An image encryption scheme based on swapping operation and block scrambling

Xinyu Gao, Junqiao Liu, Huizhen Yan

{ email: dalianliujunqiao@126.com}

School of Information Science and Engineering, Dalian polytechnic University, Dalian 116034, China

Abstract. For purpose of meeting the requirement of encryption security, this paper brings an image encryption scheme based on chaotic system, block scrambling, swapping of rows and columns. The chaotic matrixes and index sequences are obtained to realize the rows and columns exchange and block scrambling, and the diffusion method is used to make the pixels fully diffuse so that the security can be improve. The image gray distribution, the correlation, the key space and the robustness against cropping attack are analyzed and simulated. The results show that the proposed scheme has high security and provides theoretical guidance.

Keywords: Swapping operation; Block scrambling; Chaotic system.

1 Introduction

Image information has the characteristics of intuitive and vivid, which is widely used in the digital age, but it is vulnerable to various attacks by hackers [1]. In recent years, due to the sensitivity of initial value, aperiodic of chaos, many scholars have used chaotic systems to generate random data streams to encrypt images [2-4]. There are many kinds of chaos system from one-dimensional to five-dimensional or even seven-dimensional [5-8]. One-dimensional map is simple, and the generation time is short, but the distribution of blank windows is not uniform. The chaotic system with higher dimensions has stronger chaotic dynamics, but it takes a long time. The encryption process usually has two steps: pixels scrambling in which the pixel positions are changed and diffusion, and in diffusion the pixel values are changed [9]. There are many methods of scrambling, such as Arnold scrambling, two-dimensional image spreading into one-dimensional image scrambling, two-dimensional image directly scrambling [10]. The common methods of diffusion are addition and modulo operation, XOR operation and cyclic shift operation.

Large number of encryption algorithms about chaos have been suggested [11-14]. Wang et al. presented a plaintext-related image encryption scheme according to Josephus traversing and pixel permutation [15]. Zhu et al. [16] used 3-D cat map 3-D DNA level permutation scheme for encryption scheme. Farah et al. [17] introduced a hybrid chaotic map and used it to generate chaotic sequence to encrypt a gray image. Sun et al. encrypted color images by using

EAI GreeNets 2021, June 06-07, Dalian, People's Republic of China

DOI 10.4108/eai.6-6-2021.2307948

a new memristive chaotic system [18]. Similarly, Hua et al. introduced chaotic maps with good dynamic performance and used one of their to encrypt images [19]. The combination of chaotic system and image encryption has good performance and gradually becomes a research hotspot [20].

This paper proposed an encryption scheme which uses block operation and swapping operation. The scrambling process swaps the rows and columns of the image, then breaks the image into small pieces for further scrambling. The diffusion process enhances the security of image encryption.

This paper is made up of six parts. In Section 2, the chaotic system, swapping operation and block scrambling are introduced. The image encryption scheme and simulation results are shown in Section 3 and Section 4. Section 5 and Section 6 give security analysis and conclusions.

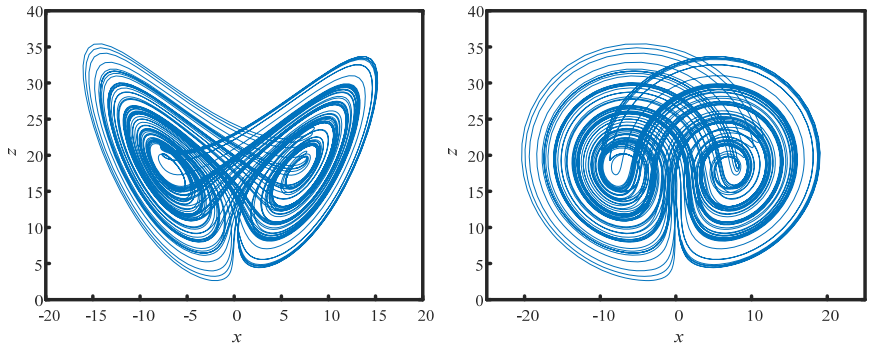
2 Preliminaries

2.1 Lorenz system

In the encryption scheme, simple Lorenz system is defined by

$$\begin{cases} \dot{x}=10(y-x) \\ \dot{y}=-xz+(24-4c)x+cy \\ \dot{z}=xy-\dfrac{8}{3}z \end{cases}, \tag{1}$$

Where c∈[-1.59,7.75]. In this paper, we set control parameter c=2, initial condition $[x_0, y_0, z_0]$ = [1, 2, 3], iteration time step h=0.001. The attractor phases of simple Lorenz system are given in Figure 1.



(a) (b)

Fig.1 Attractors phase: (a) *x*-*z* plane, (b) *y*-*z* plane

2.2 Swapping operation

In this section, the swapping operation is introduced. Firstly, the index sequences q_1 and q_2 are as same as chaotic sequences x and y. Secondly, sequence $q1$ and sequence $q2$ are used for row swapping and column swapping. The details are described as follows:

Step 1: By using the control parameter and initial conditions, three chaotic sequences x, y, z can be produced by equation (1).

Step 2: The sequences are dealt with Eq. (2) and Eq. (3)

$$\begin{cases} X = x\left(end - 512\times512 + 1 : end\right) \\ Y = y\left(end - 512\times512 + 1 : end\right) \\ Z = z\left(end - 512\times512 + 1 : end\right) \end{cases}, \tag{2}$$

$$\begin{cases} X\left(i\right) = \left(\left(X\left(i\right) + 100\right)\times10^{10}\right) \backslash 256 + 1 \\ Y\left(i\right) = \left(\left(Y\left(i\right) + 100\right)\times10^{10}\right) \backslash 256 + 1 \\ Z\left(i\right) = \left(\left(Z\left(i\right) + 100\right)\times10^{10}\right) \backslash 256 + 1 \end{cases}, \tag{3}$$

where equation (2) and equation (3) include the operation of remainder after division. Then, three sequences are changed to three matrixes with size of 512×512.

Step 3: Diagonal elements from the matrixes X and Y are picked out and arranged as the index sequences q_1 and q_2.

Step 4: The rows and columns are processed by equation (4) and equation (5)

$$\begin{cases} t_1 = C\left(i,:\right) \\ C\left(i,:\right) = C\left(q_1\left(i\right),:\right) \\ C\left(q_1\left(i\right),:\right) = t_1 \end{cases}, \tag{4}$$

$$\begin{cases} t_2 = C\left(:,j\right) \\ C\left(:,j\right) = C\left(:,q_2\left(j\right)\right) \\ C\left(:,q_2\left(j\right)\right) = t_2 \end{cases}, \tag{5}$$

we can get image C which has swapped the rows and columns.

2.3 Block scrambling

Block scrambling is to divide the original image into $m1\times n1$ small pieces and scramble those small pieces. The scrambling step consists of the following four steps:

Step 1: The chaotic matrixes are obtained as step 1 and step 2 in section 2.2. Then, three sequences a, b and q are processed by equation (6)

$$\begin{cases} a = X(:) \\ b = Y(:) \\ q = (a+b) \setminus 256 + 1 \end{cases}. \tag{6}$$

Where $(a+b)\backslash 256$ is the operation of taking the remainder.

Step 2: The original image is divided into $m1 \times n1$ small blocks with size of $m \times n$.

Step 3: All image blocks are arranged into block vectors. Then, the block vectors are processed by equation (7)

$$\begin{cases} t_3 = C(i) \\ C(i) = C(q(i)), \\ C(q(i)) = t_3 \end{cases} \tag{7}$$

we can obtain image C which has scrambled by block scrambling.

Step 4: Block vectors are pieced into $(m1 \times m) \times (n1 \times n)$ image.

3 Encryption scheme

The whole encryption procedures are drawn in Figure 2.

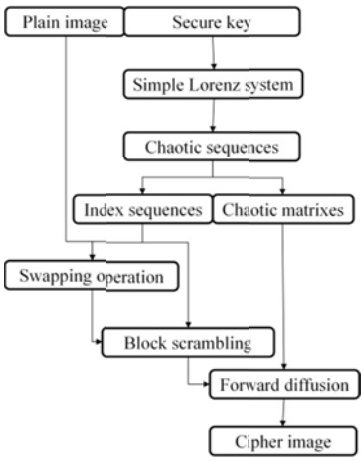


Fig.2 The diagram of encryption algorithm

Step 1: According to the parameter x_0, y_0, z_0 and k, the chaotic matrixes X, Y, Z and index sequences q_1, q_2 can be obtained as the step 1-3 in section 2.2.

Step 2: Each row of the image is put into the swap space t_1, then the corresponding swap sequence is found by using the pseudo-random index sequence and swapped.

Step 3: Each column of the image is put into the swap space t_2, then the corresponding swap sequence is found by using the pseudo-random index sequence and swapped.

Step 4: The image is divided into $m1 \times n1$ blocks, then the image is scrambled in blocks, as presented in section 2.3.

Step 5: The first pixel is following the operation by equation (8)

$$C(1,1) = I(1,1) \oplus X(1,1) \oplus Z(1,1), \tag{8}$$

where $I(1,1) \oplus X(1,1)$ means xor operation.

Step 6: The first row is processed by equation (9)

$$C(1, j) = I(1, j) \oplus X(1, j) \oplus C(1, j-1), \tag{9}$$

where j from 2 to end.

Step 7: The first row is processed by equation (10)

$$C(i,1) = I(i,1) \oplus X(i,1) \oplus C(i-1,1), \tag{10}$$

where i from 2 to end.

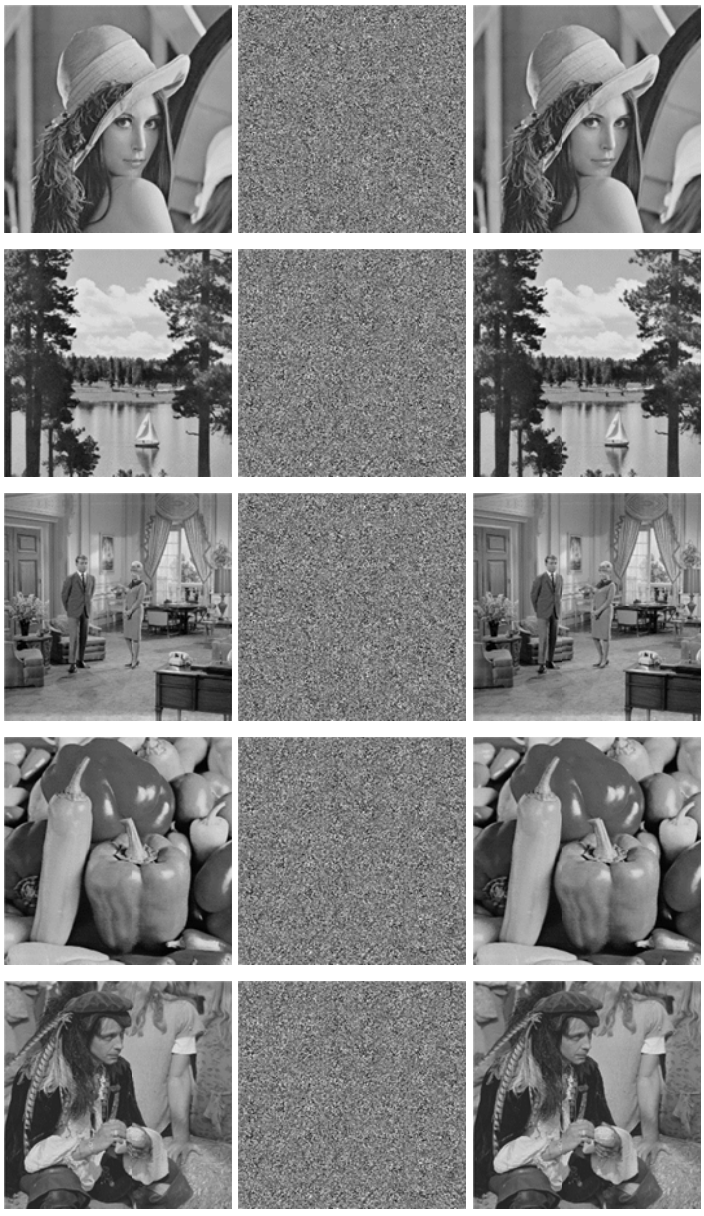
Step 8: The rest of the image pixels are processed by equation (11)

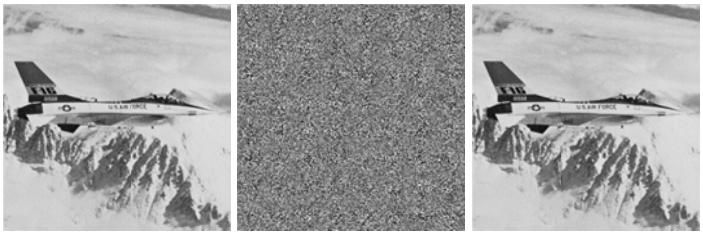
$$C(i, j) = I(i, j) \oplus X(i, j) \oplus C(i-1, j) \oplus C(i, j-1). \tag{11}$$

4 Simulation results

The experiments are simulated on MATLAB (version R2018a) to testify the security of the image algorithm. In experiment, the test images “Lena”, “Lake”, “Livingroom”, “Peppers”, “Man”, and “Jet” with size of 512 ×512 are tested. Simplified Lorenz system initial keys x_0, y_0, z_0 and c are fixed as 1, 2, 3 and 2. Figure 3 gives simulation results: test images mentioned above is arranged in the first column of Figure 3 (a), the corresponding encrypted images and the decrypted images after applying the decryption strategy to it are shown in Figure 3(c) and (d), respectively. First of all, through the observation of the image, the encrypted image obtained after encryption cannot be seen visually with any valuable information. Secondly, the

image obtained by the decryption experiment is compared with the test image, and the experimental results show that the encryption algorithm mentioned in this paper is reversible. In summary, this encryption algorithm meets the two most basic requirements of image encryption, namely, the hiding of information and the recoverability of encrypted images.





(a) (b) (c)

Fig.3 Experimental results of encryption and decryption

5 Security analysis

5.1 Key space test

For an attacker, the easiest way to crack the encryption system may be a brute force attack. In other words, when the key space of the encryption system is small, the attacker can crack the encryption system after a limited number of tests whether the key is true or not. Therefore, after research by cryptographers, the key space of a good encryption system should be at least 2^{100}.

The keys in our algorithm are composed of control parameter c and initial values x_0, y_0, z_0 and the specific value of the key space is approximately 2^{212} after giving the accuracy of the computer 10^{-16}. This shows that brute force attack [21] is not feasible for the encryption system with such a large key space.

5.2 Information entropy

Image information entropy is a statistical form of features, which reflects the average amount of information in the image. It is generally believed that in an encryption system, when the image is encrypted, the higher the information entropy of the image, the less visible information of the image. This entropy is defined by equation (12)

$$H(S)=\sum_{S} P(S_i)\log_2\frac{1}{P(S_i)}bit\ , \tag{12}$$

where S_i represents source that value belongs [0 255], $P(S_i)$ represents probability of occurrence of S_i. When the gray value distribution of the image is consistent, the information entropy value of the image is the ideal value 8. That is to say, the closer the information entropy of the encryption algorithm is to 8, the better its performance.

Table 1 lists that specific values of information entropy of plain images and the encrypted images, the test results are close to the expectation value. The test results found that the information entropy of the encrypted image has been greatly improved compared to the information entropy of the flat image, and its information entropy value is around 7.9993, which indicates that the entropy-related attack [22] is invalid for the encryption algorithm proposed in this paper [23].

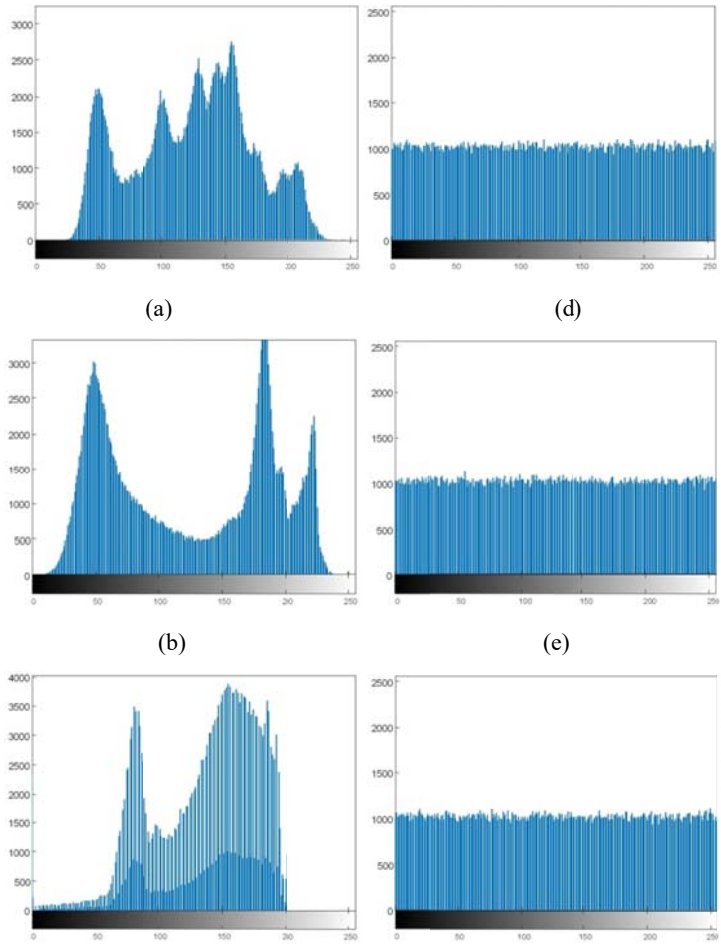
Table 1 Information entropies of six grayscale images

Image	Lena	Lake	Living room	Peppers	Man	Jet
Plain image	7.4451	7.4826	7.2925	6.7624	7.2367	6.7135
Cipher image	7.9992	7.9992	7.9993	7.9993	7.9993	7.9993

5.3 Statistic analysis

5.3.1 Histogram

Histogram is the most intuitive way to view the distribution of image pixel information. Histogram distribution of encrypted image from a good encryption scheme should be uniform. Figure 4 presents the histograms of the test images and its encrypted images in this experiment. From the Figure 4, the histograms of encrypted images distribution are fairly uniform while their corresponding original images are undulating. It can get a conclusion that statistical attacks [16] alone are not capable of deciphering the encryption scheme proposed in this paper.



(c) (f)

Fig.4 Histograms of the original and encrypted images, (a) (d) original Lena and its encrypted image; (b) (e) original Lake and its encrypted image; (c) (f) original Woman and its encrypted image.

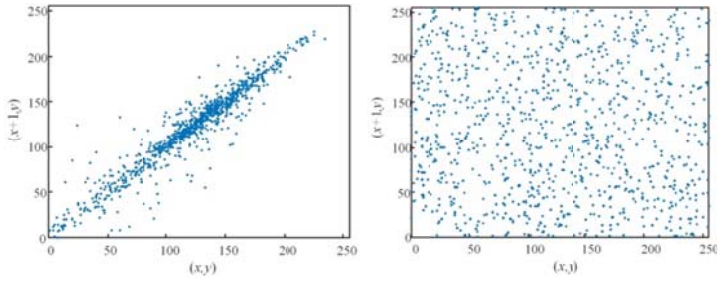
5.3.2 Correlation coefficient

Correlation test refers to the degree of connection between adjacent pixels where the correlation is measured by correlation coefficient. For an original image, absolute value of correlation coefficient is about 1 [24]. On the contrary, correlation will be destroyed after image encryption while the closer the absolute value of the correlation is to 0, the better the encryption effect of the image. The correlation coefficient can be derived from Equation (13)

$$\begin{cases} r_{xy} = \dfrac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \\ \operatorname{cov}(x,y) = \dfrac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \\ D(x) = \dfrac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2 \\ E(x) = \dfrac{1}{N}\sum_{i=1}^{N} x_i \end{cases}, \tag{13}$$

where x and y are gray values of two adjacent pixels x, which can be the horizontal (H), vertical (V) and diagonal (D) directions.

The correlation analysis is shown in Table 2 and Figure 5 in a quantitative and qualitative manner by using the results calculated by Equation 15. From the Figure 5, it can be seen that the plain image has strong correlation close to 1 while the cipher image does not close to 0. Table 2 is a further verification of the conclusions obtained in Figure 5 by numerical methods. This just proves that our encryption algorithm can not only change image correlation, but also it can resist statistical attacks [25].



(a) (d)

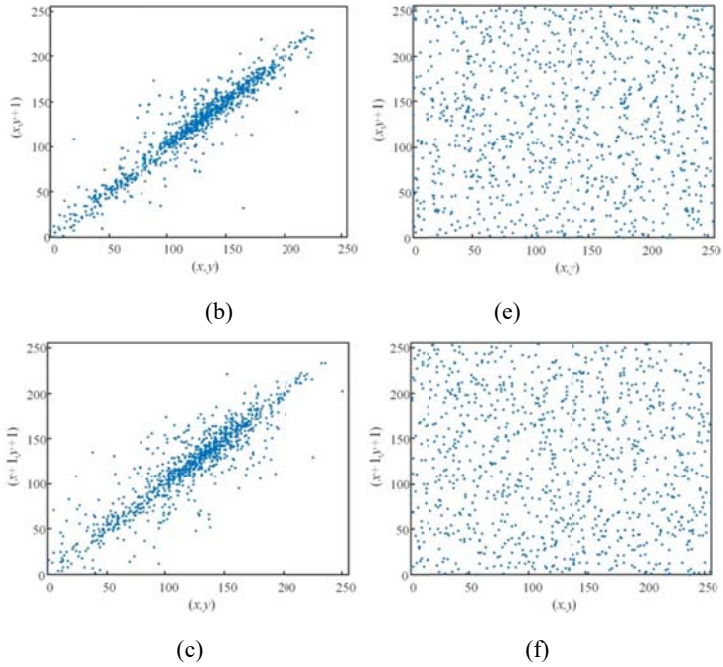


Fig.5 Test results of correlation distribution: (a) (b) (c) correlation of "Living room" in H, V, D direction; (d) (e) (f) correlation of cipher image in H, V, D direction.

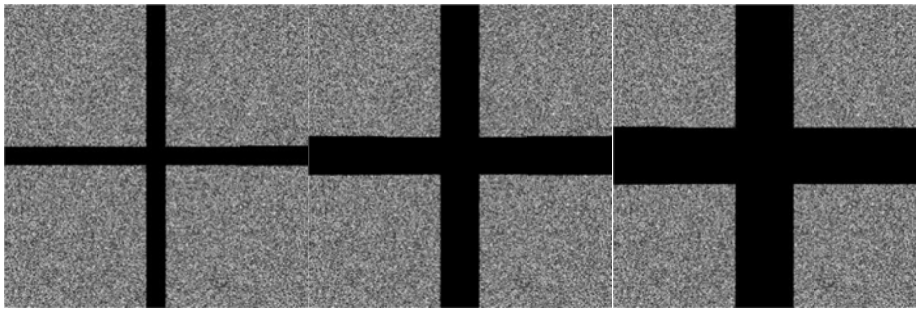
Table 2 Correlation of different images in H, V, D directions

Image	Direction	Plain image	Cipher image
Lena	H	0.9849	0.0020
	V	0.9718	-00017
	D	0.9590	-0.0031
Lake	H	0.9764	-0.0001
	V	0.9767	0.0009
	D	0.9622	0.0001
Living room	H	0.9524	-0.0008
	V	0.9459	0.0011
	D	0.9116	-0.0009
Peppers	H	0.9804	0.0003
	V	0.9802	0.0003
	D	0.9705	-0.0008
Man	H	0.9694	0.0021
	V	0.9602	0.0029
	D	0.9421	0.0026
	H	0.9702	-0.0005

Jet	V	0.9730	-0.0012
	D	0.9491	0.0005
	H	-	0.0010
Average	V	-	0.0014
(absolute value)	D	-	0.0013

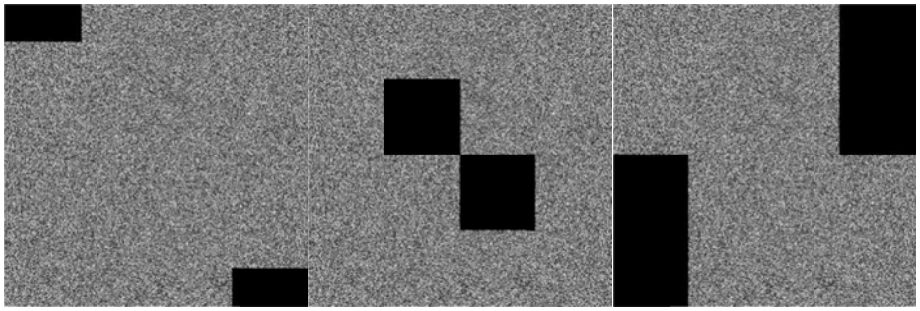
5.4 Cropping attack analysis

The cipher image could be cropped during the transmission process, which leads to the loss of some essential date in the decrypted image. Therefore, whether the key information of the image can be smoothly restored after a part of the information is lost becomes an important indicator for evaluating the encryption system. That is to say, even if some information of cipher image is lost, the cipher image can also be decrypted successfully, so the encryption scheme performs well. Figure 6 shows the experiment results after the information lost: the plain image "Lena" as test image is cropped according to different size and different direction. Since the image can be restored with a higher quality when a small amount of information is lost, the main outline information of the image can still be seen when a large amount of information is lost, which indicates that the loss of information will not become the weak point of this encryption scheme.



(a) data loss of 12.1% (b) data loss of 17.9% (c) data loss of 23.4%

(d) decrypted image, 12.1% (e) decrypted image, 17.9% (f) decrypted image, 23.4%



(g) data loss of 6.25% (h) data loss of 12.5% (i) data loss of 25%

(j) decrypted image, 6.25% (k) decrypted image, 12.5% (l) decrypted image, 25%

Fig.6 Cropping attack results

6 Conclusion

The algorithm in this paper uses swapping operation and block operation to encrypt the gray image. Firstly, the pseudo-random sequences are constructed by simple Lorenz system, and then the image is scrambled by exchanging rows and columns and scrambling blocks, so as to realize pixel scrambling and improve the encryption effect. Secondly, image encryption can be achieved by replacing pixel values. Theoretical analysis and simulation results indicate that encryption system used in this paper can pass most of the performance tests smoothly like key space, statistical and entropy tests, and has good robustness against cropping. Therefore, this algorithm provides another new encryption strategy for the secure transmission of image information on the Internet, and has certain application value.

References

[1] M. Roy, S. Chakraborty, K. Mali, D. Roy, and S. Chatterjee, "A robust image encryption framework based on DNA computing and chaotic environment," Microsystem Technologies, pp. 1-11, (2021)

[2] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," Information Sciences, vol. 547, pp. 1154-1169, (2021)

[3] Y. Yang, L. Wang, S. Duan, and L. Luo, "Dynamical analysis and image encryption application of a novel memristive hyperchaotic system," Optics & Laser Technology, vol. 133, pp. 106553-106567, (2021)
[4] X. Yan, X. Wang, and Y. Xian, "Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation," Multimedia Tools and Applications, no. 1, pp. 1-35, (2021)
[5] Z. Hua, Y. Zhou, C. M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," Information Sciences, vol. 297, pp. 80-94, (2015)
[6] Liu, Hongjun, Kadir, and Abdurahman, "Asymmetric color image encryption scheme using 2D discrete-time map," Signal Processing the Official Publication of the European Association for Signal Processing, pp. 104-112, (2015)
[7] C. Li, K. Qian, S. He, H. Li, and W. Feng, "Dynamics and Optimization Control of a Robust Chaotic Map," IEEE Access, vol. PP, no. 99, pp. 1-1, (2019)
[8] Z. H. A, Z. Z. A, S. Y. B, Z. Z. C, and H. H. A, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map - ScienceDirect," Information Sciences, vol. 546, pp. 1063-1083, (2021)
[9] H. Li, Y. Wang, and Z. Zuo, "Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms," Optics & Lasers in Engineering, vol. 115, no. APR., pp. 197-207, (2019)
[10] M. Kaur and V. Kumar, "A Comprehensive Review on Image Encryption Techniques," Archives of Computational Methods in Engineering, pp. 1-29, (2018)
[11] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, "Integrated Chaotic Systems for Image Encryption," Signal Processing, vol. 147, no. JUN., pp. 133-145, (2018)
[12] R. Lan, Y. Zhou, Z. Liu, and X. Luo, "Prior Knowledge-Based Probabilistic Collaborative Representation for Visual Recognition," IEEE Transactions on Cybernetics, pp. 1-11, (2018)
[13] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm," Optics and Lasers in Engineering, vol. 128,pp. 105995-106008, (2020)
[14] C. L. Li, Z. Y. Li, W. Feng, Y. N. Tong, and D. Q. Wei, "Dynamical behavior and image encryption application of a memristor-based circuit system," AEU - International Journal of Electronics and Communications, vol. 110, pp. 152861-152881, (2019)
[15] Y. Niu and X. Zhang, "A Novel Plaintext-Related Image Encryption Scheme Based on Chaotic System and Pixel Permutation," IEEE Access, vol. PP, no. 99, pp. 22082-22093, (2020)
[16] C. Zhu, Z. Gan, Y. Lu, and X. Chai, "An image encryption algorithm based on 3-D DNA level permutation and substitution scheme," Multimedia Tools and Applications, vol. 79, no. 4, (2020)
[17] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," Nonlinear Dynamics, vol. 99, no. 1, pp. 1-24, (2020)
[18] J. Sun, C. Li, T. Lu, A. Akgul, and F. Min, "A memristive chaotic system with hypermultistability and its application in image encryption," IEEE Access, pp. 1-10, (2020)
[19] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," Information Sciences, vol. 480, pp. 403-419, (2019)
[20] C. Xu, J. Sun, and C. Wang, "An Image Encryption Algorithm Based on Random Walk and Hyperchaotic Systems," International Journal of Bifurcation and Chaos, vol. 30, no. 04, pp. 2050060-2050075, (2020)

[21] Chai et al., "A novel image encryption algorithm based on the chaotic system and DNA computing," International Journal of Modern Physics C Physics & Computers, vol. 28, no. 5, pp. 1750069-1750092, (2017)
[22] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," Signal Processing Image Communication, vol. 52, pp. 6-19, (2017)
[23] X. Jin, S. Yin, N. Liu, X. Li, G. Zhao, and S. Ge, "Color image encryption in non-RGB color spaces," Multimedia Tools and Applications,vol. 77, pp. 15851-15873, (2017)
[24] S. Som, S. Dutta, R. Singha, A. Kotal, and S. Palit, "Confusion and diffusion of color images with multiple chaotic maps and chaos-based pseudorandom binary number generator," Nonlinear Dynamics, vol. 80, no. 1-2, pp. 615-627, (2015)
[25] Zheng et al., "Encryption method based on a new secret key algorithm for color images," Aeu Archiv Fur Elektronik Und Ubertragungstechnik Electronic & Communication, vol. 70, no. 1, pp. 1-7, (2016)