A PLAIN- IMAGE DEPENDENT IMAGE ENCRYPTION SCHEME USING HALF-PIXEL-LEVEL INTERCHANGE PERMUTATION OPERATION

Li Liu, Yucheng Chen and Ruisong Ye

Department of Mathematics, Shantou University
Shantou, Guangdong, 515063, P. R. China

ABSTRACT

In this paper, a chaos-based image encryption scheme with half-pixel-level interchange permutation strategy and plain-image dependence is proposed. The proposed image encryption scheme consists of a confusion process and a diffusion process. In the confusion process, a pixel-swapping operation between higher bit planes and lower bit planes is employed to replace the traditional confusion operation. The half-pixel-level interchange permutation strategy between the higher 4-bit plane part and the lower 4-bit plane part not only improves the conventional permutation efficiency within the plain-image, but also changes all the pixel gray values. The system parameters of generalized Arnold map applied for the permutation operation relies on the plain-image content and consequently can resist chosen-plaintext and known-plaintext attacks effectively. To enhance the security of the proposed image encryption, one multimodal skew tent map is utilized to generate pseudo-random gray value sequence for diffusion operation. Simulations have been carried out thoroughly with comparisons with some other existing image encryption schemes. The experimental results demonstrate that the proposed image encryption scheme is highly secure thanks to its large key space and efficient permutation-diffusion operations.

KEYWORDS

Generalized Arnold map, Interchange permutation, Chaotic system, Multimodal skew tent map, Image encryption

1. INTRODUCTION

The rapid development of network technologies, cloud technologies and smart phone systems make remarkable progress for network-based services. Multimedia processing technologies also make numerous digital images and videos with private and confidential information ubiquitous over the network. Therefore, protection of digital images and videos against illegal copying and distribution becomes urgent challenge than ever before. Many researchers have devoted to studying the security issue of images and videos and the research in image encryption gained new momentum at the last decades. While general data encryption algorithms have been widely applied in various fields, specialized image encryption schemes still undergo studying. A great number of chaos-based image encryption schemes are then investigated intensively to meet the real time need of protection of images transmitted on the Internet and wireless network. On the one hand, traditional symmetrical encryption algorithms, such as International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES) and RSA, are especially designed for text data information, and have been proved not well applied for image encryption due to the weakness of low-level efficiency while encrypting images with some intrinsic features, such as bulky data capacity, strong correlation between adjacent pixels and high redundancy[1]. On the other hand, chaotic system has attracted tremendous interest from researchers thanks to its good features, such as ergodicity, pseudo-randomness and sensitivity to initial conditions and control parameters, which are in line with the basic requirements, like confusion and diffusion, in cryptography [2, 3]. These good chaotic properties make chaotic systems potential for constructing cryptosystems in multimedia field [3-8].

DOI: 10.5121/ijnsa.2017.9405

Most of the existing chaos-based image encryption algorithms employ a permutation-diffusion architecture, in which one encryption round includes several confusion operations and one round diffusion operation. This architecture was initially presented by Fridrich in 1998 [3]. In the permutation stage, two-dimensional chaos systems are usually used to modify each pixel's location, while in the diffusion stage the value of all the pixels is systematically changed controlled by one pseudo-random gray value sequence generated by one chaotic map. As we know, a good encryption scheme should possess some fundamental requirements. For example, it should sensitive enough to cipher keys; the key space should be large enough to resist brute-force attack; the permutation and diffusion processes should possess good statistical properties to frustrate statistical attack, differential attack, known-plaintext attack and chosen-plaintext attack, etc. However, the traditional permutation-diffusion architecture with fixed key streams is blamed for one big flaw. The permutation and diffusion stages will become independent if the plain-image is a homogeneous one with identical pixel gray value. Therefore, such a kind of image encryption schemes can be broken by the following steps: (1) a homogeneous image with identical pixel gray value is applied eliminate the confusion effect; (2) the key streams of the diffusion process is obtained using known-plaintext, chosen-plaintext or chosen-ciphertext attacks; (3) the remaining cipher-image can be regarded as the output of a kind of permutation-only cipher, which has been shown insecure and can be broken by known-plaintext or chosen plaintext attacks[9, 10]. As a matter of fact, image encryption schemes with conventional permutation-diffusion architecture have been analyzed or shown to suffer from security drawbacks [11-15].

To overcome the drawbacks such as small key space and weakly secure permutation-diffusion architecture in the existing chaos-based image encryption schemes, many researchers turn to find improved chaos-based cryptosystems with large key spaces and efficient permutation-diffusion or permutation-substitution mechanisms. Ye proposed an image encryption scheme with an efficient permutation-diffusion mechanism, which shows good performance, including huge key space, efficient resistance against statistical attack, differential attack, known-plaintext as well as chosen-plaintext attack [16]. In both the permutation and diffusion stages, generalized Arnold maps with real number control parameters are applied to generate pseudo-random sequences and therefore enlarge the key space greatly. Meanwhile, a two-way diffusion operation is executed to improve the security of the diffusion function. Patidar et al. [17] proposed a secure and robust chaos-based pseudorandom permutation substitution scheme to encrypt color image. The proposed scheme consists of three processes: preliminary permutation, substitution and main permutation. The proposed image encryption scheme shows strong robustness and great security. The three processes are performed row-by-row and column-by-column instead of pixel-by-pixel to improve the speed of encryption. To obtain excellent key sensitivity and plaintext sensitivity, both preliminary permutation and main permutation are set to be dependent on the plain-image and controlled by the pseudo-random number sequences generated from the chaotic standard map. The substitution process is initialized with the initial vectors generated via the cipher keys and chaotic standard map, and then the pixel gray values of row and column pixels of input 2D matrix are bitwise exclusive OR with the pseudo-random number sequences. Zhou et al. introduced new chaotic systems by integrating the tent, Logistic and sine maps into one single system to produce the pseudo-random sequence [18, 19]. The intertwining Logistic map and reversible cellular automata were applied in an image encryption scheme presented by Wang et al. in [20]. This encryption scheme performs operations at bit level considering higher four bits of each pixel value. Some novel image encryption schemes using bit-level permutation strategy are proposed recently to improve the security issue of chaos-based image encryption schemes. For bit-level permutation, each pixel gray value is divided into 8 bits for 256 gray-scale images. Since each bit of a pixel contains different percentage of the pixel information, the situation of performing confusion at bit-level is quite different from pixel-level case. The bit-level permutation not only relocates the pixel positions, but also alters the pixel gray values [21, 22]. Therefore certain diffusion effect has been introduced in the confusion stage with a bit-level permutation. Thanks to the superior characteristics of bit-level operations and the intrinsic bit features of images, Zhang et al. proposed a novel image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion in [23] .They also applied an expand-and-shrink strategy at bit-level to shuffle the image with reconstructed permuting plane [24]. All the proposed image encryption schemes show good performances compared with the traditional permutation-diffusion structure operating at pixel-level. However, there exists one flaw in all bit-level based image encryption schemes. Although the bit-level confusion operations can change the pixel gray values, they consume much execution time to get the eight bit planes.

In this paper, a plain-image dependent image encryption scheme with half-pixel-level interchange permutation strategy is proposed. In the proposed permutation operation, a pixel-swapping operation between higher 4-bit plane part and lower 4-bit plane part is employed to replace the traditional confusion operation. The plain-image with size $H \times W$ and 256 gray levels is divided into two images with the same size, each of which is of 16 gray levels. They consist of the 1-4 and 5-8 bit planes respectively. The half-pixel-level swapping strategy between the higher 4-bit plane part and the lower 4-bit plane part has two effects compare with the traditional permutation operation. It not only improves the conventional permutation efficiency within the plain-image, but also changes all the pixel gray values of the entire image. In the proposed image encryption scheme, the parameters of generalized Arnold map applied for the permutation operation are designed to be dependent on the plain-image content and consequently can resist chosen-plaintext and known-plaintext attacks effectively. The plain-image content dependent permutation makes the proposed image encryption scheme more sensitive with respect to plain-image, so the cryptosystem is truly one-time pad. To achieve more security of the proposed image encryption, one multimodal skew tent map is applied to generate pseudo-random gray value sequence for diffusion operation. Multimodal skew tent map has shown good chaotic features; it is generalized from unimodal skew tent map. Unimodal skew tent map is widely applied to generate pseudo-random sequences in chaos-based image encryption schemes [16, 25]. We apply multimodal skew tent map to enlarge the cipher key space as it has more choices of control parameters. In the diffusion phase, a multimodal skew tent map is utilized to generate a pseudo-random gray value sequence, which is used to modify the pixel gray values sequentially. The yielded pseudo-random gray value sequence shows good sensitivity to the control parameters and initial conditions of multimodal skew tent map, and therefore the proposed image encryption scheme can resist statistical attack, differential attack, known-plaintext attack as well as chosen-plaintext attack. The security and performance analysis of the proposed image encryption scheme are carried out thoroughly. All the experimental results show that the proposed image encryption scheme is highly secure and demonstrates excellent performance. Especially, we compare the performance with some other existing image encryption schemes. The comparison also demonstrates that the proposed image encryption scheme is superior. For example, the correlation between adjacent pixels is significantly reduced compared with Wang's scheme [26], Chen's schemes [27, 28]. Moreover, we introduce co-occurrence histogram to reflect the encryption effect of the cipher-image. The information entropy correlated with co-occurrence is also introduced to measure uniformity level of the two-dimensional histogram. The experimental results on co-occurrence histogram and its related entropy are compared with Zhang's scheme proposed in [29]. As for differential attack analysis, the NPCR and UACI performance reach a satisfactory level; NPCR and UACI are very close to their expectation values by one round of encryption.

The rest of the paper is organized as follows. In Section 2, multimodal skew tent map with M tents is constructed and its chaotic properties are simply analyzed. Section 3 proposes a novel image encryption scheme composed of one half-pixel-level interchange permutation process and one diffusion process based on multimodal skew tent map. The decryption process is also stated in this section. The security and performance of the proposed image encryption scheme are evaluated via detailed analysis and experiments in Section 4. Section 5 draws some conclusions.

2. THE MULTIMODAL SKEW TENT MAP

The unimodal skew tent map $T_0:[0,1]\to[0,1]$ is given by

$$T_0(x)=\begin{cases} x/a, & \text{if } x\in[0,a], \\ (1-x)/(1-a), & \text{if } x\in(a,1], \end{cases} \tag{1}$$

where $a\in(0,1)$ is the control parameter and $x\in[0,1]$ is the state of the map. It is a noninvertible map of the unit interval onto itself. For any $a\in(0,1)$, the unimodal skew tent map (1) has Lyapunov exponent $-a\ln a-(1-a)\ln(1-a)$, which is larger than 0, implying that the map is chaotic. There exist some good dynamical features in the skew tent map. It has been verified that the probability density function $\rho_0(x)$ of the skew tent map is the same as the regular tent map [30],

$$\rho_0(x)=\begin{cases} 1, & \text{if } x\in(0,1), \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

We generalize the unimodal skew tent map (1) to multimodal skew tent map $T:[0,1]\to[0,1]$ defined by

$$T(x)=\begin{cases} (x-a_{2i})/(a_{2i+1}-a_{2i}), & \text{if } x\in[a_{2i},a_{2i+1}], \\ (a_{2i+2}-x)/(a_{2i+2}-a_{2i+1}), & \text{if } x\in(a_{2i+1},a_{2i+2}], i=0,\cdots,M-1, \end{cases} \tag{3}$$

where $0=a_0<a_1<\cdots<a_{2M-1}<a_{2M}=1$, and M is referred to the number of the map. See Fig. 1 for the case of $M=3$, $a=[0, 0.16, 0.3, 0.51, 0.68, 0.78, 1.0]$.

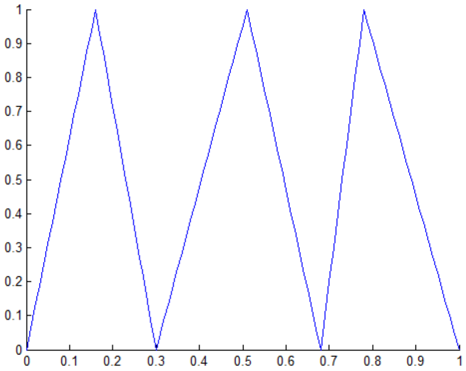
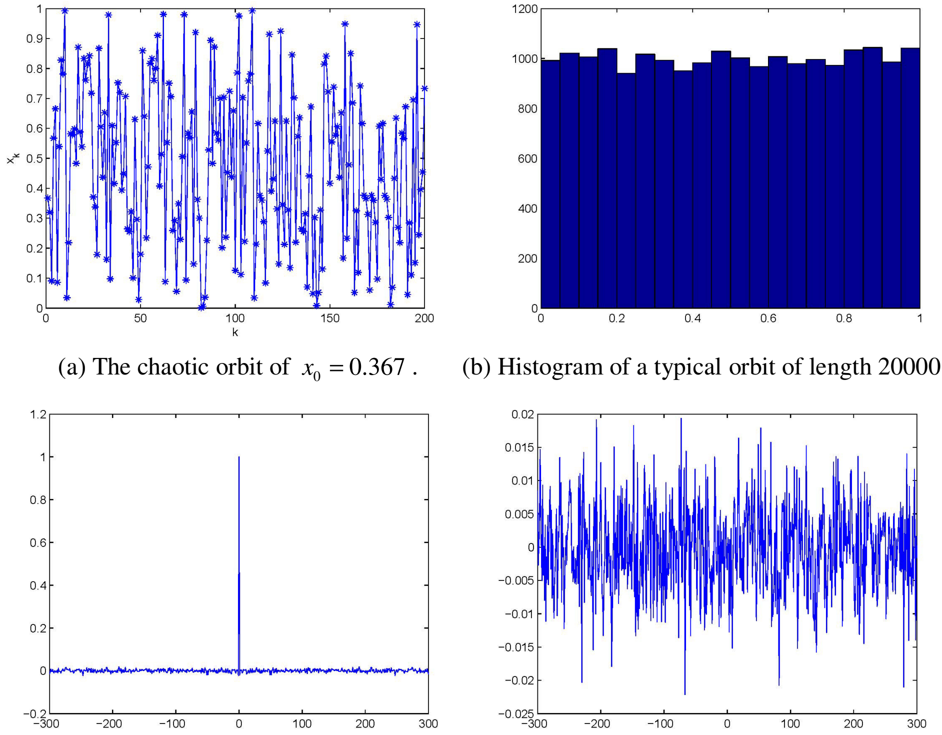


Fig. 1. The diagram of a multimodal skew tent map.

A typical orbit of $x_0=0.367$ generated by the dynamical system (3) is $\{x_k=T^k(x_0), k=0,1,\cdots\}$, shown in Fig. 2(a) for $a=[0\ 0.16\ 0.3\ 0.51\ 0.68\ 0.78\ 1.0]$, $M=3$. Its waveform is quite irregular, implying the system's chaotic nature. To illustrate the distribution of the orbit points $\{x_k: k=0,1,\cdots,20000\}$, we depict the histogram of Fig. 2(b). It can be seen that the points of the orbit spread more or less evenly over the unit interval. As a matter of fact, multimodal skew tent map possesses desirable auto-correlation and cross-correlation features as well. The trajectory is applied to calculate the correlation coefficients, which are shown in Figs. 2(c)-(d) respectively. The cross-correlation coefficients are calculated by the orbits of $x_0=0.367$ and $y_0=0.368$. The control parameter $a_1,\cdots,a_{2M-1}$ and the initial condition x_0 can be regarded as cipher keys if the multimodal skew tent map is applied to design image encryption schemes.



(a) The chaotic orbit of $x_0 = 0.367$. (b) Histogram of a typical orbit of length 20000.

(c) The auto-correlation. (d)The cross-correlation

Fig. 2. Orbits derived from the considered multimodal skew tent map with $a = [0\ 0.16\ 0.3\ 0.51\ 0.68\ 0.78\ 1.0]$.

The probability density $\rho(x)$ for multimodal skew tent map on [0, 1] is the same as that of unimodal one [31]. This fact has been illustrated by Fig. 2(b). The existence and unique value of the Lyapunov exponent also follows from the following theorem. It has been shown that for the multimodal skew tent map (3) with the constant probability density $\rho(x) \equiv 1$, the Lyapunov exponent of (3) is (see [31] for more details)

$$\lambda = -p_1 \ln p_1 - p_2 \ln p_2 - \cdots - p_{2M-1} \ln p_{2M-1} - p_{2M} \ln p_{2M} . \tag{4}$$

λ is always larger than zero, implying the dynamical system is always chaotic. For $M = 3, a = [0\ 0.16\ 0.3\ 0.51\ 0.68\ 0.78\ 1.0]$, we obtain

$$p_1 = 0.16, p_2 = 0.14, p_3 = 0.21, p_4 = 0.17, p_5 = 0.1, p_6 = 0.22 ,$$

so $\lambda = 1.7608$. It is usually larger than the Lyapunov exponent for the unimodal skew tent map (1). As a matter of fact, for the unimodal skew tent map (1), the largest Lyapunov exponent $\ln 2 = 0.6931$ occurs at the extreme case $a = 0.5$. It implies that the multimodal skew tent map (3) is in a stronger sense chaotic, and therefore can perform better data mixing, which makes it a better choice for designing encryption schemes than the unimodal skew tent map. We will show more details in the following sections on the proposed image encryption scheme based on the chaotic multimodal skew tent map.

3. The Process of Image Encryption Scheme

In this section, the proposed image encryption scheme is proposed. We read a 8-bit (256 gray-level) plain-image P with size $H \times W$. In this paper, we restrict the plain-images with equal height H and width W , that is, $H = W$. Regarding the plain-images with unequal height H and width W , we can just enlarge the image to be one with equal height and width and then encrypt it by the proposed image encryption scheme. The plain image is expressed by a two-dimensional matrix sized $H \times W$ whose elements belong to the integers between 0 and 255. The flowchart of the encryption process is depicted in Fig. 3. The image encryption scheme consists of two processes: permutation and diffusion.

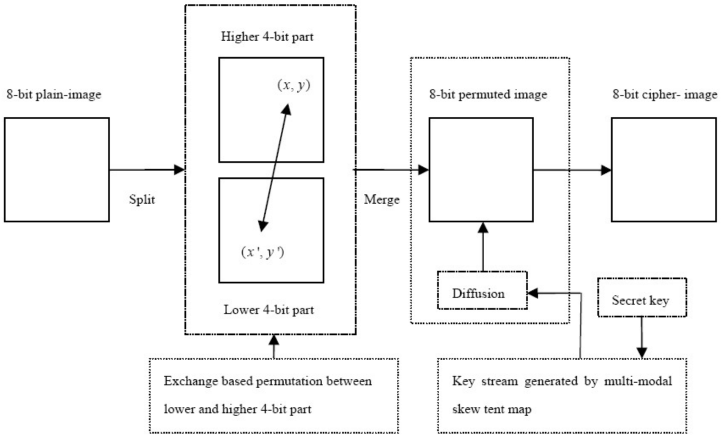


Fig. 3. Flowchart of the encryption process.

3.1. Permutation Process

In the permutation process, the plain-image P is decomposed into two parts: the higher 4-bit plane part I_2 and the lower 4-bit plane part I_1. I_1, I_2 can be regarded as 16 gray-level images consisting of the 1-4 and 5-8 bit planes of the plain-image respectively. The pixels between I_1 and I_2 are exchanged by generalized Arnold map defined as Eq. (5).

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & 1+pq \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod H, \tag{5}$$

where $p, q \in 0,1,2,...,H-1$, p and q are control system parameters for the generalized Arnold map; function "$z \bmod H$" represents the remainder after division; (x, y) refers to the original position of the higher 4-bit part while (x', y') represents the pseudo-random position of the lower 4-bit part governed by the generalized Arnold map. The detail permutation process is depicted as follows:

Step 1. The control system parameters p, q in generalized Arnold map are set to be related to the plain-image so as to enhance the security of the encryption algorithm. They are calculated by

$$p = (\sum_{i=1}^{H} \sum_{j=1}^{W} I_1(i, j)) \bmod H, \quad q = (\sum_{i=1}^{H} \sum_{j=1}^{W} I_2(i, j)) \bmod H. \tag{6}$$

A minor change in the plain-image will cause the change of p, q. It is known that generalized Arnold map is strongly sensitive to system parameters p, q. As a result, the corresponding cipher-images of two plain-images with minor difference will be dramatically different.

Step 2. The generalized Arnold map is applied to confuse the pixel positions. For each position of the higher 4-bit plane part, a corresponding random position (x', y') in the lower 4-bit plane part is calculated by the generalized Arnold map Eq. (5) with coefficients p, q. Exchange the pixel value locating at (x, y) of the higher 4-bit part with the pixel value locating at (x', y') of the lower 4-bit part. The exchanging positions and gray value exchange operation are defined by

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & 1+pq \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod H, I_2(x,y) \leftrightarrow I_1(x',y'), x, y = 0,1,\cdots,H-1.$$

Step 3. Integrate the two exchanged images together to be one permutated image B :

$$B(i,j) = I_1(i,j) + I_2(i,j) \times 16, i, j = 0,1,\cdots,H-1.$$

3.2. Diffusion Process

Though the permutation process has changed the pixel positions of the plain-image as well as the pixel gray values, it has been pointed out that the permutation-only encryption is not secure [10]. In order to enhance the security, some diffusion function should be designed to assist the permutation process. In the diffusion phase, the values of all the pixels are systematically modified. An ideal secure encryption scheme should have a good diffusion mechanism. The diffusion process can significantly change the statistical properties of the plain-image by spreading the influence of each bit of the plain-image all over the cipher-image. The diffusion process will enhance the resistance to statistical attack and differential attack effectively, in which the histogram of the cipher-image is fairly uniform and is significantly different from that of the plain-image. The opponent cannot find any useful clues between the plain-image and the cipher-image and so cannot break the cryptosystem even when they spend a lot of time and effort. We applied the multimodal skew tent map to produce pseudo-random gray value sequence in the diffusion process. The diffusion process is outlined as follows.

Step 1. Set the values of M , the control system parameters $a_i (i = 1,...,2M-1)$, and the initial condition x_0 .

Step 2. Iterate the multimodal skew tent map Eq. (3) to get the truncated orbit of x_0 , say $x_n, n = 0,1,...,W \times H + 99$ and reject the first 100 points to overcome the transient process of the chaotic map and save the remainder $H \times W$ points. For the sake of simplicity, we still write them as $x(i), i = 1,...,W \times H$.

Step 3. The key stream element $k(n)$ is calculated by Eq. (7), in which function "$floor(x)$" means the value nearest integers less than or equal to x , $x(n)$ represents the current state of a chaotic map and is calculated in Step 2, and L is the gray level of the plain-image, respectively.

$$k(n) = floor(x(n) \times 10^{14}) \bmod L. \tag{7}$$

Step 4. Pixel values are modified sequentially according to Eq. (8), where $B(n)$, $k(n)$, $c(n)$, $c(n-1)$ are the gray values of the current operated pixel in the permuted image B , key stream element, output cipher-pixel, previous cipher-pixel, respectively.

$$c(n) = B(n) \oplus ((k(n) + c(n-1)) \bmod \ L). \tag{8}$$

Step 5. Repeat the above steps for all the pixels. An initial value seed $c(-1)$ is required for the first pixel.

The complete diffusion process is composed of Step 1 to Step 5. The permutation process and the diffusion process form the image encryption scheme.

3.3. The Decryption Process

The decryption procedure is the reverse process of the encryption and the flowchart of the decryption process is shown in Fig. 4. The entire decryption procedure is depicted as follows.

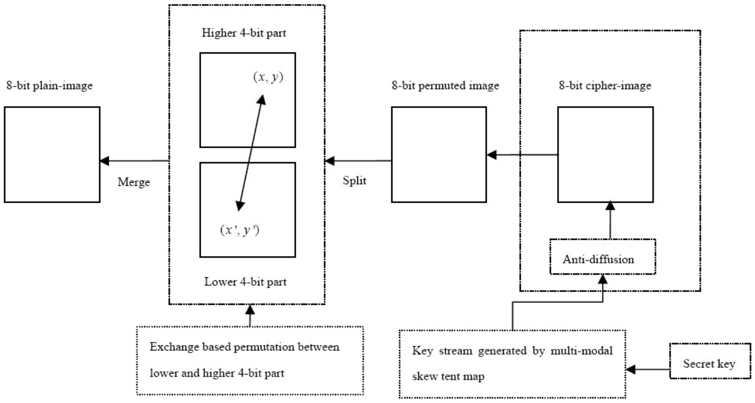


Fig. 4. Flowchart of the decryption process.

Step 1. Set the values of M , the control parameters $a_i(i=1,...,2M-1)$, and the initial condition x_0 .

Step 2. Iterate the multimodal skew tent map Eq. (3) to get the truncated orbit of x_0 , say $x(n), n=1,...,W\times H$ as the same as those in the encryption process.

Step 3. The key stream element $k(n)$ is calculated by Eq. (7) as the same as that in the encryption process.

Step 4. The decrypted image B is obtained according to Eq. (9), where $B(n), k(n), c(n)$, $c(n-1)$ are the output decipher-pixel, key stream element, the current cipher-pixel, previous cipher-pixel, respectively.

$$B(n)=c(n)\oplus(k(n)+c(n-1)modL). \qquad (9)$$

Step 5. Repeat the above steps for all the pixels. An initial value $c(-1)$ is required for the first pixel as well.

Step 6. Split the yielded image B into the lower 4-bit plane part I_1 and the higher 4-bit plane part I_2 . The control parameters p,q for the generalized Arnold cat map are obtained by Eq. (10).

$$p=(\sum_{i=1}^{H}\sum_{j=1}^{W}(I_2(i,j)) \mod H),\quad q=(\sum_{i=1}^{H}\sum_{j=1}^{W}(I_1(i,j)) \mod H). \qquad (10)$$

Step 7. For each position of the higher 4-bit plane part, a corresponding random position (x', y') in the lower 4-bit plane part is calculated by the Arnold map Eq. (5) with coefficients p,q . Exchange the gray values of pixel pairs between I_1 and I_2 . The exchange positions and gray value exchange operation are defined by

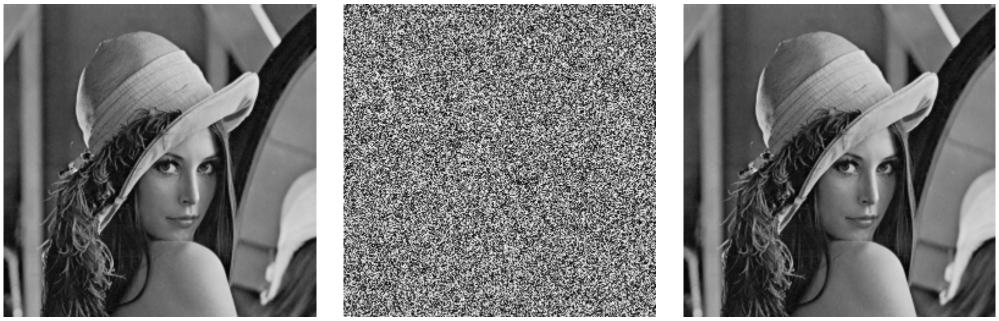
$$\begin{pmatrix} x' \\ y' \end{pmatrix}=\begin{pmatrix} 1 & p \\ q & 1+pq \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \mod H, I_1(x,y)\leftrightarrow I_2(x',y'), x,y=0,1,\cdots,H-1.$$

Step 8. Integrate the two exchanged images together to get the plain-image P :

$$P(i,j)=I_1(i,j)+I_2(i,j)\times 16, i,j=0,1,\cdots,H-1.$$

4. SECURITY AND PERFORMANCE ANALYSIS

According to the basic principle of cryptology [2], a good encryption scheme requires sensitivity to cipher keys, i.e., the cipher-text should have close correlation with the keys. An ideal encryption scheme should have a large key space to make brute-force attack infeasible; it should also well resist various kinds of attacks like statistical attack, differential attack, etc. In this section, some security analyses have been performed on the proposed image encryption scheme, including the most important ones like key space analysis, statistical analysis, and differential analysis. All the analyses show that the proposed image encryption scheme is highly secure. We use MATLAB 7.0 to run the encryption and decryption process in computer with 1.70 GHz CPU, 4 GB memory and Microsoft Windows 8 operation system. All the results in this article are obtained under this circumstance. The plain-image is Lena.bmp of size 256×256, the keys are $c(-1)=87$, $x_0=0.367$, $a=[\ 0\ , 0.16\ ,\ 0.3\ , 0.51\ , 0.68\ , 0.78\ , 1.0\ ]$. Fig. 5 shows the results of encryption and decryption.



(a) plain-image Lena. (b) cipher-image of Lena. (c) decrypted image.

Fig. 5. Encryption and decryption results.

4.1. Statistical Analysis

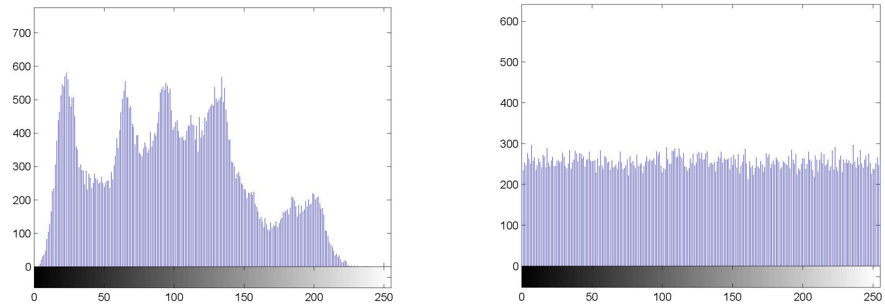
It is well known that the statistical property of a cipher-image is enormously vital and an ideal image algorithm should be robust against any statistic attacks. Histogram and correlation of adjacent pixels are two important indicators of statistical analysis.

Histogram. Histogram analysis visually reveals the distribution information of pixel gray values. A good cipher-image should have a uniform and completely different histogram in comparison with that of the plain-image. Histograms of plain-image and cipher-image are plotted, through which we can intuitively see the number of pixels of each intensity value. A good image algorithm should make the histogram of cipher-image as uniform as possible. The histograms of plain-image Lena and its cipher-image are shown in Fig.6. Fig. 6(a) and Fig. 6(b) are Lena image and its histogram respectively; Fig. 6(c) and Fig. 6(d) are the cipher-image of Lena and its histogram respectively. We can observe that the histogram of the cipher-image obtained by the proposed image encryption scheme is fairly uniform and is significantly different from that of the plain-image. The proposed image encryption scheme does not provide any useful information for the opponents to perform any effective statistical analysis attack on the cipher-image.

Correlation of adjacent pixels. Generally speaking, as for an ordinary nature image with definite meaningful visual content, each pixel is highly correlated with its adjacent pixels either in horizontal, vertical or diagonal direction. An ideal encryption technique should produce cipher-images with less correlation between adjacent pixels. To quantify and compare the horizontal, vertical and diagonal correlations of adjacent pixels in the plain and cipher images, we calculate the correlation coefficients for all the pairs of horizontally, vertically and diagonally adjacent pixels respectively. The results are shown in Fig.7. The correlation coefficients r_{xy} for two groups of adjacent pixels' intensity values are calculated using Eq. (11) [32] :

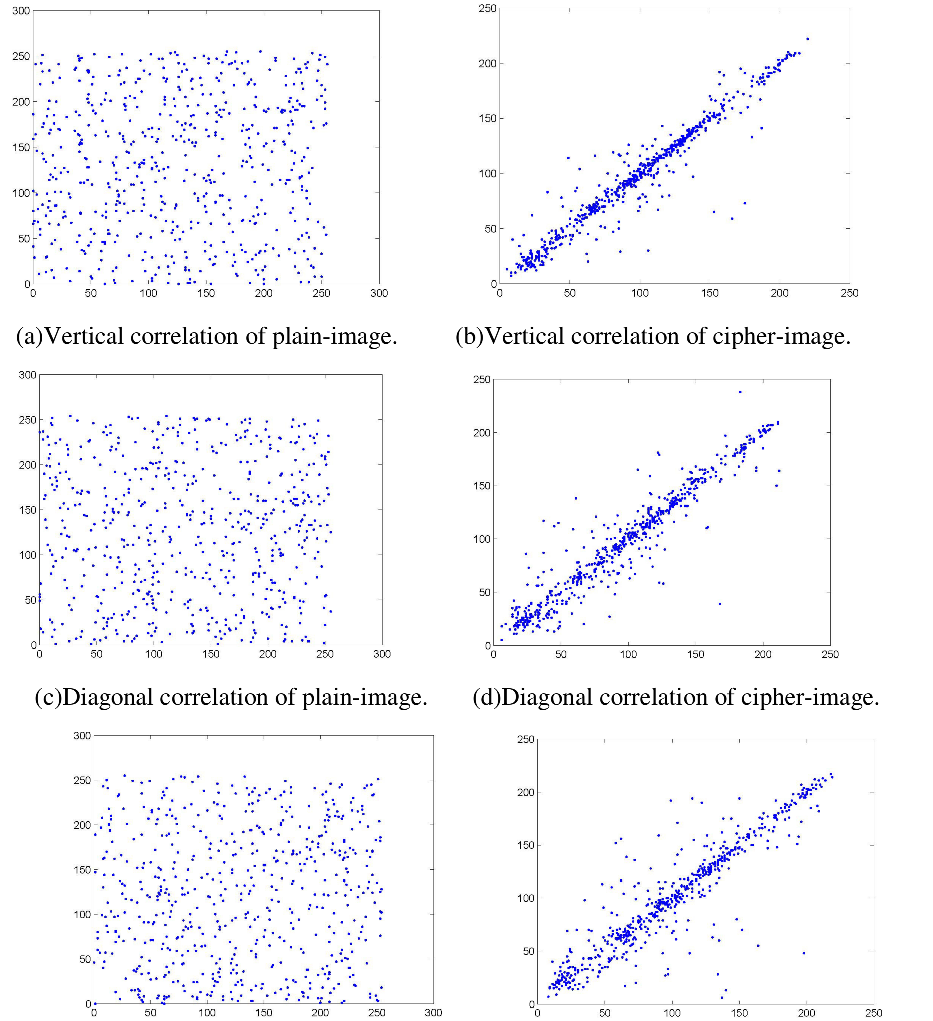
$$cov(x,y)=E\{(x-E(x))(y-E(y))\}\ ,\quad r_{xy}=\frac{cov(x,y)}{\sqrt{D(x)D(y)}}\ , \tag{11}$$

where x and y are the gray values of the two selected groups of adjacent pixels from the image, $E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$ and $D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2$.



(a)The histogram of plain-image. (b) The histogram of cipher-image.

Fig. 6. Histograms of plain-image Lena and its cipher-image.



(a)Vertical correlation of plain-image. (b)Vertical correlation of cipher-image.

(c)Diagonal correlation of plain-image. (d)Diagonal correlation of cipher-image.

(e)Horizontal correlation of plain-image. (f)Horizontal correlation of cipher-image.

Fig. 7. Correlations of adjacent pixels.

The correlation distributions of two adjacent pixels in the plain-image Lena and that in its corresponding cipher-image are show in Fig. 7. From Fig.7 and Table 1, We can conclude that the correlation between adjacent pixels is greatly reduced in the cipher-image. There are no detectable correlations between the plain-images and their corresponding cipher-images. We also perform the comparison of dajacent pixel correlation with Wang's algorithm [26], Chen's algorithm [27] and Chen's algorithm [28]. In our proposed scheme, the correlation coefficients are significantly reduced than other algorithms, we can intuitively see the changes from Table 2.

Table 1. Correlation coefficients of adjacent pixels in the plain and cipher images.

Figure	Plain image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9401	0.9695	0.9180	0.0003	-0.0074	-0.0043
couple	0.9371	0.8926	0.8557	0.0006	-0.0017	-0.0023
aerial	0.9050	0.8602	0.8213	-0.0116	-0.0007	0.0038
liftingbody	0.9764	0.9755	0.9566	0.0025	0.0012	0.0007
pout	0.9784	0.9842	0.9716	-0.0026	-0.0029	0.0012
cameraman	0.9335	0.9592	0.9087	0.0004	0.0034	-0.0027

Table 2. Correlation coefficients of adjacent pixels in plain-image Lena by different algorithms.

Algorithm	Cipher image		
	Horizontal	Vertical	Diagonal
Proposed algorithm	-0.0003	-0.0043	-0.0074
Wang's algorithm [26]	0.0074	0.0020	-0.0070
Chen's algorithm [27]	-0.0038	0.0092	0.0033
Chen's algorithm [28]	0.0660	-0.0341	-0.0278

Furthermore, we introduce a new statistic index to reflect the effect of the cipher-image, which is called the co-occurrence histogram [33]. The co-occurrence histogram in the horizontal direction is defined by Eq. (12).

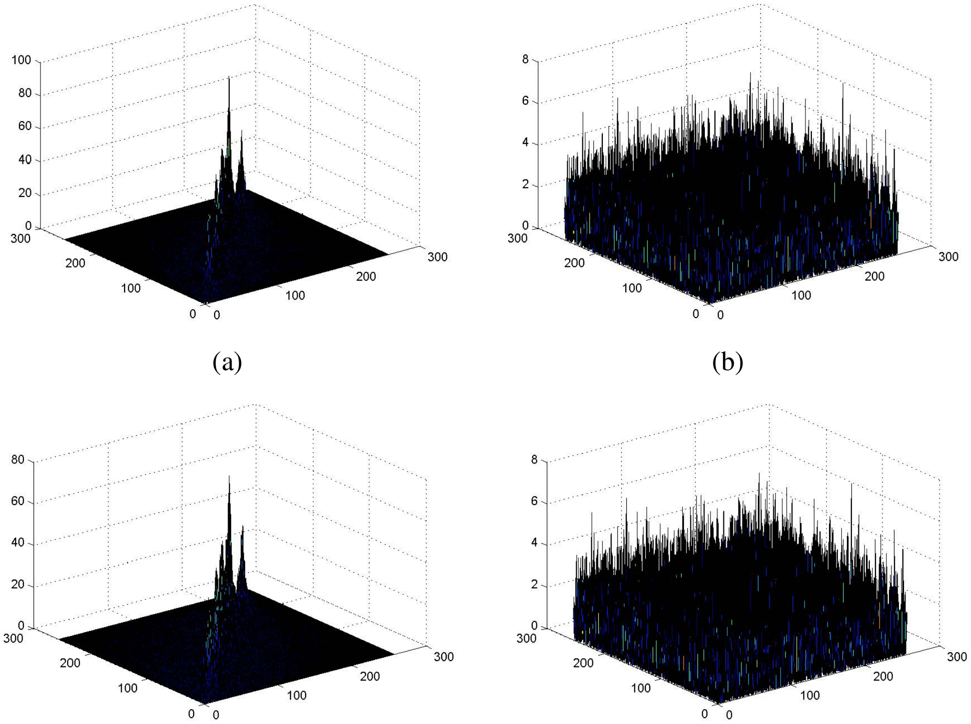
$$co_1(i,j)=\sum_{x=1}^{n-1}\sum_{y=1}^{n}\delta(g(x,y)-i)\delta(g(x+1,y)-j), i,j=0,1,...,255. \tag{12}$$

The co-occurrence histogram in the vertical direction is defined by Eq. (13).

$$co_2(i,j)=\sum_{x=1}^{n}\sum_{y=1}^{n-1}\delta(g(x,y)-i)\delta(g(x,y+1)-j), i,j=0,1,...,255. \tag{13}$$

where $g(x,y)$ is the pixel value at the location (x,y). If $x=y$, then $\delta(x,y)=1$, otherwise, $\delta(x,y)=0$. The detail co-occurrence histograms of the plain-image and cipher-image are shown in Fig.8. Besides, the information entropy Eq. (14) correlated with co-occurrence is introduced to measure uniformity level of the two-dimension histogram. The distribution of the pixel space will be more uniform when the value of information entropy is bigger. Compared with Wang's algorithm [26], Chen's algorithm [28] and Zhang's algorithm [29], our proposed algorithm obtains better results in Table 3 and Table 4. We employ four 256 gray scales standard test images with the size of 256×256. From the results we can see that, when ciphering the same image, our proposed algorithm obtains better values than other algorithms. Especially, when encrypting image pout.tif, the vertical information entropy in Table 3 is 11.1762, however, the corresponding value by Zhang's algorithm in Table 4 is just 9.2713.

$$H(co_l)=-\sum_{i=0}^{255}\sum_{j=0}^{255}\frac{co_l(i,j)}{n(n-1)}\ln(\frac{co_l(i,j)}{n(n-1)}), l=1,2. \tag{14}$$



(a) (b)

(c) (d)

Fig. 8. Co-occurrence histograms: (a), (c) are vertical and horizontal co-occurrence histograms of plain-image; (b), (d) are vertical and horizontal co-occurrence histograms of cipher-image.

Table 3. Co-occurrence histogram entropies of our proposed algorithm.

Image	Plain image		Cipher image	
	Horizontal	Vertical	Horizontal	Vertical
Lena	8.8162	8.4882	10.5191	10.5121
aerial	9.0160	9.1406	10.5185	10.5145
pout	6.5881	6.4524	11.1694	11.1762
cameraman	7.8065	7.8449	10.5151	10.5145

Table 4. Co-occurrence histogram entropy of other algorithms.

Image	Wang's algorithm [26]		Chen's algorithm[28]		Wang's algorithm [26]	
	Horizontal	Vertical	Horizontal	Vertical	Horizontal	Vertical
Lena	10.5149	10.5193	10.5025	10.5021	10.5146	10.4821
aerial	10.5152	10.5136	10.5158	10.5199	10.5143	10.4966
pout	10.5137	10.5153	10.3349	10.2815	11.1182	9.2713
cameraman	10.5163	10.5149	10.4833	10.4524	10.5157	10.4247

4.2. Information entropy analysis

In [2], entropy was proposed by Shannon so as to quantitatively measure the randomness and the unpredictability of an information source. The mathematical formula for the entropy of a message source is defined in Eq. (15), where s is the source, N is the number of bits to represent the symbols, and $P(s_i)$ is the probability of the symbol s_i.

$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i)\log_2 P(s_i). \qquad (15)$$

For a purely random source emitting of 2^N symbols, the entropy is N. Therefore, the upper-bound entropy of an effective cipher-image with 256 gray levels is 8. Such expected value will be achieved when the cipher-image is uniformly distributed, i.e., the image has complete flat histogram.

The results of the information entropy analysis for four 256 gray scales standard test images with size 256×256 are listed in Table 5. The results illustrate that the entropies of the cipher-images are very close to the upper-bound value 8. As indicated by the calculated values, the information entropy of our proposed algorithm is bigger than that of Chen's algorithm [28]. Nevertheless, all of them are very close to the ideal value 8. We can therefore come to the conclusion that there is little possibility to eavesdrop and our encryption scheme has high robustness against entropy attack.

Table 5. Entropies of plain image and its cipher image.

Image	Plain image	Cipher image	Chen's algorithm [28]
Lena	7.5682788	7.9972907	7.9923
aerial	7.3118072	7.9970804	7.9963
pout	5.7598895	7.9968558	7.9573
cameraman	7.0097163	7.9970644	7.9903

4.3. Differential Attack Analysis

Number of pixel change rate (NPCR) and unified average changing intensity(UACI) are usually used to measure the sensitivity of the cryptosystem to a slight modification of the plain-image. In an ideal situation, a slight modification of the plain-image will lead to a completely different cipher-image which would indicate its resistance to differential attack. Otherwise, it would have been possible to obtain the correlation between the plain-image and the cipher-image by a series of attacks of this nature. In order to calculate NPCR and UACI, suppose two plain images I_1 and I_2 with difference in only one pixel, and their cipher images are denoted as C_1 and C_2. Then we create a matrix D, when $C_1(i,j) = C_2(i,j)$, $D(i,j)=0$; otherwise, $D(i,j)=1$. NPCR and UACI are calculated by Eq. (16).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W\times H}\times100\%,\ \ UACI = \frac{1}{W\times H}(\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255})\times100\%\ , \qquad (16)$$

where *W*, *H* are the width and height of the images.

To test the influence of one pixel change on the whole cipher-image, we randomly select 100 pixels from the processing image and then alter each pixel's gray value by one bit each time. Then, we calculate the corresponding 100 NPCR and UACI values and take the average of them. The average NPCR and UACI values are shown in Table 6. It shows clearly that the algorithm reaches very good NPCR performance when encrypted just one round of encryption. The UACI performance is similar. From the results we know that the proposed image encryption scheme is extremely sensitive to plaintext, which is very important to resist differential attack. Table 7 gives the comparison of performance of UACI and NPCR when encrypting the image of Lena applying one round of encryption. The expectation value of NPCR and UACI are 99.6094% and 33.4636%. Table 7 indicates that the performance of the proposed algorithm is better than Wang's algorithm [26], Chen's algorithm [27] and Chen's algorithm [28] when encrypting images one round. Therefore, one round of encryption by our proposed scheme is secure enough to resist differential attack.

Table 6. NPCR-UACI performance of the Lena and cameraman images.

Image	Average NPCR	Average UACI
Lena	99.638366699	33.500366211
Cameraman	99.606323242	33.573919558

Table 7. NPCR-UACI performance of different algorithms.

Algorithm	NPCR	UACI
Proposed algorithm	99.6058	33.4488
Wang's algorithm[26]	99.6017	33.4343
Chen's algorithm[27]	99.5723	33.7661
Chen's algorithm[28]	98.0536	32.6984

4.4. Key Space Analysis

The key space is the total number of different keys that can be used in a cryptosystem. In [34], it is suggested that the key space of a chaos-based image cryptosystem should be larger than 2^{100}. As to the proposed scheme, no other chaotic system is introduced in the permutation phase, and the key space wholly depends on the diffusion key, denoted as $Key-P$. The initial value x_0, $c(-1)$ and control parameter $a_i(i=1,...,2M-1)$ of multimodal skew tent map serve as the primary key of the proposed cryptosystem. According to the IEEE floating-point standard [35], the computational precision of the 64-bit double-precision number is about 10^{-16}. Due to the fact that x_0 can be any one among those 10^{16} possible values within (0,1), and so as a_i, $(i=1,...,2M-1)$. Regarding L gray-level image, the valid values of $c(-1)$ is L. For the case $M=3$, we can take an example, x_0=0.367, a=[0, 0.16, 0.3, 0.51, 0.68, 0.78, 1.0], $c(-1)$=87, then the key space of the proposed cryptosystem is

$$Key-P=10^{16}\times10^{16}\times10^{16}\times10^{16}\times10^{16}\times10^{16}\times256\approx2^{327}.$$

which satisfies the security requirement suggested in [34], and is large enough to resist brute-force attack.

4. 5. Key Sensitivity Analysis

Key sensitivity of an image cryptosystem can be observed in two aspects: (i) completely different cipher images should be produced when slightly different keys are applied to encrypt the same plain-image; (ii) the cipher-image cannot be correctly decrypted even tiny mismatch existing in decryption keys. With regard to the symmetrical characteristic of the secret key, we typically test the sensitivity of $c(-1)$, x_0, u so as to avoid redundancy.

To evaluate the key sensitivity in the first case, the encryption is first performed with master cipher keys $c(-1)$=87, x_0=0.367, u=[0, 0.16, 0.3, 0.51, 0.68, 0.78, 1.0]. A valid and slight modification is introduced to one of the cipher keys with others remaining unchanged and the encryption process is executed once again. The corresponding cipher-images and the difference images are shown in Fig. 9. The differences between the corresponding cipher-images are numerically computed, as listed in Table 8. The results obviously demonstrate that the cipher-images exhibit no similarity one another and there is no significant correlation that could be observed from the differential images.

Table 8. Key sensitivity

Figure	Cipher keys					Difference
	$c(-1)$	x_0	$u(2)$	$u(3)$	$u(5)$	
Fig. 9(b)	87	0.367	0.16	0.3	0.68	--
Fig. 9(c)	88	0.367	0.16	0.3	0.68	1.0
Fig. 9(e)	87	$0.367{+}10^{-16}$	0.16	0.3	0.68	0.9957
Fig. 9(g)	87	0.367	$0.16+10^{-16}$	0.3	0.68	0.9960
Fig. 9(i)	87	0.367	0.16	$0.3+10^{-16}$	0.68	0.9966
Fig. 9(k)	87	0.367	0.16	0.3	$0.68+10^{-16}$	0.9960

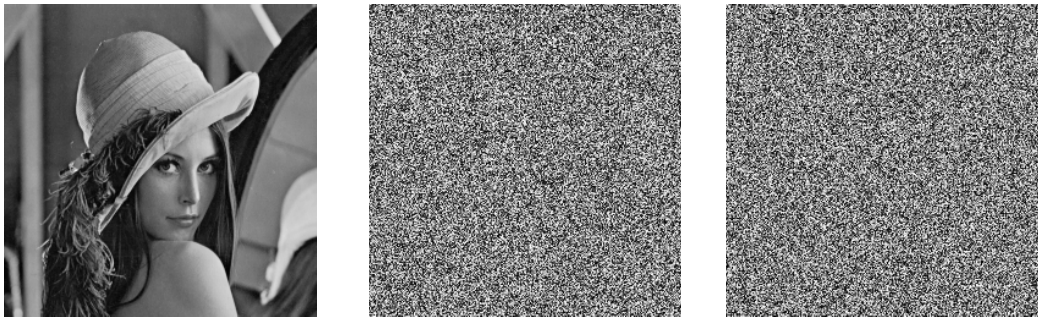
The key sensitivity of the second case is tested by implementing decryption with slightly different keys. The decrypted images are shown in Fig. 10. The differences of the incorrect decipher-images to the plain image are 1.00, 0.995712, 0.996002, 0.996613, and 0.996017, respectively. As pointed out by the previous achievements in [27], our proposed scheme achieving the satisfactory security level, the difference even reaches to 1.00 between two decipher when only a slight modification is introduced.

In this paper, to verify the sensitivity of key parameter K, the original plain-image $I=(I(i,j))_{H\times W}$ is encrypted with $K=p$, $K=p-\Delta$ and $K=p+\Delta$ respectively while keeping the other key parameters unchanged. The corresponding encrypted images are denoted by J_1, J_2, J_3 respectively. The sensitivity coefficient to the parameter K is denoted by the following formula:

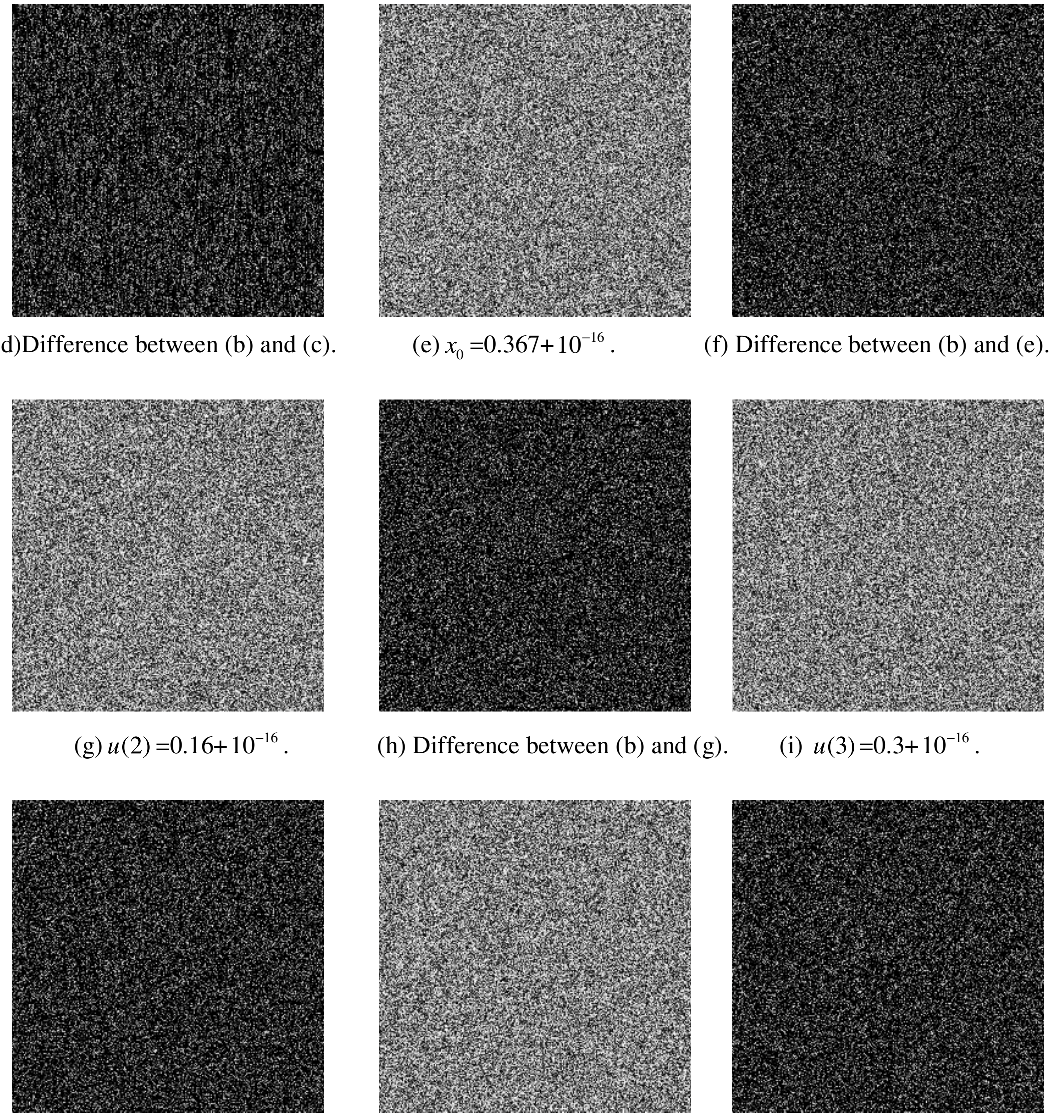
$$P_s(K)=\frac{1}{2\times W\times H}\sum_{i=1}^{H}\sum_{j=1}^{W}[N_s(J_1(i,j),J_2(i,j))+N_s(J_1(i,j),J_3(i,j))]\times 100\%,$$

$$N_s(x,y)=\begin{cases}1, x\neq y,\\ 0, x=y.\end{cases}$$

where Δ is the perturbing value. $P_s(K)$ implies the sensitivity to the perturbation of parameter K. The greater $P_s(K)$, the more sensitive for the parameter K. Table 9 shows the results of the sensitivity test where the initial key values are set to be the following: $c(-1)$=87, x_0=0.367, u=[0, 0.16, 0.3, 0.51, 0.68, 0.78, 1.0].



(a) plain-image Lena. (b) master key. (c) $c(-1)$=88.



(d)Difference between (b) and (c).

(e) x_0 =0.367+10^{-16}.

(f) Difference between (b) and (e).

(g) $u(2)$ =0.16+10^{-16}.

(h) Difference between (b) and (g).

(i) $u(3)$ =0.3+10^{-16}.

(j)Difference between (b) and (i).

(k) $u(5)$ =0.68 +10^{-16}.

(l) Difference between (b) and (k).

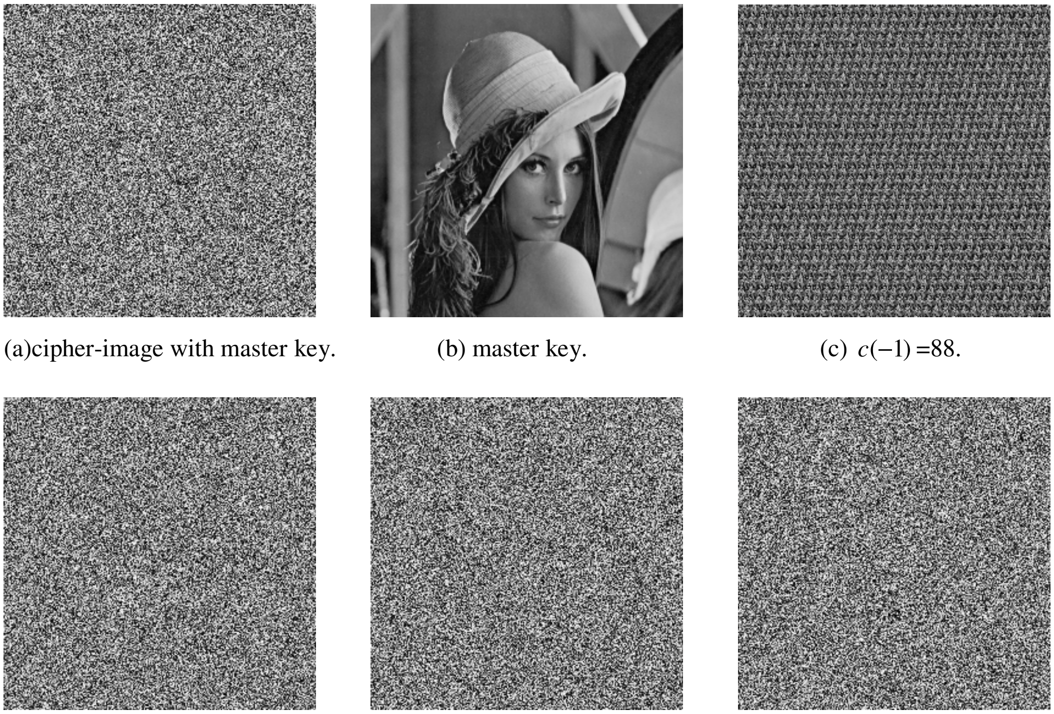
Fig. 9. Key sensitivity test I: master key is set to be $c(-1)$ =87, x_0 =0.367, u =[0, 0.16, 0.3, 0.51, 0.68, 0.78, 1.0]. (b),(c),(e),(g),(i),(k) are the cipher-images using different cipher keys with minor perturbing.

4.6. Speed Performance

Wong et al. have pointed out that the consumption time of an image cryptosystem is mainly resulted from the real number arithmetic operation in the encryption process [36,37]. To evaluate the execution time of the proposed scheme and those of the comparable algorithms, the standard test image Lena.bmp is subjected to one round of encryption. The execution times can be found in Table 10. Table 10 illustrates that the total execution time of the proposed scheme is much shorter than those of the comparable algorithms. Especially, in Chen's algorithm [27], the authors divided the whole image into four parts based on dynamic random, the time-consuming is inevitable in both the confusion phase and the diffusion phase.

Table 9. Results regarding the sensitivity to cipher keys.

K	u(2)	u(3)	u(4)	u(5)	u(6)	x_0
$P_s(K)\,(\%)$	99.6048	99.6246	99.5918	99.6429	99.6048	99.5880



(a)cipher-image with master key. (b) master key. (c) $c(-1)$ =88.

(d) x_0 =0.367+10^{-16} . (e) $u(2)$ =0.16+10^{-16} . (f) $u(4)$ =0.51+10^{-16} .

Fig. 10. Key sensitivity test II: (b)-(f) are the corresponding decrypted images using different cipher keys with minor perturbing.

Table 10. Speed performance.

Algorithm	Confusion time (s)	Diffusion time (s)	Total time (s)
Proposed algorithm	0.053	0.323	0.376
Wang's algorithm[26]	0.156	0.469	0.625
Chen's algorithm[27]	0.658	1.652	2.310
Chen's algorithm[28]	0.559	1.536	2.095

5. CONCLUSION

An efficient image encryption scheme based on a half-pixel-level interchange between the higher 4-bit plane part and the lower 4-bit plane part is proposed in the paper. The proposed encryption scheme can shuffle the plain-image efficiently in the permutation process. An effective diffusion process is also designed to alter the gray values of the whole image pixels. Security and performance analyses including co-occurrence histogram, key space analysis, key sensitivity analysis, statistical analysis, information entropy analysis, differential attack analysis and speed rate are performed numerically and visually. All the experimental results show that the proposed encryption scheme is highly secure thanks to its large key space, its high sensitivity to the cipher keys and plain-images. The proposed encryption scheme is easy to manipulate and can be applied to color images as well. All these satisfactory properties make the proposed scheme a potential candidate for encryption of multimedia data such as images, audios and even videos.

REFERENCES

[1] D. R. Stinson, Cryptography: Theory and Practice, CRC Press, Boca Raton, 1995.

[2] C. E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J, 28(1949): 656-715.

[3] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos, 8(1998): 1259-1284.

[4] Z.-H. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm, Physics Letters A, 346(2005): 153-157.

[5] S. Lian, J. Sun, Z. Wang, A block cipher based on a suitable use of the chaotic standard map, Chaos, Solitons and Fractals, 26 (2005): 117-129.

[6] Y. Wang, K. W. Wong, X. F. Liao, T. Xiang, G. R. Chen, A chaos-based image encryption algorithm with variable control parameters, Chaos, Solitons and Fractals, 41:4(2009): 1773-1783.

[7] W. Zhang, Kwok-wo. Wong, H. Yu, Z. Zhu, An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion, Commun. Nonlinear Sci. Numer. Simul., 18:8(2013): 2066-2080.

[8] Y. Xi, X. Zhang, R. Ye, Color image encryption based on multiple chaotic systems, International Journal of Network Security & Its Applications, 8:5(2016): 39-50.

[9] C. Q. Li, S. J. Li, G. R. Chen, G. Chen, L. Hu, Cryptanalysis of a new signal security system for multimedia data transmission. EURASIP J. Appl. Signal Process., 8(2005): 1277-1288.

[10] S. J. Li, C. Q. Li, G. R. Chen, N. G. Bourbakis, K. T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plain-image attacks. Signal Process. Image Commun., 23(2009): 212-223.

[11] D. Xiao, X. Liao, P. Wei, Analysis and improvement of a chaos-based image encryption algorithm, Chaos, Solitons and Fractals, 40(2009): 2191-2199.

[12] E. Solak, C. Cokal, O. T. Yildiz, and T. Biyikoglu, Cryptanalysis of fridrich's chaotic image encryption, International Journal of Bifurcation and Chaos, 20:5 (2010): 1405-1413.

[13] J. M. Liu, Q. Qu, Cryptanalysis of a substitution-diffusion based on cipher usingchaotic standard and logistic map, in: Third International Symposium on Information Processing, 2010, pp.67-69.

[14] R. Rhouma, E. Solak, S. Belghith, Cryptanalysis of a new substitution-diffusion based image cipher, Commun. Nonlinear Sci. Numer. Simulat., 15 (2010): 1887-1892.

[15] X. Wang, G. He, Cryptanalysis on a novel image encryption method based on total shuffling scheme, Optics Commun., 284 (2011): 5804-5807.

[16] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Optics Commun., 284(2011): 5290-5298.

[17] Vinod Patidar, N. K. Pareek. G. Purohit, K. K. Sud, A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption. Optics Commun., 284(2011): 4331-4339.

[18] Y. Zhou, L. Bao, C.L. Philip Chen, Image encryption using a new parametric switching chaotic system, Signal Processing, 93(2013): 3039-3052.

[19] Y. Zhou, L. Bao, C.L. Philip Chen, A new 1D chaotic system for image encryption, Signal Processing, 97(2014): 172-182.

[20] X. Wang, D. Luan, A novel image encryption algorithm using chaos and reversible cellular automata, Commun Nonlinear Sci. Numer. Simulat., 18(2013): 3075-3085.

[21] Z.-L. Zhu, W. Zhang, K.-W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, Information Sciences, 181(2011): 1171-1186.

[22] L. Teng, X. Wang, A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive, Optics Communications, 285(2012): 4048-4054.

[23] W. Zhang, K.-W. Wong, H. Yu, Z.-L. Zhu, An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion. Optics Commun., 285 (2012): 2343- 2354.

[24] W. Zhang, K.-W. Wong, H. Yu, Z.-L. Zhu, A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Commum. Nonliear Sci. Numer. Simulat., 18 (2013): 584-600.

[25] G. J. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, Optics Commun., 284(2011): 2775-2780

[26] X. Wang, L. Liu, Y. Zhang, A novel chaotic block image encryption algorithm based on dynamic random growth technique, Optics and Lasers in Engineering, 66(2015): 10-18.

[27] J. Chen, Z. Zhu, C. Fu, H. Yu, L. Zhang, An efficient image encryption scheme using gray code based permutation approach, Optics and Lasers in Engineering,67(2015): 191-204.

[28] J. Chen, Z. Zhu, C. Fu, H. Yu, Y. Zhang, Reusing the permutation matrix by dynamically for efficient image cryptographic algorithm, Signal Processing, 111(2015): 294-307.

[29] Y. Q. Zhang, X. Y. Wang, A new image encryption algorithm based on non-adjacent coupled map lattices , Applied Soft Computing, 26(2015): 10-20.

[30] M. Hasler and Y. L. Maistrenko, An introduction to the synchronization of chaotic systems: coupled skew tent map, IEEE Transactions on Circuits and Systems, 44(1997): 856-866.

[31] R. Ye, W. Guo, A Chaos-based Image Encryption Scheme Using Multimodal Skew Tent Maps, Journal of Emerging Trends in Computing and Information Sciences, 4:10(2013): 800-810.

[32] Y. Wang, K.W. Wong, X.F. Liao, G.R. Chen, A new chaos-based fast image encryption algorithm, Appl. Soft. Comput.,11(2011): 514-522.

[33] M. Wu, An improved discrete Arnold transform and its application in image scrambling and encryption, Acta Phys. Sin., 63:9(2014): 090504.

[34] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystem, International Journal of Bifurcation and Chaos, 16(2006): 2129-2151.

[35] IEEE Computer Society, IEEE standard for binary floating-point arithmetic, ANSI/IEEE std. 1985:754-1985.

[36] K. Wong, B. Kwok, W. Law, A fast image encryption scheme based on chaotic standard map, Physics Letters A, 372:15(2008), 2645-2652.

[37] K. Wong, B. Kwok, C. Yuen, An efficient diffusion approach for chaos-based image encryption, Chaos, Solitons and Fractals, 41:5(2009): 2652-2663.

Authors

Li Liu, master degree candidate at department of mathematics in Shantou University.

Yucheng Chen, master degree candidate at department of mathematics in Shantou University.

Ruisong Ye, born in 1968 and received the B.S. degree in Computational Mathematics in 1990 from Shanghai University of Science and Technology, Shanghai, China and the Ph. D. degree in Computational Mathematics in 1995 from Shanghai University, Shanghai, China. He is a professor at Department of Mathematics in Shantou University, Shantou, Guangdong, China since 2003. His research interest includes bifurcation theory and its numerical computation, fractal geometry and its application in computer science, chaotic dynamical system and its application in computer science, specifically the applications of fractal chaotic dynamical systems in information security, such as, digital image encryption, digital image hiding, digital image watermarking, digital image sharing.