \) pixels selected in Step 2), and the encryption method can be “add and modulus” operations. Denote the plain image without considering the \( u \) pixels selected in Step 2 by \( I_i; \{I_i,j=0,1,...,m-u-1\} \), whose corresponding cipher image is denoted by \( C_{ij}; \{c_{ij}, j=0,1,...,m-u-1\} \) after the following Eqs. 14-15, and denote the intermediate cipher image by \( C_{1j}; \{c_{1j},i=0,1,...,m-1\} \), which consists of \( C_{1j} \) and \( v \) obtained in Step 3.

\[
c_{1j} = \left( I_i + x_{H,j} \right) \mod 2^L,
\]

(14)

\[
c_{ij} = \left( I_i + x_{H,j} + c_{1j-1} \right) \mod 2^L, \quad j=1,2,...,m-u-1
\]

(15)

**Step 6.** Make the \( C_{1j} \) as the new plain image \( I \) and repeat the above Steps 2-5 to get the cipher image \( C \).

The decryption processes are similar to the encryption processes but in reverse order.

4. Results of Simulation Experiments

Here, the encryption results of one representative plain image are given. Figure 3a is 8-bit grayscale image Lenna (of size 512×512 pixels). Figure 3b shows the histogram of Figure 3a. With the secret key (i.e. L1SK) \{0.12345, 0.67890, 0.24680, 0.97531, 0.54768\}, the encryption result is shown in Figure 3c. Figure 3d shows the histogram of Figure 3c which can be decrypted to be exactly identical to Figure 3a.

![Figure 3. Plain image Lenna and its cipher image](image)

5. Encryption Performance Analysis

5.1. Features of Ciphered Image

The cipher image has white noise-like flat histogram (Figure 3d). From Figure 3a and Figure 3c, respectively, we randomly choose 10,000 pairs of adjacent pixels in horizontal, vertical and diagonal directions to calculate the statistical correlation coefficients [7], denoted by \( r_h, r_v, \) and \( r_d \), respectively. We can get that \( r_h=0.0014, \ r_v=0.0060, \) and \( r_d=0.0095 \) in cipher image, which are almost irrelevant, while \( r_h=0.9673, \ r_v=0.9835, \) and \( r_d=0.9559 \) in plain image.

From Figure 3a, we randomly selected 1000 pixels, and changed the value of each pixel (each pixel gray value plus 1) in turn, then used the secret key \{0.12345, 0.67890, 0.24680, 0.97531, 0.54768\} to encrypt the plain images with one pixel different to get the corresponding cipher images, which are employed to calculate the NPCR and UACI, whose mean values are denoted by NPCRav and UACIav, respectively. Then we get that NPCRav = 99.6138% and UACIav = 33.4689%.
5.2. Encryption and Decryption Speed

It was pointed out in [30] that its encryption scheme has fast encryption speed, which is much faster than the traditional DES method. So we analyzed the encryption/decryption speed of the proposed scheme, compared with that of in [30]. The computer with Intel Core i5 460M processor, 2GB memory, windows 7 and MATLAB 7.12 was used for testing. The secret key of proposed scheme is \(0.57832101, 0.14895421, 0.96323408, 0.39712064, 0.82610432\), and the time of generating sequences \(s_1\), \(s_2\) and \(s_3\) is neglected; the secret key of the scheme [30] is \(K=1600, h_1=0.342101, h_2=0.732302, h_3=0.521084, k_1=0.621094, k_2=0.432187, k_3=0.821904\), and according to requirements of [30], the iteration times are set to 4. 10 grayscale images (of size 512×512) are used for testing. The mean speed of the proposed scheme is 2.91s superior to that of 3.64s in [30].

5.3. Key Space

The proposed scheme belongs to the symmetric secret key encryption scheme based on block encryption. The secret keys \(\{x_A, p_A, p_B, x_C\}\) of the proposed scheme are all floating-point numbers, also called L1SK, whose design accuracy is \(10^{-10}\), so that the total key space capacity adds up to \(0.25×10^{50}≈10^{49.9270}\). The same plain image will be encrypted into two completely different cipher images with slightly changed secret keys (more than 99.6% pixels are different between two cipher images), i.e. the secret key is very sensitive. The L2SK is employed directly to produce the secret code stream \(\{s, x, p, b\}\), so we can consider L2SK as secret key of the proposed scheme, then the volume of secret key space is \(10^{60(m^2)}\).

5.4. Against Chosen Plaintext Attack

According to Kerchoff’s rules [31], assuming that the attacker can fully access to the encryption scheme of knowledge, a good encryption scheme should be able to resist against chosen plaintext attack and chosen cipher-text attack. Chosen plaintext attack is intended to obtain secret key or equivalent secret key of encryption system. The evolution of from L1SK to L2SK in the proposed scheme is processed by chaotic maps iterations and numerical truncations, so that even if the attacker knows all of L2SKs, he still cannot recover the L1SK from the truncated data, i.e. the L1SK is secure. In addition, the secret code stream \(\{x, p, b\}\) is an integer sequence which is related with selected \(u\) feature pixels of plain image, i.e. “L2SK 1” in Figure 2. For a particular cipher image, the attacker can choose specific plain image to obtain the locations of “L2SK 1”, which requires that the attacker can take complete control of encryption system and change the output of encryption algorithm of Step 5. The processing time mainly comes from calculating the locations of \(2u\) pixels of “L2SK 1”, i.e. \(kNM(NM-u)\tau_1\), where \(\tau_1\) represents the encryption time, and \(k=2\) is the number of choosing plaintext. When the speed of image processing is 100Mbps, for an 8-bit gray scale image of size 512×512, the cryptanalysis time is at least 87.16 years. However, the proposed scheme can effectively protect “L2SK 1” with information diffusion methods, and even known “L2SK 1”, “L2SK \(k\)”, \(k>1\), the equivalent secret code stream are still unpredictable, so the aforesaid chosen plaintext attack method is invalid.

5.5. Against Chosen Cipher-text Attack

The aim of chosen cipher text attack is to obtain the secret keys or equivalent secret keys of the decryption system, which is equivalent to obtain the secret keys of encryption scheme, as the proposed scheme is the symmetric secret key encryption scheme, and the secret keys for encryption and decryption are strictly identical. Generally, chosen cipher-text attack is considered much easier to implement than chosen plaintext attack. Here, in chosen cipher-text attack which is similar to chosen plaintext attack, the attacker first selects a cipher image (can be any image), then changes each pixel value of cipher image in turn, after that, by comparing the decrypted images to find whether some pixels values are unchanged, to determine the \(2u\) locations of pixels in “L2SK 1” in Figure 2, which requires the time of \(kNM(NM-u)\tau_2\), where \(\tau_2\) represents the decryption time, and \(k=2\) is the number of changing pixel value.

For some specific cipher images, through the chosen cipher-text decryption processes the attacker can obtain the \(u\) pixels of “L2SK 1”. The processes mainly spend time in positioning
pixels of “L2SK 1”, e.g. for an 8-bit gray scale image of size 512×512, the time is at least 87.16 years with the image processing speed of 100Mbps. However, in the proposed scheme with information diffusion, the attacker cannot decrypt the “L2SK k”, k>1, and the equivalent secret code streams, so the proposed can resist chosen cipher-text attack effectively.

6. Conclusion

In view of the defect about secret code streams independent of plain image in some of currently chaotic encryption systems, this paper proposed two-level secret key image encryption scheme based on piecewise linear map and Logistic map, which includes two levels of secret keys, i.e. L1SK and L2SK. The L1SK is the symmetric secret key shared by both communication pairs, and the L2SK is generated by L1SK and information extracted from plain image, which is deployed as initial values or parameters of chaotic maps for iteration to produce chaotic sequences, which are truncated into integer sequences as secret code streams for encryption. The key space of L1SK can reach 10^{49}, while the key space of L2SK is extremely large. In this paper, when the L1SK is fixed and \( u = 16 \), to encrypt two arbitrarily selected plain images (both of \( L \)-bit and of the same size grayscale images), the probability of the secret code streams for encryption being identical is \( \frac{1}{(2^{2L})^u} \), when \( L = 8 \), i.e. approximately 4.1276e-91, which means that the secret code streams generated by the proposed scheme for two arbitrarily selected different plain images are always different, indicating that in the proposed scheme the secret code streams are strongly related to plain image, thus the proposed scheme can effectively resist against both chosen plaintext attack and chosen cipher-text attack. Meanwhile, the cipher images obtained by the proposed image encryption scheme have characteristics of flat histograms, NPCR and UACI being close to the theoretical value, and fast encryption /decryption speed, and the performance analyses show that the proposed scheme is valid, and can be applied to real communications.

Acknowledgement

This work was fully supported by the Natural Science Foundations of Jiangxi Province (Grant Nos. 20122BAB201036 and 20114BAB211011).

References


