Asymmetric image encryption algorithm based on a new three-dimensional improved logistic chaotic map

Guo-Dong Ye(叶国栋)[1,2,†], Hui-Shan Wu(吴惠山)[1], Xiao-Ling Huang(黄小玲)[1], and Syh-Yuan Tan[3]

[1] *Faculty of Mathematics and Computer Science, Guangdong Ocean University, Zhanjiang* 524088, *China*
[2] *Guangdong Provincial Engineering and Technology Research Center of Far Sea Fisheries Management and Fishing of South China Sea, Zhanjiang* 524088, *China*
[3] *School of Computing, Newcastle University, Newcastle* NE4 5TG, *UK*

(Received 29 March 2022; revised manuscript received 24 May 2022; accepted manuscript online 2 July 2022)

Based on some analyses of existing chaotic image encryption frameworks and a new designed three-dimensional improved logistic chaotic map (3D-ILM), an asymmetric image encryption algorithm using public-key Rivest–Shamir–Adleman (RSA) is presented in this paper. In the first stage, a new 3D-ILM is proposed to enhance the chaotic behavior considering analysis of time sequence, Lyapunov exponent, and Shannon entropy. In the second stage, combined with the public key RSA algorithm, a new key acquisition mathematical model (MKA) is constructed to obtain the initial keys for the 3D-ILM. Consequently, the key stream can be produced depending on the plain image for a higher security. Moreover, a novel process model (NPM) for the input of the 3D-ILM is built, which is built to improve the distribution uniformity of the chaotic sequence. In the third stage, to encrypt the plain image, a pre-process by exclusive OR (XOR) operation with a random matrix is applied. Then, the pre-processed image is performed by a permutation for rows, a downward modulo function for adjacent pixels, a permutation for columns, a forward direction XOR addition-modulo diffusion, and a backward direction XOR addition-modulo diffusion to achieve the final cipher image. Moreover, experiments show that the the proposed algorithm has a better performance. Especially, the number of pixels change rate (NPCR) is close to ideal case 99.6094%, with the unified average changing intensity (UACI) close to 33.4634%, and the information entropy (IE) close to 8.

Keywords: three-dimensional improved logistic chaotic map (3D-ILM), Rivest–Shamir–Adleman (RSA) algorithm, image encryption, confusion, entropy

PACS: 05.45.Gg, 05.45.Ac, 07.05.Pj **DOI:** 10.1088/1674-1056/ac7dbb

1. Introduction

In the society of the information age and the big data age, multimedia information, such as video, audio, image, digital magazine, etc., has gradually become an indispensable part in people's daily life. Among them, digital image, as one of the important multimedia information, has more intuitive performance than other multimedia such as text and audio, and also has better property of small capacity and easy sharing compared with video. Therefore, image communication is widely used in various application scenarios. However, in recent years, due to illegal attacks or unsatisfactory confidentiality schemes, some image information has been leaked, which has caused a great impact. Therefore, the security protection of images has attracted extensive attention from experts and scholars from all over the world.[1] In the process of communication or storage, encryption for the image data is a direct and effective way to solve the problem of image security.[2,3] However, compared with text content, digital image has some different characteristics like high redundancy, strong correlation and large amount of data. Therefore, the encryption and protection method of image data deserve further study. The nonlinear chaotic system not only has strong sensitivity to the initial value, but also has the characteristics of pseudo-randomness and long-term unpredictability, so it is suitable for digital images permutation and diffusion. Therefore, many image encryption schemes[4–12] based on the nonlinear chaotic map (systems) have been proposed. For example, by using the dual logistic chaotic map, Pan *et al.*[4] constructed a new encryption algorithm to promise the image security, which encrypts image by exclusive OR (XOR) and permutation. However, the chaotic property of logistic chaotic map is not ideal. In order to reduce the defect of chaotic map without complex dynamic performance, Ref. [5] designed a new two-dimensional hyper-chaotic map using one-dimensional chaotic map, employed the structure of permutation–diffusion for all pixels, so as to achieve the effect of encrypting the image. However, the chaotic map in two-dimension still suffers small key space to resist the violent attack when the system parameters are determined. In order to resist brute force attacks effectively and enhance the dynamic performance of chaos, Ye *et al.*[7] presented an image encryption algorithm based on the chaotic quantum map. They generated a random keystream from the quantum map, and then used a different keystream to permute pixels from different directions. Finally, the cipher image could be got through the corresponding diffusion operation. In order to reach a larger key space, an im-

[†]Corresponding author. E-mail: guodongye@hotmail.com

© 2023 Chinese Physical Society and IOP Publishing Ltd

age encryption algorithm using 5D hyperchaotic system and Logistic map in parallel was presented in Ref. [9]. The performance of the generated pseudo-random sequence is better, and the relationship to the adjacent pixels for each pixel is established in the encryption process, so it has strong plaintext sensitivity. However, due to the complex structure and complicated calculation of the high-dimensional chaotic system, the encryption process takes a long time. For an image of size 512×512, the encryption time takes about 5 s, which is hard to meet the real-time communication over the network. To solve it, Ref. [10] suggested a new parallel processing architecture, which divides the whole image data into partitions, and then uses multiple identical chaotic ciphers that run independently at the same time to process each image block.

Image encryption algorithms mentioned above are all in spatial domain. Furthermore, frequency domain transform based encryption schemes[13–17] has also been studied recently. For example, Ding *et al.*[14] presented a multiple chaotic systems based image encryption algorithm together with discrete wavelet transform (DWT), in which the plain image is first transformed by DWT operation, and permuted by low-dimensional chaotic system, then followed by diffusion with high-dimensional chaotic system. In addition, the biological DNA coding technology has the characteristic of the combination rule diversification, as well as has good performance such as large storage capacity and low power consumption. As a result, DNA coding was widely employed in the image encryption algorithms.[18,19] In Ref. [20], Wang *et al.* designed a chaotic image encryption scheme which combines block permutation and DNA encoding. The scheme uses chaotic sequences for inter-block and intra-block permutation, and then performs image diffusion through different DNA encoding rules to obtain cipher images. In addition, optical technology is favored by many experts and scholars because of its high transmission speed, large storage capacity, and high parallelism. Thus, many optical image encryption algorithms[21–23] have been presented. Although the use of optical technology can effectively resist illegal attacks, the use of optical technology to encrypt images is prone to noise and requires higher equipment, resulting in poor practicability.

The symmetric image encryption algorithm has the characteristics of high efficiency, easy implementation and simple operation. However, the defect is the difficulty of the key management and key distribution. In response to such problems, many researchers have introduced public key cryptography based image encryption algorithms.[24–26] In Ref. [24], a novel image encryption algorithm using Rivest–Shamir–Adleman (RSA) was suggested under asymmetric structure, in which keys used are designed and related to the plain image. So, it achieves the effect of one-time pad for each image, solves the management and distribution of key effectively, and consequently improves the security. By virtue of the excellent characteristics of chaotic system and the advantages of public-key algorithm, a new three-dimensional improved logistic chaotic map (3D-ILM) is proposed in this paper, which not only ensures the large key space, but also improves the complex dynamic performance of the chaotic map, and makes the chaotic sequence distributed widely. In addition, the mathematical model of key acquisition is constructed to increase the dependence of the key on the plain image, so as to strongly enhance the security of the proposed encryption algorithm. The main contributions for this paper are: (i) A new 3D-ILM is designed, which has stronger chaotic behavior. (ii) A new mathematical model of key acquisition (MKA) is constructed, which increases the dependence of the keystream on the plain image. (iii) A novel process mechanism (NPM) for the input of the 3D-ILM is built, which improves the distribution uniformity of chaotic sequence. (iv) An asymmetric image encryption is presented using the 3D-ILM and RSA, which enhances the security for image communication.

The rest parts of this paper are organized as: Section 2 gives some preparatory knowledge such as the public-key cryptography RSA and the new 3D-ILM. Section 3 describes the initial key acquisition model MKA, the process model NPM, and the complete image encryption process. In Section 4, the decryption process is explained. Then, Section 5 displays the experiments together with security analysis. At the end, Section 6 summarizes the whole paper.

2. Preliminary knowledge

2.1. Public algorithm RSA

RSA algorithm is a classical public-key cryptographic algorithm, with security dependent on difficulty of factoring large integers. At present, public-key RSA algorithm mainly consists of the following parts. (i) Key generation. Choose prime numbers p and q, then compute n by $n = p \times q$ and Euler function is $\varphi(n) = (p-1) \times (q-1)$. Select a public key e, and then compute the corresponding private key d by $d = e^{-1} \bmod \varphi(n)$, where $\gcd(\varphi(n), e) = 1$. (ii) Encryption process. For a plain text message m, compute the cipher text message by $c \equiv m^e \bmod n$. (iii) Decryption process. Decrypt the secret message c by $m \equiv c^d \bmod n$.

In this paper, RSA algorithm is only employed to encrypt the plain messages extracted from the plain image, with the cipher messages open. The main aim is to enhance the security of the algorithm with key stream related to the plain image. Of course, other public algorithms can also be used.

2.2. The new 3D-ILM

On one hand, compared with low-dimensional chaotic map, the 3D chaotic map has larger key space and can resist

violent attack more safely. On the other hand, compared with the hyper chaotic system, 3D chaotic map can also show good chaotic behavior with small computation and simple structure for the output chaotic sequence. A three-dimentional logistic chaotic map (3D-LM) proposed in Ref. [27] is as follows:

$$\begin{aligned} x_{i+1} &= r_1 x_i(1-x_i) + r_2 y_i^2 x_i + r_3 z_i^3, \\ y_{i+1} &= r_1 y_i(1-y_i) + r_2 z_i^2 y_i + r_3 x_i^3, \\ z_{i+1} &= r_1 z_i(1-z_i) + r_2 x_i^2 z_i + r_3 y_i^3, \end{aligned} \tag{1}$$

where r_1, r_2, and r_3 are the parameters of the system, when $3.53 < r_1 < 3.81$, $0 < r_2 < 0.022$, and $0 < r_3 < 0.015$, the chaotic map exhibits chaotic behavior. If $r_1 = 3.7028$, $r_2 = 0.0105$, and $r_3 = 0.0126$ are set respectively with the initial values $x_0 = 0.1268$, $y_0 = 0.2586$, and $z_0 = 0.5456$, the time series of each sequence are depicted in Fig. 1.

So, as can be seen from the time series above, the values of x, y, and z sequences generated by the 3D-LM are all distributed between [0.2,0.9], but not distributed in the whole [0, 1], and are centrally distributed between [0.7, 0.9]. In order to effectively solve this defect, a new 3D improved logistic chaotic map (3D-ILM) is designed as follows:

$$\begin{aligned} x_{i+1} &= r_1 x_i(1-x_i) + r_2 y_i^2 x_i + r_3 z_i^3 + 0.01\cos(x_i), \\ y_{i+1} &= r_1 y_i(1-y_i) + r_2 z_i^2 y_i + r_3 x_i^3 + 0.01\cos(y_i), \\ z_{i+1} &= r_1 z_i(1-z_i) + r_2 x_i^2 z_i + r_3 y_i^3 + 0.01\cos(z_i). \end{aligned} \tag{2}$$

Especially, when solving the 3D-ILM, a new process NPM for the input of the 3D-ILM is built for each iteration as follows:

$$\begin{aligned} x_i &= x_i \times 10^2 - \mathrm{floor}(x_i \times 10^2), \\ x_{i+1} &= r_1 x_i(1-x_i) + r_2 y_i^2 x_i + r_3 z_i^3 + 0.01\cos(x_i), \\ y_i &= y_i \times 10^2 - \mathrm{floor}(y_i \times 10^2), \\ y_{i+1} &= r_1 y_i(1-y_i) + r_2 z_i^2 y_i + r_3 x_i^3 + 0.01\cos(y_i), \\ z_i &= z_i \times 10^2 - \mathrm{floor}(z_i \times 10^2), \\ z_{i+1} &= r_1 z_i(1-z_i) + r_2 x_i^2 z_i + r_3 y_i^3 + 0.01\cos(z_i), \end{aligned} \tag{3}$$

where $3.53 < r_1 < 3.81$, $0 < r_2 < 0.022$, and $0 < r_3 < 0.015$, the 3D-ILM will exhibit better chaotic behavior. Set parameters $r_1 = 3.7028$, $r_2 = 0.0105$, and $r_3 = 0.0126$ with initial values $x_0 = 0.1268$, $y_0 = 0.2586$, and $z_0 = 0.5456$, the time series of 3D-ILM are shown in Fig. 2.

By comparing Figs. 1 and 2, the outputs of the new 3D-ILM are more uniformly distributed between [0, 1]. Therefore, the new 3D-ILM can show better ergodicity.

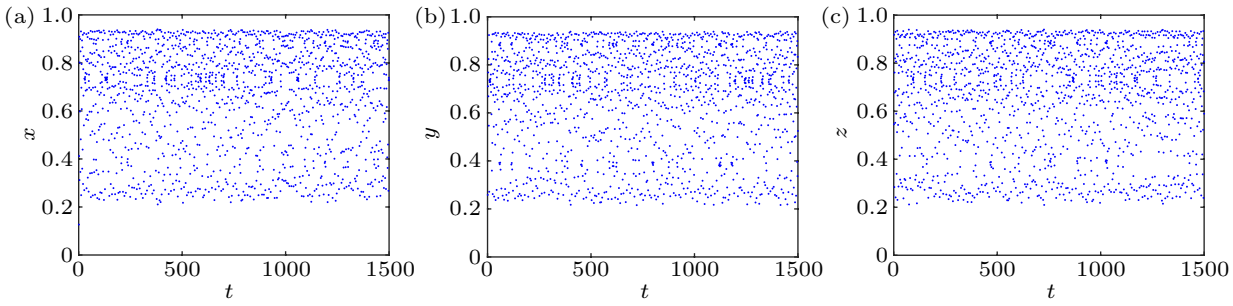


Fig. 1. Time series of the 3D-LM in (a) x direction, (b) y direction, and (c) z direction.

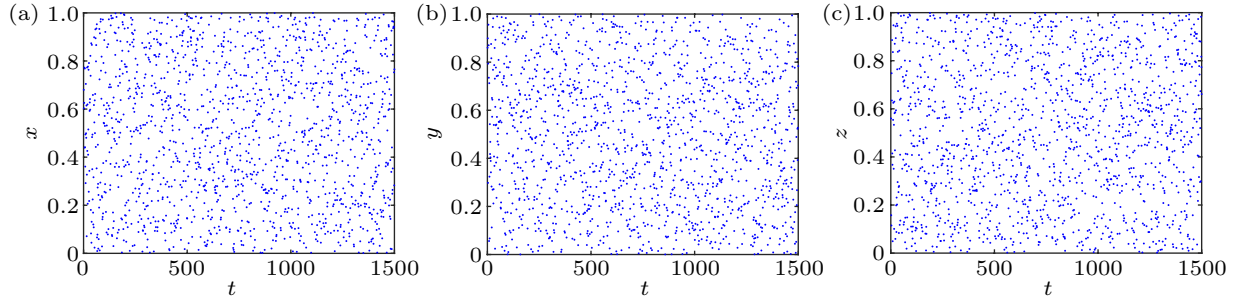


Fig. 2. Time series of the new 3D-ILM in (a) x direction, (b) y direction, and (c) z direction.

2.3. Performance of the new 3D-ILM

(i) Lyapunov exponent Lyapunov exponent (LE), which describes the numerical characteristics of the average exponential divergence of adjacent orbits in phase space, is usually used to judge the chaotic degree for a given system. Set parameters $r_2 = 0.0105$, $r_3 = 0.0126$, and $r_1 \in (3.53, 3.8)$, the Lyapunov exponent spectrum for 3D-LM and the new 3D-ILM is depicted in Fig. 3 by the parameter r_1.

Therefore, it is obvious that the Lyapunov exponent spectrum is larger for the new 3D-ILM than that of 3D-LM, which shows that the new 3D-ILM always in a chaotic state, and exhibits more complex chaotic behavior.

(ii) Shannon entropy Shannon entropy (SE) is often used

to describe the chaotic degree of time sequences generated by nonlinear system.[28] For a chaotic map, if the value of Shannon entropy is higher, the pseudo-randomness of the sequence generated is higher. On the contrary, it means that the sequence is more ordered. Shannon entropy of the 3D-LM and the new 3D-ILM is calculated respectively with the same fixed parameters r_2, r_3 and the control parameter $r_1 \in (3.53, 3.8)$, as shown in Fig. 4.

So, it can be easily found that the Shannon entropy of the new 3D-ILM is larger than that of the 3D-LM in the entire interval, and the fluctuation range is smaller, indicating that the sequences generated by the new 3D-ILM exhibit more stable and more random performance. Therefore, from the analyses of time series, Lyapunov exponent, and Shannon entropy, the new 3D-ILM can display more complex dynamic performance and better randomness.

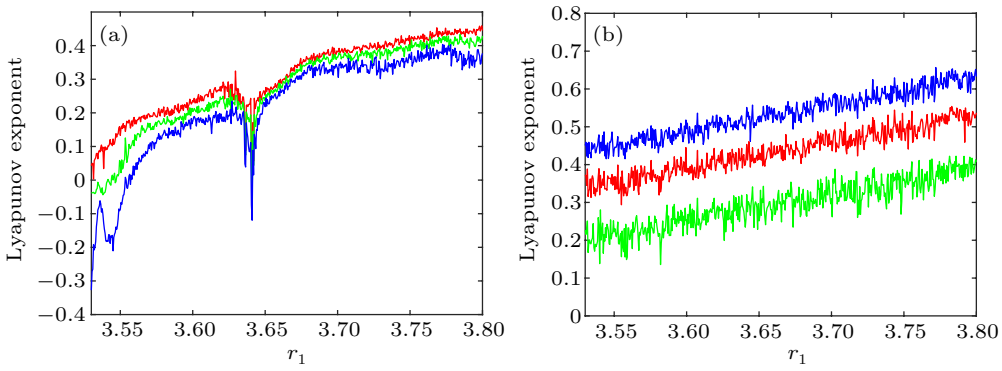


Fig. 3. Lyapunov exponent spectrum of (a) 3D-LM and (b) new 3D-ILM.

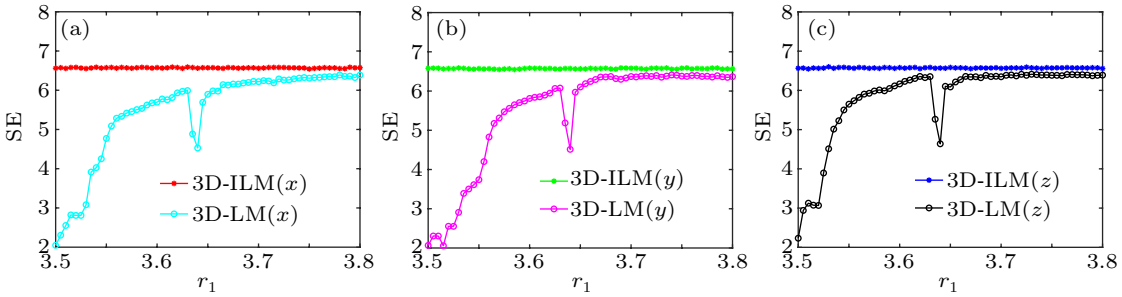


Fig. 4. Shannon entropy comparisons: (a) x sequence, (b) y sequence, and (c) z sequence.

Table 1. NIST SP800-22 test results.

Statistical test	P value			
	X	Y	Z	Result
The frequency (monobit) test	0.3311	0.9172	0.2510	pass
Frequency test within a block	0.6772	0.9666	0.1914	pass
The runs test	0.1530	0.7189	0.7969	pass
Tests for the longest run of ones in a block	0.1146	0.7886	0.9183	pass
The binary matrix rank test	0.0793	0.2920	0.3189	pass
The discrete Fourier transform (spectral) test	0.3683	0.5617	0.3840	pass
The non-overlapping template matching test	0.3450	0.9220	0.1897	pass
The overlapping template matching test	0.7087	0.2538	0.5865	pass
Maurer's "universal statistical" test	0.2307	0.0309	0.1574	pass
The serial test	0.1309	0.2251	0.1453	pass
The approximate entropy test	0.2426	0.0316	0.0374	pass
Cusums-forward	0.4296	0.9908	1	pass
Cusums-reverse	0.2148	1	1	pass
The random excursions test	0.4794	0.1453	0.6972	pass
The random excursions variant test	0.2311	0.5114	0.6850	pass

(iii) NIST SP800-22 test of randomness To further demonstrate the good property of the new 3D-ILM in terms of pseudo-randomness, independence and uniform distribution. Table 1 presents the NIST SP800-22 test results of the new 3D-ILM. That is to say, besides of the analyses of time series, Lyapunov exponent, and Shannon entropy, NIST SP800-22 test results also prove the generated sequences passing the randomness test, demonstrating that the new 3D-ILM can be used as a pseudorandom number generator with better chaotic behavior.

3. The proposed image encryption algorithm

3.1. Key acquisition and keystream generation

Different from traditional way to randomly select keys, to enhance the dependence of the key on the plain image with a high sensitivity to the plain image, a new key acquisition MKA is proposed as seen in Algorithm 1. Suppose that the plain image P with size $M \times N$. Produce a random number μ belonged to [0, 1] and a random matrix $\boldsymbol{Q}$ with elements in [0, 255]. Then, three plain messages m_1, m_2, m_3 are calculated by P and $\boldsymbol{Q}$. Consequently, by using RSA algorithm, three cipher

messages c_1, c_2, c_3, and $c\mu$ are obtained according to m_1, m_2, m_3, and μ. After constructing sin function together with modulo operation, the initial keys x_0, y_0, z_0 in the range of [0,1] can be obtained. Then, all x_0, y_0, z_0 are substituted into the 3D-ILM with some iterations to get the three keystreams x, y, z, which can be seen detailly in Algorithm 1.

Algorithm 1: Key acquisition MKA

Input: Plain image P, public key e, and n.

Output: Initial keys x_0, y_0, z_0.

(i) Read the plain image and get the size, i.e., $[M,N] = \text{size}(P)$.

(ii) Randomly generate random numbers μ and matrix $\boldsymbol{Q}$.

(iii) Extract the plain messages m_1, m_2, m_3 by

$$m_1 = \left\lceil \sum (P_{i,j} \oplus \boldsymbol{Q}_{i,j} + 50 \times (P_{i,j} + \boldsymbol{Q}_{i,j}))/(M+N) \right\rceil$$

$$m_2 = \left\lceil \sum (P_{i,j} \oplus \boldsymbol{Q}_{i,j} + 100 \times (P_{i,j} + \boldsymbol{Q}_{i,j}))/(M+N) \right\rceil, i = 1,2,\ldots,M$$

$$m_3 = \left\lceil \sum (P_{i,j} \oplus \boldsymbol{Q}_{i,j} + 150 \times (P_{i,j} + \boldsymbol{Q}_{i,j}))/(M+N) \right\rceil, j = 1,2,\ldots,N$$

(iv) Compute cipher messages c_i and $c\mu$ by RSA, i.e., $c_i = m_i^e \bmod n$ and $c\mu = \mu^e \bmod n$, respectively, where $i = 1,2,3$.

(v) Obtain the initial keys x_0, y_0, z_0 by new MKA

$$x_0 = \sin\left(\frac{(c_1 \times M + m_1 \times N) \times \mu \times \pi}{n} \bmod \frac{\pi}{2}\right)$$

$$y_0 = \sin\left(\frac{(c_2 \times M + m_2 \times N) \times \mu \times \pi}{n} \bmod \frac{\pi}{2}\right)$$

$$z_0 = \sin\left(\frac{(c_3 \times M + m_3 \times N) \times \mu \times \pi}{n} \bmod \frac{\pi}{2}\right)$$

Table 2. Minimum space tests.

Image sizes	Minimum space
64×64	5×10^{16}
128×128	4×10^{17}
256×256	3×10^{18}
512×512	2×10^{19}
1024×1024	2×10^{20}
2048×204	1.7×10^{21}

In order to test the space of plain messages m_1, m_2, m_3 calculated from the plain images, black images with different sizes are selected to compute the minimum space for these plain messages. The results for different sizes are shown in the Table 2.

From the key acquisition MKA, we can see that if the plain image is not all black, the corresponding minimum space will be larger. Moreover, Table 2 lists key space analysis for different plain messages. In addition, this paper randomly generates a 64×64 matrix as a plain image for testing the initial keys x_0, y_0, z_0, and repeats 5000 times to obtain the distribution as shown in the Fig. 5. It is obvious that the range of x_0, y_0, z_0 distributes fully in [0, 1].

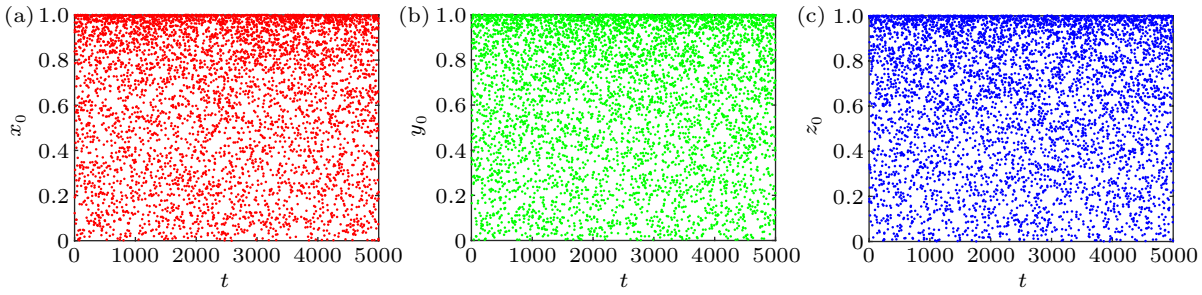


Fig. 5. The distributions for initial key of (a) x_0, (b) y_0, and (c) z_0.

3.2. Image encryption process

Based on 3D-ILM, RSA, MKA, NPM, an image encryption algorithm with asymmetric structure is designed including following steps. Figure 6 displays the flowchart for the proposed image encryption algorithm.

Step 1 Transform chaotic sequence x into a matrix $\boldsymbol{X}$ with size $M \times N$ whose elements are in [0, 255], as follows:

$$xx = \text{floor}(x \times 10^{14}) \bmod 256,$$
$$\boldsymbol{X} = \text{reshape}(xx, M, N). \tag{4}$$

Step 2 Do XOR operation for P and $\boldsymbol{X}$ to get the image P', as follows:

$$P' = \boldsymbol{X}^{\mathrm{T}} \oplus P \oplus \boldsymbol{X}. \tag{5}$$

Step 3 Select M values from sequence y to form keystream y', and do sort operation for it to get the index sequence $L = \{l_1, l_2, \ldots, l_M\}$. Then use the index L to permute the image P' and get permuted image P'', as follows:

$$P''(i,:) = P'(L(i),:), \quad i = 1,2,\ldots,M. \tag{6}$$

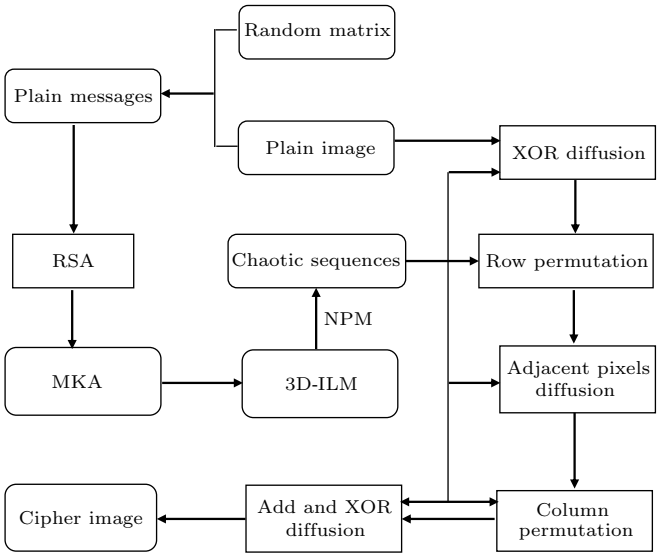


Fig. 6. Encryption flowchart.

Step 4 Perform add and XOR functions under modulus operation for the adjacent pixels. For the first row, each ele-

ment is diffused only by the adjacent element on the left. The same is to the first column, i.e., each element is diffused only by the adjacent element on the upper. Then, all rest elements are diffused by both adjacent elements in the upper and left, as shown in the Fig. 7.

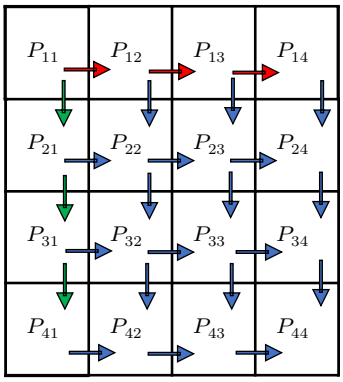


Fig. 7. Diffusion pattern for pixels.

Assuming that the image H is obtained after the above diffusion operation, the complete process is as follows:
the diffusion operation for the first row is

$$H(1,j+1) = (P''(1,j+1) + P''(1,j)) \bmod 256,$$
$$j = 1,2,\ldots N-1, \tag{7}$$

the diffusion operation for the first column is

$$H(i+1,1) = (P''(i+1,1) + P''(i,1)) \bmod 256,$$
$$i = 1,2,\ldots,M-1, \tag{8}$$

the rest elements are diffused by

$$H(i,j) = \big[\big((P''(i,j) + P''(i,j-1)\big) \bmod 256\big) + P''(i-1,j)\big] \bmod 256, \tag{9}$$

where $i = 2,3,\ldots,M$, $j = 2,3,\ldots,N$.

Step 5 Permute the image H by index sequence L in column direction as

$$A(:,j) = H(:,L(j)), \quad j = 1,2,\ldots,N. \tag{10}$$

Step 6 Arrange keystream z into a vector $\boldsymbol{Z}$ of length MN, with values in [0, 255], as follows:

$$\boldsymbol{Z} = \text{floor}(z \times 10^{14}) \bmod 256. \tag{11}$$

Step 7 Arrange image A into a one-dimensional vector $\boldsymbol{a}'$. Then, perform functions of add and XOR under modulus operation in forward direction for $\boldsymbol{a}'$ and vector $\boldsymbol{Z}$ to get vector $\boldsymbol{b}'$ as

$$\boldsymbol{b}'(1) = (\boldsymbol{b}'_0 \oplus \boldsymbol{a}'(i) + \boldsymbol{Z}(i)) \bmod 256,$$
$$\boldsymbol{b}'(i) = (\boldsymbol{b}'(i-1) \oplus \boldsymbol{a}'(i) + \boldsymbol{Z}(i)) \bmod 256, \tag{12}$$

where $i = 2,3,\ldots,MN$, and $\boldsymbol{b}'_0 = 0$.

Step 8 Do the backward functions of add and XOR under modulus operation for the vector $\boldsymbol{Z}$ and vector $\boldsymbol{b}'$ to get vector $\boldsymbol{e}$, as follows:

$$\boldsymbol{e}(MN) = (\boldsymbol{e}_0 \oplus \boldsymbol{b}'(MN) + \boldsymbol{Z}(i)) \bmod 256,$$
$$\boldsymbol{e}(j) = (\boldsymbol{e}(j+1) \oplus \boldsymbol{b}'(j) + \boldsymbol{Z}(j)) \bmod 256, \tag{13}$$

where $j = MN-1,\ldots,2,1$ and $\boldsymbol{e}_0 = 0$.

Step 9 Rearrange the vector $\boldsymbol{e}$ into the cipher image C, as follows:

$$C = \text{reshape}(\boldsymbol{e},M,N). \tag{14}$$

4. Decryption process

After receiving the cipher messages c_1, c_2, c_3, and $c\mu$, the receiver first computes the plain messages m_1, m_2, m_3, and μ by using the RSA algorithm with the private key d. Then, the initial key x_0, y_0, z_0 can be got by MKA. Consequently, by substituting the new 3D-ILM with NPM, the three chaotic sequences x, y, z can be easily obtained. Finally, inverse process of image encryption step-by-step for the cipher image can be executed.

5. Experiment details

5.1. Experimental results

To simulate, MATLAB2019A is used for experiments on a platform of Windows 10. Set the parameters of the 3D-ILM to be $r_1 = 3.6868$, $r_2 = 0.0196$, and $r_3 = 0.0126$, respectively. Select primes $p = 6203$, $q = 6211$, public key $e = 263$, and random number $\mu = 0.2568$. Images mountain and landscape are chosen randomly for tests, with sizes 256×256 and 512×512, respectively. By using the proposed encryption algorithm, the initial keys of the 3D-ILM corresponding to mountain are $x_0 = 0.9404$, $y_0 = 0.1136$, $z_0 = 0.8415$, while the initial keys for the landscape are $x_0 = 0.7172$, $y_0 = 0.6491$, $z_0 = 0.1391$. Figure 8 gives the test results as follows.

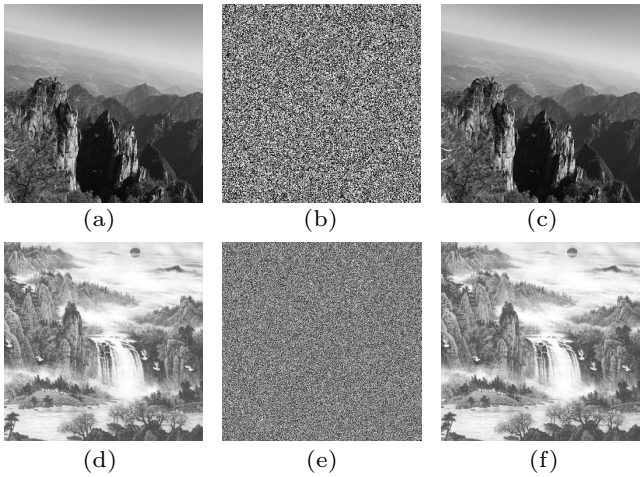


Fig. 8. Simulations for mountain: (a) the plain image, (b) the cipher image, and (c) correct decrypted image. Simulations for landscape: (d) the plain image, (e) the cipher image, and (f) correct decrypted image.

Therefore, by using the proposed algorithm, the cipher image is a noise-like image, and no information can be directly understood. Of course, the plain image can be decrypted using correct keys.

5.2. Histogram and statistical analyses

Histogram can directly describe the pixel distributions for any given image. Generally, a plain image contains a large number of visual information under some certain rules. However, after an ideal encryption, it should be flat and uniform for the cipher image to resist statistical attacks. Images peppers and barbara of size 512×512 are randomly chosen for tests, with corresponding results shown in Fig. 9. In addition, color image peppers of size 512×512 are also randomly selected for tests as seen in Fig. 10. Therefore, the new image encryption algorithm proposed has a good effect.

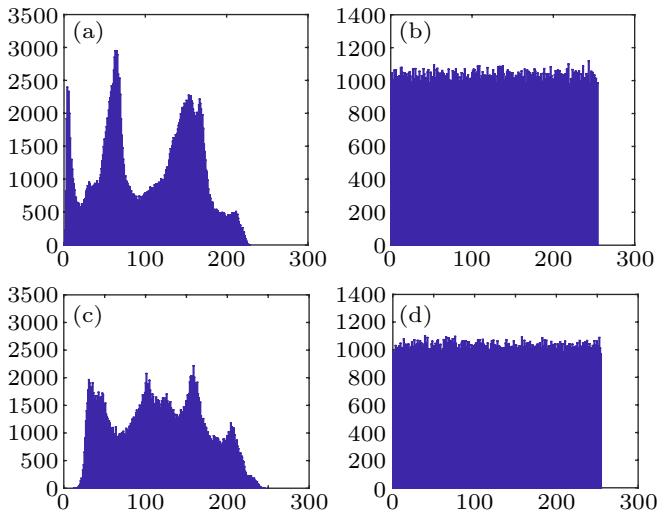


Fig. 9. Histogram tests for (a) the plain image peppers, (b) the cipher image peppers, (c) the plain image barbara, and (d) the cipher image barbara.

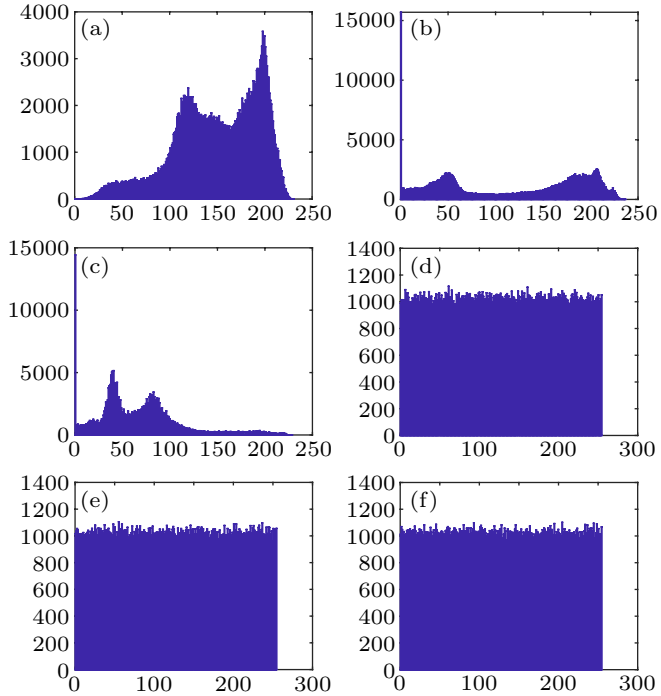


Fig. 10. Histogram tests for plain color image peppers: (a) channel R, (b) channel G, (c) channel B; cipher color image peppers: (d) channel R, (e) channel G, (f) channel B.

To further determine whether the proposed encryption method can resist statistical attacks, the Chi-square test χ^2 is employed for an evaluation objectively. Assuming the gray image size is $M \times N$, and f_i denotes the frequency of pixel. Then, the computation of χ^2 is defined in the following equation:

$$\chi^2 = \sum_{0}^{255} \frac{(f_i - g)^2}{g}, \quad g = M \times N/256, \quad i = 0, 1, \ldots, 255, \tag{15}$$

where the significance level $\alpha = 0.01$ is chosen. If the χ^2 test result of a cipher image is less than $\chi^2_\alpha(255) = 310.45739$, it shows that cipher image passes χ^2 test and has good resistance to statistic attack. Table 3 lists the results of χ^2 tests for each cipher image. So, from these results, the image algorithm proposed can resist the statistical attack effectively.

Table 3. Test results of Chi-square.

Test image	Plain image	Cipher image	Results
Lena (256×256)	3.0666×10^4	217.7031	pass
Mountain (256×256)	2.0960×10^4	207.4453	pass
Cameraman (256×256)	1.6127×10^5	225.6172	pass
Lena (512×512)	1.5768×10^5	233.3203	pass
Boat (512×512)	3.9584×10^5	227.4863	pass
Landscape (512×512)	1.7062×10^5	227.5664	pass
Girl (512×512)	2.9009×10^5	232.8887	pass
Barbara (1024×1024)	3.7827×10^5	257.6968	pass

5.3. Information entropy analysis

Information entropy (IE) is usually taken to describe the uncertainty and the fuzziness of the given data. For an image, the higher the IE is, the higher the degree of confusion is. IE is calculated as

$$H(x) = -\sum_{i=0}^{L-1} p(x_i) \log(p(x_i)), \tag{16}$$

where, for a gray image, we can get $L = 256$. The $p(x_i)$ represents the probability of occurrence of gray level value x_i. The value of IE for the cipher image should be close enough to $H = \log_2 L = 8$, in order to better protect the image information. Table 4 shows the IE values for different images with different sizes. Moreover, Table 5 shows the comparisons between the proposed algorithm and other algorithms. Therefore, one can see that the proposed method can provide a good performance for image encryption.

5.4. Key space analysis

Based on the new 3D-ILM and RSA, an asymmetric image encryption algorithm is proposed in this paper. Three plain messages m_1, m_2, m_3 are extracted from the original plain image, which can depend on the plain image strongly. Then all

the plain messages and cipher messages are used to compute initial keys x_0, y_0, z_0 by conversion MKA together with the random number μ. Therefore, if one of them changes, each initial key will also be changed significantly. Compared with the analysis in Table 1, the minimum key space corresponding to different sizes of image is shown in Table 6 considering the random number. So, the proposed encryption algorithm has a large enough key space with respect to minimum request of 2^{100}, which can effectively resist violent attacks. Because the initial keys x_0, y_0, and z_0 are not only related to the plain image, but also related to a random matrix and a random number as seen in the algorithm. So, x_0, y_0, and z_0 will change on the random matrix and random number, but the ranges of them are always fallen fully into [0,1]. The initial key distribution can also be seen in Fig. 5.

Table 4. IE tests.

Images	Results	
	Plain image	Cipher image
Lena (256×256)	7.5683	7.9976
Mountain (256×256)	7.6749	7.9977
Landscape (512×512)	7.4110	7.9994
Peppers (512×512)	7.5391	7.9994
Baboon (512×512)	7.3585	7.9994
Girl (512×512)	7.2520	7.9994
Lena (512×512)	7.4474	7.9994
Boat (512×512)	7.1238	7.9994
Barbara (1024×1024)	7.6462	7.9998
Man (1024×1024)	7.5237	7.9998

Table 5. Comparisons of IE with different images.

Images	Ours	Ref. [29]	Ref. [30]
Lena (512×512)	7.9994	7.9992	7.9992
Peppers (512×512)	7.9994	7.9992	–
Cameraman (256×256)	7.9975	–	7.9972

Table 6. Minimum key space.

Size	Key space
64×64	2^{102}
128×128	2^{105}
256×256	2^{108}
512×512	2^{111}
1024×1024	2^{114}
2048×2048	2^{117}

5.5. Key sensitivity analysis

In addition to effective against common attacks, a new designed image encryption algorithm should also has high key sensitivity, that is, when one of the keys changes slightly, the original plain image can not be decrypted. In this paper, image mountain is randomly tested as shown in the Fig. 11. Furthermore, to show the key sensitivity numerically, the number of pixels change rate (NPCR) is taken to test the difference using small difference in correct keys, as results shown in the Table 7.

Table 7. NPCR tests.

Decrypted image	Decrypted key	Results
Figure 9(c)	correct key	0
Figure 9(d)	m_1+1	99.6353%
Figure 9(e)	m_2+1	99.6323%
Figure 9(f)	m_3+1	99.6277%
Figure 9(g)	$\mu+10^{-14}$	99.6140%

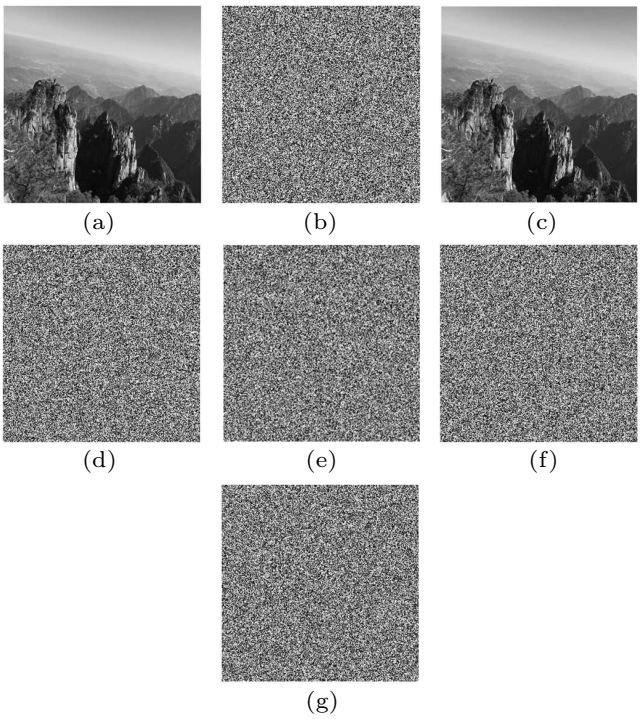


Fig. 11. Key sensitivity tests for image mountain: (a) the plain image, (b) the cipher image, (c) decrypted image with correct key, (d) decrypted image with m_1+1, (e) decrypted image with m_2+1, (f) decrypted image with m_3+1, (g) decrypted image with $\mu+10^{-14}$.

From the above analysis, it is clear that one cannot correctly recover the plain image when the key changes slightly, with NPCR values close to 1. That is to say, the strong key sensitivity can be achieved.

5.6. Correlation analysis

To describe the correlation between adjacent pixels for an image, correlation coefficient is usually taken as an important tool. If the value is closed to zero, the randomness is higher; otherwise, the randomness is lower. Normally, for a natural meaningful image, the adjacent pixels have strong correlations. Therefore, for a new designed encryption algorithm, it is necessary to reduce the correlation to close to zero considering the directions in horizontal, vertical and diagonal lines. The correlation coefficient is computed as follows:

$$\rho_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{17}$$

where

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)), \tag{18}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right)^2. \tag{19}$$

In this paper, image boat of size 512×512 is chosen randomly to do the tests. 3000 pairs of adjacent pixels are randomly selected from boat and its cipher image. Test results of the correlation coefficients are shown in Fig. 12 with three directions. Moreover, Table 8 lists results of the correlation coefficients after testing different images. It is obvious that the correlation is almost zero by using the proposed encryption algorithm with a good performance.

Table 8. Tests of correlation coefficients.

Image	Plain image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena (256×256)	0.9687	0.9356	0.9196	0.0090	0.0173	−0.0088
Girl (256×256)	0.9779	0.9747	0.9521	−0.0007	0.0013	−0.0148
Peppers (512×512)	0.9831	0.9810	0.9752	0.0020	−0.0041	0.0085
Bridge (512×512)	0.9301	0.9414	0.9132	−0.0022	0.0276	0.0109
Goldhill (512×512)	0.9731	0.9704	0.9536	0.0094	−0.0023	0.0089
Lena (512×512)	0.9843	0.9733	0.9622	−0.0099	0.0101	0.0037
Man (1024×1024)	0.9799	0.9792	0.9646	0.0033	0.0055	−0.0249

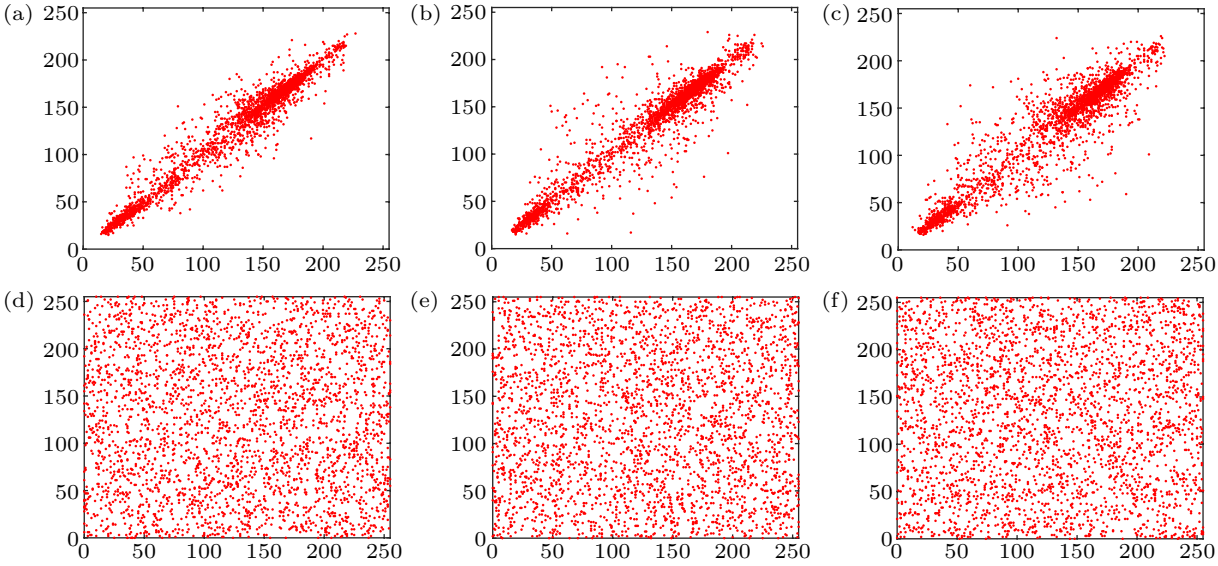


Fig. 12. Correlation tests for boat: plain image in (a) horizontal direction, (b) vertical direction, and (c) diagonal direction; cipher image in (d) horizontal direction, (e) vertical direction, and (f) diagonal direction.

5.7. Differential attack analysis

The NPCR and the unified average changing intensity (UACI) are commonly employed to evaluate differential attack, which are defined as follows:

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\%, \tag{20}$$

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j), \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j), \end{cases} \tag{21}$$

$$\mathrm{UACI} = \frac{1}{M \times N}\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{22}$$

where, the ideal values are 99.6094% and 33.4634% for NPCR and UACI, respectively. To have a test, a pixel in random position of image barbara is modified each time, with results being shown in the Fig. 13.

Table 9. The average values of NPCR and UACI.

	Lena	Boat	Peppers	Baboon	Goldhill
NPCR	99.6092	99.6070	99.6095	99.6088	99.6046
UACI	33.4540	33.4646	33.4644	33.4609	33.4723

Table 10. Comparisons of NPCR and UACI.

Image	Ours		Ref. [31]		Ref. [32]	
	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)
Lena	99.6092	33.4540	99.66	33.62	99.61	33.46
Boat	99.6070	33.4646	99.61	33.62	–	–
Baboon	99.6088	33.4609	99.60	33.65	99.62	33.44
Peppers	99.6095	33.4644	99.60	33.56	99.60	33.45
Barbara	99.6087	33.4628	–	–	99.61	33.46

Moreover, the average values of NPCR and UACI calculated from different images are listed in Table 9. So, all values are very near to the ideal case after using the proposed method,

which tells us that the encryption algorithm has a good ability to resist differential attack. Furthermore, to show better performance, Table 10 gives the comparisons between our algorithm and other methods by considering the NPCR and the UACI. Therefore, the new algorithm here is more effective.

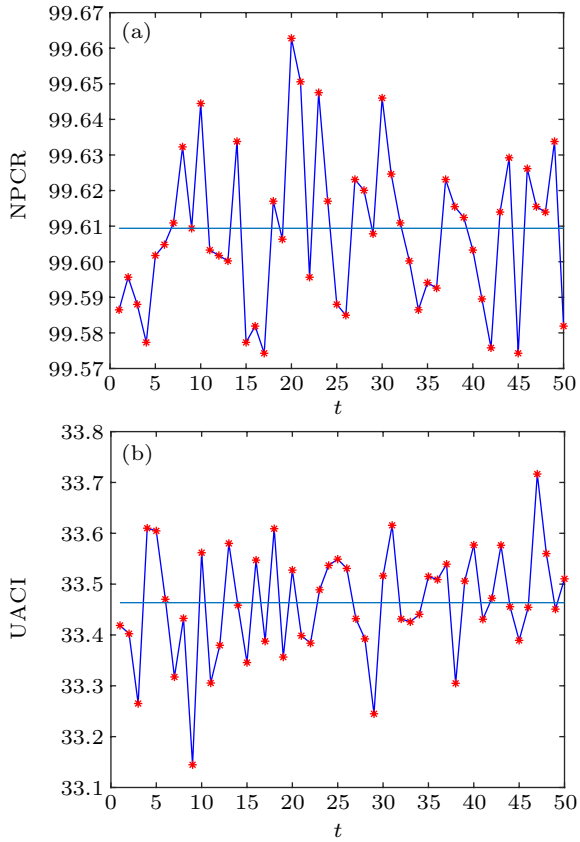


Fig. 13. Differential attack tests: (a) NPCR values and (b) UACI values.

5.8. Robustness analysis

Among the common attacks, robustness ability should also be considered for a designed image encryption scheme, which is directly related to the quality of the decryption after being attacked. In this paper, the robustness analysis is tested by adding salt-and-pepper noise attack and clipping attack. Figure 14 shows the test results by adding salt and pepper noise, and Fig. 15 displays the test results by making clipping attack. So, one can see that the image encryption algorithm presented has a good robustness performance.

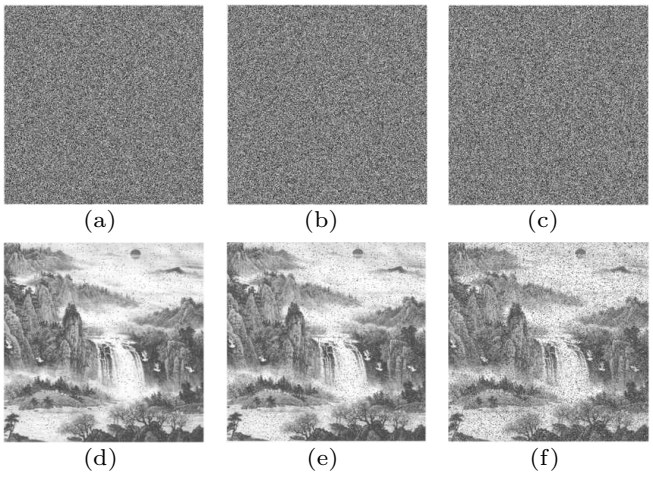


Fig. 14. Attack tests of salt-and-pepper noise to the cipher image landscape: (a) with 0.005 noise, (b) with 0.01 noise, (c) with 0.03 noise, (d) decrypted image from panel (a), (e) decrypted image from panel (b), and (f) decrypted image from panel (c).

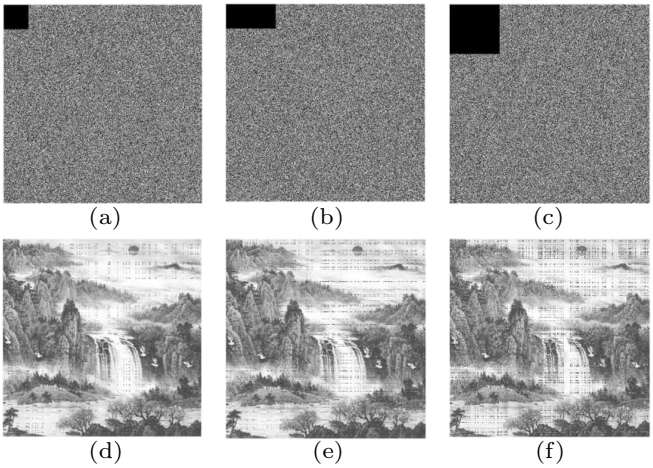


Fig. 15. Cropping attack tests t_0 the cipher image landscape: (a) with cropping of 64×64, (b) with cropping of 64×128, (c) with cropping of 128×128, (d) decrypted image from panel (a), (e) decrypted image from panel (b), (f) decrypted image from panel (c).

5.9. Execution efficiency analysis

The computation complexity and time efficiency are important metrics to evaluate an encryption algorithm. In our encryption scheme, the whole encryption process is divided into two stages. Suppose the size of the plain image is $M \times N$ with length $n = M \times N$. In the first stage, there is a computation complexity about $O(48n)$ to obtain the secret keys and generate chaotic sequences. In the second stage, there is a computation complexity about $O(13n)$ to complete the image encryption process. Therefore, the total computation complexity is about $O(61n)$, i.e., $O(n)$. Table 11 shows the encryption time and decryption time of the different images. Therefore, it can be seen that the algorithm proposed in this paper has good performance.

Table 11. Time cost analysis (unit: s).

Size	Image	Encryption time	Decryption time
256×256	Lena	0.2784	0.2571
	Cameraman	0.2620	0.2510
	Girl	0.2628	0.2593
512×512	Bridge	1.0351	0.9943
	Boat	1.0263	0.9819
	Peppers	1.0260	0.9989
1024×1024	Barbara	4.1320	4.0233
	Lena	4.1235	4.0042
	Landscape	4.1270	4.0371

6. Conclusion

A novel chaotic map 3D-ILM is constructed and an asymmetric image encryption algorithm is designed with the help of

RSA. The new 3D-ILM has more complex chaotic dynamic behavior after the analyses of time series, Lyapunov exponent, Shannon entropy, and NIST SP800-22 test. In process of image encryption, a new key acquisition MKA is designed, which combines random number, random matrix, and pixel information of plain image. As a result, the relationship of key stream generated to the plain image is enhanced. Moreover, to ensure the security, RSA is employed to transmit the initial keys to avoid extra transmission, and solve the difficulty of key distribution and management. Especially, a new NPM is suggested to process the input of the 3D-ILM before each iteration. All the experiments and test results have proved that the proposed encryption algorithm in this paper has high security with a strong robustness, and can provide a new secure scheme for image communication.

Due to direct encryption of a plain image into a noise-like cipher image, which is one of the efficient ways to protect the security of communication images, like other current image encryption algorithms, it may cause the attention of the attackers from visual effect. In the future work, we will continue to study another method information hiding technology and to design new image hiding algorithm.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (Grant No. 61972103), the Natural Science Foundation of Guangdong Province of China (Grant No. 2023A1515011207), the Special Project in Key Area of General University in Guangdong Province of China (Grant No. 2020ZDZX3064), the Characteristic Innovation Project of General University in Guangdong Province of China (Grant No. 2022KTSCX051), the Postgraduate Education Innovation Project of Guangdong Ocean University of China (Grant No. 202263), and the Foundation of Guangdong Provincial Engineering and Technology Research Center of Far Sea Fisheries Management and Fishing of South China Sea.

References

[1] Chuman T, Sirichotedumrong W and Kiya H 2019 *IEEE Trans. Inform. Foren. Sec.* **14** 1515
[2] Wang J, Zhang Y X, Wang F, Ni R J and Hu Y H 2022 *Chin. Phys. B* **31** 034205
[3] Chen J J, Yan D W, Duan S K and Wang L D 2020 *Chin. Phys. B* **29** 110504
[4] Pan H L, Lei Y M and Jian C 2018 *Eurasip J. Image Video Proc.* 142
[5] Gao X H 2021 *Opt. Laser Technol.* **142** 107252
[6] Zhou N R, Huang L X, Gong L H and Zeng Q W 2020 *Quantum Inform. Proc.* **19** 284
[7] Ye G D, Jiao K X and Huang X L 2021 *Nonlinear Dyn.* **104** 2807
[8] Elrefaey A, Sarhan A and El-Shennawy N M 2021 *J. Real-Time Image Proc.* **18** 1897
[9] Yuan H M, Liu Y, Lin T, Hu T and Gong L H 2017 *Signal Process.: Image Commun.* **52** 87
[10] Yavuz E 2021 *J. Inform. Secur. Appl.* **63** 103056
[11] Gao H and Gao T G 2019 *Multimed. Tools Appl.* **78** 7267
[12] Kamal F M, Elsonbaty A and Elsaid A 2021 *Chaos Soliton. Fract.* **144** 110686
[13] Song J and Lee Y H 2021 *Opt. Commun.* **485** 126707
[14] Ding L N and Ding Q 2020 *Electronics* **9** 1280
[15] Ding Y, Wu G Z, Chen D J, Zhang N, Gong L P, Cao M S and Qin Z G 2021 *IEEE Internet Things* **8** 1504
[16] Tang Y D, Shao Z H, Zhao X X and Shang Y Y 2021 *Signal Process.: Image Commun.* **93** 116168
[17] Wu J H, Cao X Y, Liu X F, Ma L J and Xiong J P 2019 *J. Mod. Opt.* **66** 764
[18] Zhang S J and Liu L F 2021 *Math. Comput. Simulat.* **190** 723
[19] Dagadu J C, Li J P and Aboagye E O 2019 *Wirel. Pers. Commun.* **108** 591
[20] Wang X Y and Zhao M C 2021 *Opt. Laser Technol.* **143** 107316
[21] Hazer A and Yildirim R 2021 *J. Opt.* **23** 113501
[22] Vilardy J M, Jimenez C J and Torres C O 2019 *Photonics* **6** 116
[23] Ni R J, Wang F, Wang J and Hu Y H 2021 *IEEE Photon. J.* **13** 7800116
[24] Wu H S, Zhu H Y and Ye G D 2021 *Phys. Scripta* **96** 105202
[25] Li Q Y and Boyen X 2021 *Theor. Comput. Sci.* **892** 85
[26] Ye G D, Wu H S, Jiao K X and Mei D 2021 *Math. Biosci. Eng.* **18** 5427
[27] Joshi A B, Kumar D, Mishra D C and Guleria V 2020 *J. Mod. Opt.* **67** 933
[28] Alawida M, Samsudin A, Sen Teh J and Alkhawaldeh R S 2019 *Signal Process.* **160** 45
[29] Wang X Y, Xue W H and An J B 2020 *Chaos Soliton. Fract.* **141** 110309
[30] Al-Hazaimeh O M, Al-jamal M F, Alhindawi N and Omari A 2019 *Neural Comput. Appl.* **31** 2395
[31] Ahmad J and Hwang S O 2016 *Multimed. Tools Appl.* **75** 13951
[32] Chai X L, Gan Z H, Yuan K, Lu Yang and Chen Y R 2017 *Chin. Phys. B* **26** 020504