Journal of Fiber Bioengineering and Informatics 8:2 (2015) 381–389
doi:10.3993/jfbim00115

Image Encryption Based on Complicated Chaotic ⋆

Xin Zhang [a], Lai Zhou [b], Hongbin Gu [d], Weibin Chen [c,d,*]

[a] *School of Information Engineering, Wenzhou Medical University, Wenzhou 325035, China*

[b] *Shanghai Electro-Mechanical Engineering Institute, Shanghai Academy of Spaceflight Technology Shanghai 201109, China*

[c] *College of Physics and Electronic Information Engineering, Wenzhou University Wenzhou 325035, China*

[d] *College of Civil Aviation, Nanjing University of Aeronautics and Astronautics Nanjing 210016, China*

Abstract

In order to improve the security of secret image transmission, using the property of the chaotic sequence in the encryption algorithm, a block image encryption scheme based on Logistic and Henon composite chaotic system is presented. The image encryption algorithm from two aspects that the pixel grayscale value and pixel position through two different chaotic sequences transform of the Logistic and Henon. At first, Logistic chaotic sequence is applied to the scrambling operation on the pixel position matrix. Then the pixel values of blocked images are scrambled based on Henon chaotic sequence. The experiments show that the algorithm has good encryption effect, and has better robustness to crop or noise attack. The cross correlation of encrypted image are decreased and the transport security is improved, the result shows that the project is effective.

Keywords: Chaotic System; Logistic Map; Henon Map; Image Encryption

1 Introduction

With the rapid progress of information technology, the digital image storage and transmission security problem has become an important research direction in the field of information security. The image data encryption technology takes one kind of commonly used digital image processing technology, which widely applies to domain of the military, aviation, medicine, communication. Image data is characterized by its large data volume and higher information correlation. Secret

⋆Project supported by the National Nature Science Foundation of China (No. 51305255), Natural Science Foundation of Shanghai City (No. 13ZR1455900), Research Project of Zhejiang Provincial Department of Education (No. Y201223187, Y201430709) and the Ordinary University Scientific Research of Innovation Projects in Jiangsu Province (No. CXLX13-162).

*Corresponding author.
Email address: cwb@nuaa.edu.cn (Weibin Chen).

1940–8676 / Copyright © 2015 Binary Information Press & Textile Bioengineering and Informatics Society
June 2015

key sensitivity and real-time data should be taken into consideration when design an encryption scheme. Research shows that a good password system should meet the following conditions:

(1) The plaintext should be transform for random cipher text;

(2) Highly sensitive to the encryption algorithm;

(3) Chaotic systems are sensitive to the chaotic key.

The characteristics of the chaotic system, such as well pseudorandom, long inscrutability, high sensibility to the initial value, the regularity and universality, make it be applied in the code field [1–5]. Chaotic encryption method is flexible. We take advantage of all the good qualities of chaotic signal.

2 Based on the Logistic and Henon Compound Chaotic Sequence Encryption Algorithm

Chaotic sequence has the characteristics of high ergodicity and sensitivity to initial value, this feature is suitable for the encryption of digital information. In view of the small key space, the simple encryption structure, the low chaotic sequence complexity and the low safety, the block image encryption algorithm based on the Logistic and Henon compound chaotic sequence is presented in this paper. In the new image encryption system, image encryption is implemented by changing the position and value of every pixel. Image encryption with the improved complicated chaotic sequence is studied such as encryption structure, key space and every possible attack. In this paper, the digital image encryption algorithm encryption algorithm flow chart is shown in Fig. 1. This encryption algorithm is divided into two key steps:

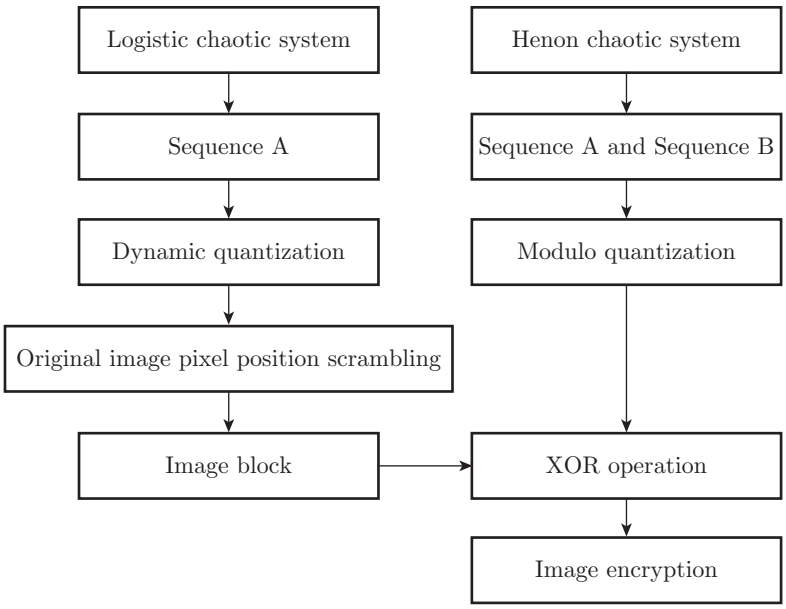


Fig. 1: Steps of the encryption algorithm

Step 1 Pixel position scrambling transformation;

Step 2 Grey value is encrypted of block image.

2.1 The Positions of Image Pixels Scrambling Transformation

Logistic sequence is the typical chaotic mapping in chaotic systems [6–8]. The chaotic sequence has easy to produce, is sensitive to the initial condition as well as has the dummy randomness. In this paper, the image encryption is implemented by changing the position of image pixel with the Logistic chaotic sequence. The Logistic chaotic sequence is constructed as Eq. (1):

$$x_k = ux_k(1 - x_k) \tag{1}$$

Here u is bifurcation parameter ($0 \leq u \leq 4$), and x^k is the state variables of the system $x^k \in (0, 1)$. If one chooses $u \in [3.5699456 \cdots, 4]$, the system is chaotic. According to the image of size $m \times n$ with the initial conditions u and x_0, the chaos sequence is generated by Eq. (1). The chaos sequence is defined as $x_k; k = 1, 2, \cdots, m \times n$. The new chaotic sequence $x_k^{'}$ is generated by sorting the chaotic sequence x_k. The location information of the new chaotic sequence x'_k can be gained from the chaotic sequence x_k. The pixel vector of position scrambling image can be obtained as $N_k; k = 1, 2, \cdots, m \times n$. And the image pixel position scrambling is realized. The image scrambling encryption experimental results with the above way is shown in Fig. 2. The experiment results show that the histogram of the original image and the cipher image are not changed. So the image encryption based on position scrambling can't change histogram distribution of original image. This will affect the security of image encryption results. The analysis indicates that the encryption algorithm can not effectively resist attack.

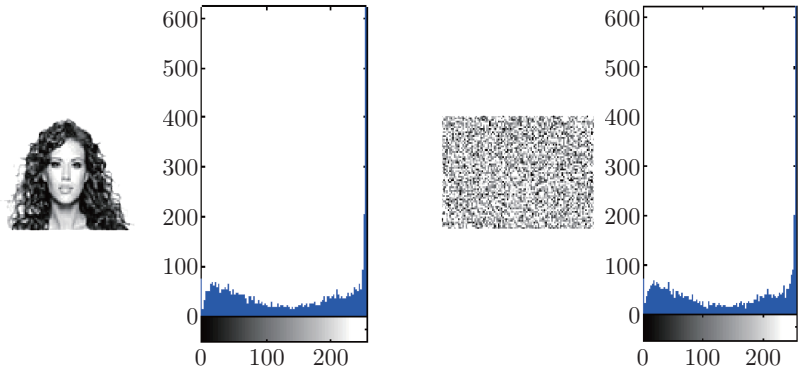


Fig. 2: The original image and position scrambling image. The left row show the image and its histogram. The right row show the original image and its histogram osition scrambling image and its histogram

2.2 Grey Value Encryption of Block Image

Studies have shown that the key space can be increased and the security of encryption algorithm can be improved by choosing different chaotic system in the grey value encryption. Compared with single dimension mapping, Henon map is nonlinear two-dimensional mapping [9, 10]. It has the following features: the complexity of the dynamic characteristics and the single inverse

value. These features make Henon map suitable for digital image encryption. In our scheme, two variables of the Henon chaotic map are adopted to encrypt the grey value. Henon chaotic map is described as follows:

$$\begin{cases} x_{n+1} = y_n + 1 - ax_n^2 \\ y_{n+1} = bx_n^2 \end{cases} \tag{2}$$

Here a and b are control parameter. The well-studied Henon map presents a simple two-dimensional map with quadratic non-linearity. This map gave a first example of the strange attractor with a fractal structure. Because of its simplicity, the Henon map easily lends itself to numerical studies. Thus a large amount of computer investigations followed. Nevertheless, the complete picture of all possible bifurcations under the change of the parameters a and b is far from completion. If one chooses $1.05 < a < 1.8, b = 0.3$, the system is chaotic. According to the image of size $m \times n$, the chaos sequence is generated by Eq. (2). The chaos sequence is defined as $Hx(k)'(k = 1, 2, \cdots, m \times n); Hy(k)'(k = 1, 2, \cdots, m \times n)$. The approximate uniform random sequence can be obtained by using quantitative methods of the integers modulo operators in the chaotic sequence $Hx(k)$. The approximate uniform random sequence is defined as $Hx'(k)'(k = 1, 2, \cdots, m \times n); Hy^k(k)'(k = 1, 2, \cdots, m \times n)$. This arithmetic is of better anti-attack. In order to improve the security of encryption algorithm, the image block is given after position scrambling. The position scrambling image is divided into upper and lower two parts, and then the position scrambling block images are encrypted by random sequence. The random sequence is adjusted by XOR operation, and then the values of block image pixel are encrypted by the adjustment random sequence. The grey value scrambling can change histogram distribution of original image. The grey value of block image is encrypted as shown in Fig. 3.

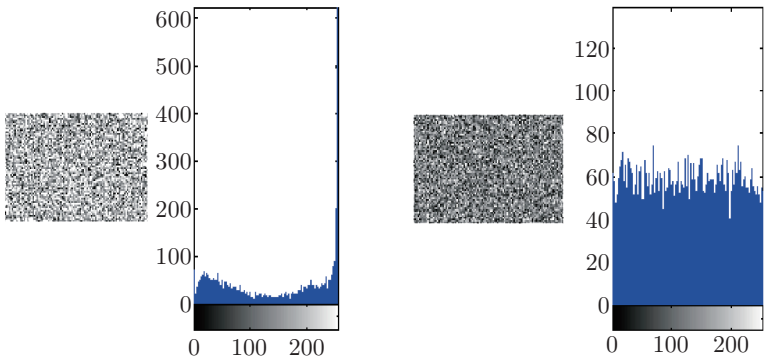


Fig. 3: Grey value encryption. The left row show the position scrambling image and its histogram. The right row show the finally encrypted image and its histogram

In our scheme, the encryption process consists of two steps of operations.

Step 1: The image encryption is implemented by changing the position of image pixel with the Logistic chaotic sequence. The results show that the correlation of adjacent pixels can not be effectively destroyed by the single chaotic system position scrambling.

Step 2: The image block is given after position scrambling. The position scrambling block images are encrypted by Henon sequence. In the new image encryption system, image encryption is implemented by changing the position and value of every pixel. In our scheme, the key space can be increased and the security of encryption can be improved.

3 The Analysis of Encryption Effect

3.1 Security Analysis

Some experimental results are given in this section to demonstrate the efficiency of our scheme. Encryption algorithm in this paper consists of three system parameters of two chaotic systems and three initial values of state variables. They can be used as key. When to encrypt the original image, take system parameters are as follows: $u = 3.8, a = 1.4, b = 0.3$. The initial value selection (key) is as follows: $x_1(0) = 0.11, x_2(0) = 0.21, x_3(0) = 0.22$. Experimental initial values for testing the safety are as follows: $x_1(0) = 0.1100001, x_2(0) = 0.2100001, x_3(0) = 0.22$. The encrypted image and the decrypted image with the right key is shown in Fig. 4. The encrypted image and the decrypted image with the wrong key is shown in Fig. 5. From the experimental results it can be seen that the subtle differences of initial value will lead to the failure of the image decryption in chaotic system. The sensitivity to initial value is validated through simulation. Experimental results show that the algorithm has high security.

The security of encryption algorithm in encryption algorithm is not only sensitive to initial value, but also the effectiveness of the exhaustive attack is affected by the size of the key space. The key space of block image encryption algorithm based on Logistic and Henon Compound chaotic sequence is composed of six parameters. The six parameters is $u, a, b, x_1(0), x_2(0), x_3(0)$. Among them, the five parameters can be accurately said to 15 double precision of real number after the decimal point. So the size of key space is $10^{15\times5=10^{75}}$. Due to realizing in double-real precision, the algorithms are provided with big secret key space. If the key space is enough big,

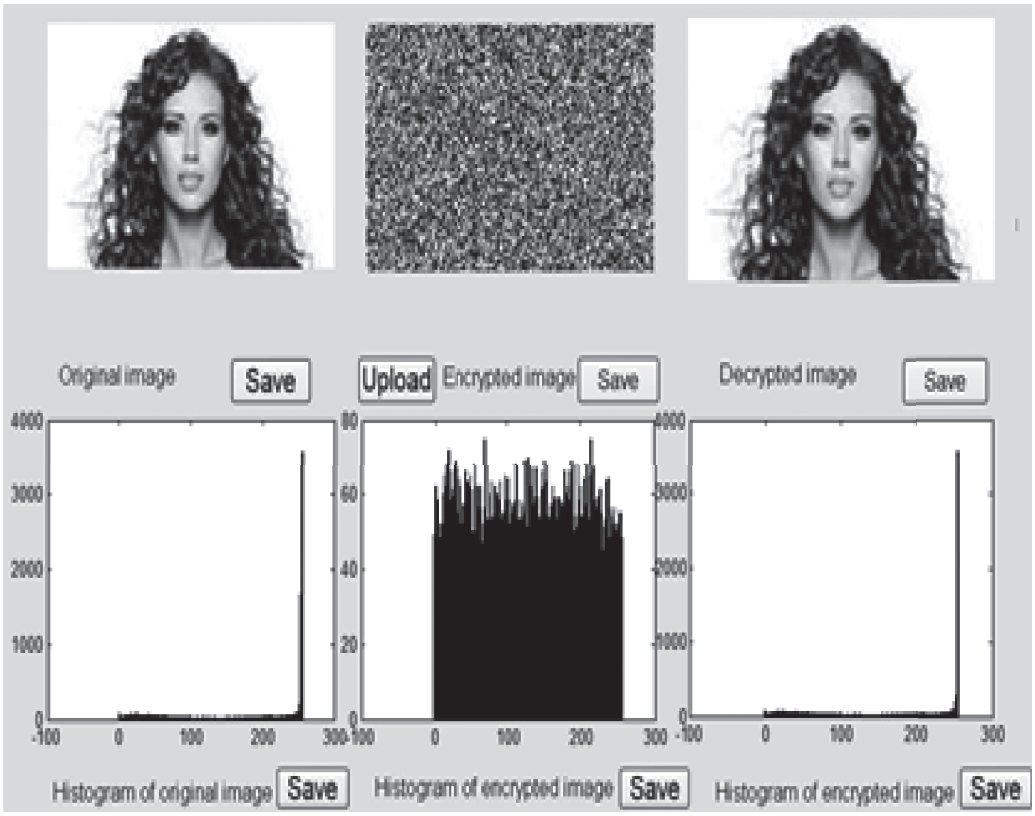


Fig. 4: Image encryption and decryption with the right key

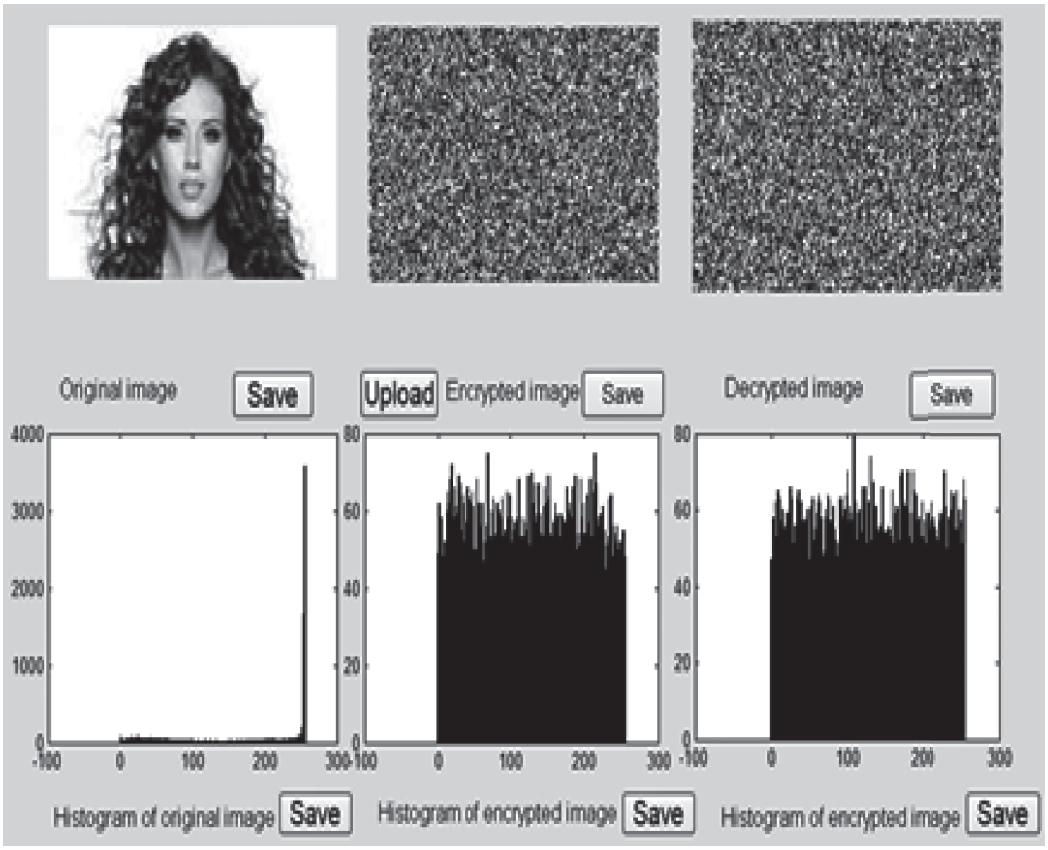


Fig. 5: Image encryption and decryption with the wrong key

the algorithm can be more effective against brute force attack.

3.2 Attack Experimental Analysis

We validate the algorithm through experiments and analyze its performance. Fig. 6 shows the final encrypted image by cutting a location and the histogram shows the results of image after decryption. The experiments show that although to cut the part of encrypted image, the most of the original image information is restored after image decryption.

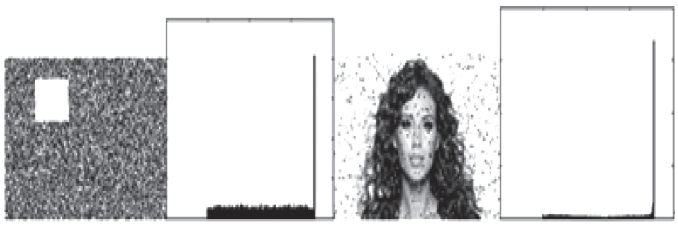


Fig. 6: Experiment results of part cutting

In the fighting against noise experimental analysis, the diagrams of two typical noises (Gaussian noise and salt-pepper noise) are given in the paper. Fig. 7 shows the decrypted image after salt-pepper noise attacking and the result of histogram. Fig. 8 shows the decrypted image after

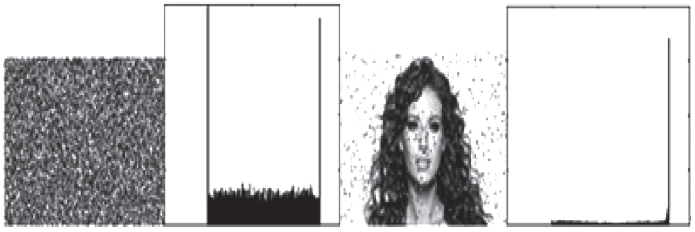


Fig. 7: The decrypted image after salt-pepper noise attacking

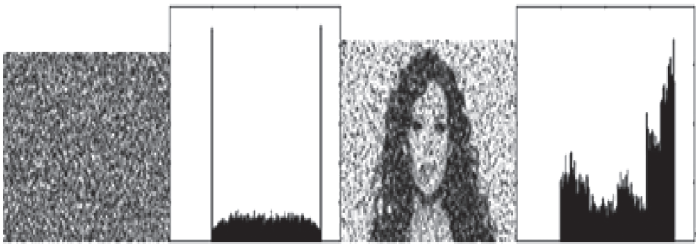


Fig. 8: The decrypted image after Gaussian noise attacking

Gaussian noise attacking and the result of histogram. Experiments show that the capability of these two methods to resist all kinds of common attacks is excellent.

3.3 Correlation Analysis

The results show that adjacent pixels of original image have great correlation. In order to effectively overcome the threat of statistical attacks, the correlation of adjacent pixels must be reduced by encryption algorithm. The calculation formulas of image correlation between adjacent pixels are described as follows:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{3}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{4}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{5}$$

$$R_(x,y) = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{6}$$

Here x and y are the adjacent pixel values in images. $E(x)$ is the average value of pixel values. $D(x)$ is the mean square error of pixel values. $cov(x,y)$ is Correlation function. $R(x,y)$ is the relativity of close pixels. In order to verify the effectiveness of the proposed chaotic encryption algorithm, the above formulas are applied to the original image and the encrypted image. The proposed chaotic encrypted algorithm was implemented and tested with experimental image. 2000 pairs of adjacent pixels which are randomly selected, are analyzed from three directions vertical, horizontal and diagonal in the image. The experimental results of Table 1 show that the original

image is large correlation between adjacent pixels. The correlation of the adjacent pixels with the proposed image encryption algorithm is less than the correlation of the original image.

Table 1: Correlation analysis

	Vertical	Horizontal	Diagonal
Original image	0.9639	0.9613	0.94035
Encrypted image with Logistic chaotic system	0.0296	0.0275	0.0424
Algorithm in this paper	0.0147	0.0018	−0.0328

3.4 Image Fidelity Analysis

Image encryption and image decryption may lead to the information loss of the original image. So the degree of the deviation between the decrypted image and the original image need to be described. Typical fidelity rule includes two types:

(1) Objective fidelity criteria.

(2) Subjective fidelity criteria.

Objective fidelity rule is easy to calculate or measure. So the root mean square error e_{rms} and peak signal-to-noise ratio ($PSNR$) are chosen to analyze the fidelity of decrypted image and original image.

$I(x,y)$ is the original image, $\hat{I(x,y)}$ is the decrypted image. The root mean square error e_{rms} and peak signal-to-noise ratio ($PSNR$) between original image and decrypted image are defined as Eq. (7) and Eq. (8). And the sizes of the two images are $M \times N$.

$$e_{rms} = \left[\frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [\hat{I}(x,y) - I(x,y)]^2 \right]^{1/2} \tag{7}$$

$$PSNR = 10lg \left[\frac{I_{max}^2}{\frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [\hat{I}(x,y) - I(x,y)]^2} \right] \tag{8}$$

where $I_{max} = maxI(x,y), x = 0, 1, \cdots, M-1, y = 0, 1, \cdots, N-1$. It is the maximum gray value of images. The fidelity of the image shown in Fig. 4 is analyzed. The mean square error is 0 between the original image and the decrypted image with the right key. And peak signal noise ratio is infinite. The experimental results show that the algorithm for image encryption and decryption is without errors. And the fidelity of the image shown in Fig. 5 is also analyzed. The mean square error is 166.0759 between the original image and the decrypted image with the wrong key. And peak signal noise ratio is 25.9277. The experimental results show that that the decrypted image with tiny difference keys will be gotten different from the original image. And root mean square error is big.

4 Conclusion

In this paper, image encryption scheme based on the Logistic and Henon compound chaotic sequence with block image is presented. The experimental results show that the algorithm has large enough key space and high security. Meanwhile, through the privacy key analysis, the histogram analysis, attack experimental analysis, correlation analysis and the image fidelity analysis, the security of this algorithm is very high. And the complexity of image encryption based on compound chaotic sequence with block image is improved. The good results were achieved. Simulation results illustrate the validity of the presented method.

References

[1] Honge Ren, Linlin Dai, Jian Zhang, Image encryption algorithm based on chaotic sequence transform [J], Computer Engineering and Design, 2013, 1615-1619

[2] Vinod Patidar, A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption [J], Optics Communications, 284(19), 2011, 4331-4339

[3] Lepeng Liu, Xuefeng Zhang, Image encryption algorithm based on chaos and bit operations [J], Journal of Computer Applications, 33(4), 2013, 1070-1073

[4] Z. L. Zhu, W. Zhang, K. W. Wong et al., A chaos-based symmetric image encryption scheme using a bit-level permutation [J], Information Sciences: An International Journal, 181(6), 2011, 1171-1186

[5] Yang Wang, Chengmao Wu et al., Dynamic block cipher algorithm base on chaos control [J], Journal of Xi'an Institute of Posts and Telecommunications, 17(6), 2012, 42-47

[6] Fengxia Yang, Encryption of compressed image based on logistic mapping [J], Laser Infrared, 43(5), 2013, 565-568

[7] Chaoyong Tuo, Zheng Qin, Qian Li, Color image encryption algorithm based on 2D logistic chaotic map and bit rearrange [J], Computer Science, 40(8), 2013, 300-308

[8] T. V. Patida, N. K. Pareek, K. Sud, Modified substitution diffusion image cipher using chaotic standard and logistic maps [J], Communications in Nonlinear Science and Numerical Simulation, 15(10), 2010, 2755-2765

[9] Ping Ping, Zhijian Wang et al., Analysis and improvement of image encryption algorithm based on Henon map [J], Journal of Nanjing University of Science and Technology, 36(4), 2012, 587-592

[10] Ping Jiang, Dinghui Zhang et al., The digital image encryption based on Henon and Rossler chaotic mapping [J], Data Communications, 4, 2012, 15-18