Journal of Computer and Communications, 2018, 6, 31-44
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A New Digital Image Encryption Algorithm Based on Improved Logistic Mapping and Josephus Circle

Zhiben Zhuang, Jing Wang, Jingyi Liu, Dingding Yang, Shiqiang Chen*

School of Science, Hubei University for Nationalities, Enshi, China
Email: *chensq8808@126.com

How to cite this paper: Zhuang, Z.B., Wang, J., Liu, J.Y., Yang, D.D. and Chen, S.Q. (2018) A New Digital Image Encryption Algorithm Based on Improved Logistic Mapping and Josephus Circle. *Journal of Computer and Communications*, **6**, 31-44.
https://doi.org/10.4236/jcc.2018.66003

Received: March 12, 2018
Accepted: June 18, 2018
Published: June 21, 2018

Abstract

Digital image encryption based on Joseph circle and Chaotic system has become a hot spot in the research of image encryption. An encryption algorithm based on improved Josephus loop and logistic mapping is proposed to scrambling blocks in this paper. At first, the original image is scrambled by using logistic mapping to obtain the encrypted image, and then the encrypted image is divided into many blocks. Finally, the position of the blocked image is scrambled by using the improved Josephus ring to get the encrypted image. According to the experiments, the information entropy of the encrypted image reaches 7.99 and the adjacent correlations in three directions are within ±0.1. The experimental results show that the proposed algorithm has advantages of large key space, high key sensitivity and can effectively resist the attacks of statistical analysis and gray value analysis. It has good encryption effect on digital image encryption.

Keywords

Digital Image Encryption, Image Block Scrambling, Josephus Loop, Logistic Mapping, Pixel Scrambling

1. Introduction

With the rapid development of the application of multimedia technology on the Internet, more and more images are transmitted in the network, such as malicious serial image information, interception and so on, which brings convenience to users and causes a series of potential safety problems. Therefore, it is very important to ensure the security of image information in the process of network transmission. Among the technologies of guarantee image security [1], image encryption [1] is a more intuitive method and the essence of image encryption is pixel scrambling [2].

In 1998, Fridrich proposed an image encryption algorithm based on permutation and confusion structure in [1]. [2] [3] discussed the use of Arnold mapping for pixel replacement, in which [3] also incorporates discrete Chen mapping of pixel values for permutation confusion; [4] [5] [6] [7] used the randomness of one-dimensional chaotic sequence to scramble the pixel position of the image to realize encryption; [8] proposed an image bit encryption algorithm based on Joseph's ergodic and generalized Henon mapping. The security image to be encrypted Hash Algorithm 1 (SHA-1) summary and user-selected encryption parameters are combined as the key to drive Generalized Henon Mapping to randomly disturb the starting position, the reported number of intervals and the reported direction of the improved Josephus traversal map, so that different encrypted images and encryption parameters correspond substantially to different site replacement processes and added a site obfuscation process to improve the security of site replacement. [9] proposed an image pixels scrambling by Tent chaotic mapping and then using S-box permutation of color image encryption algorithm at the bit; [8]-[14] introduced a bit-based encryption algorithm; [15] proposed improved the Logistic map by using scale transformation, constructing robust system and composite mapping respectively. [16] proposed an image encryption with chaotically coupled chaotic maps. [17] proposed an image encryption algorithm based on Brownian motion and image, and introduced a new one-dimensional chaotic system. [18] analyzed the security of image encryption algorithm based on the incorrect fractional-order chaotic system. In [19], a data invariant encryption algorithm based on improved Logistic mapping is proposed. The image encryption performance is analyzed and studied and some indexes of encryption performance evaluation are also given in the [3] [20].

The above works used some pixel value replacement methods in the process of encryption, such as compute of encryption pixels and adjacent elements [4], operations of encryption pixel gray value and key [9] [10] [11] [13] and so on. None of these algorithms involve encrypting the original image first, followed by blocking the entire encrypted image and then scrambling the block. Therefore, this paper presents a digital image encryption algorithm based on improved Josephus loop and improved logistic mapping to scramble block. The images selected by this algorithm are all gray-scale image. The simulation experiments are carried out by Matlab, and the experimental results are evaluated by the evaluation indexes of information entropy, histogram, fixed point ratio and adjacent pixel correlation. The experimental results show that the proposed algorithm has advantages of large key space, high key sensitivity and can effectively resist the attacks of statistical analysis and gray value analysis. It has good encryption effect on digital image encryption.

2. The Preparatory Work

2.1. Improved Joseph's Traversal Mappings

Joseph's problem describes n individuals in a circle, counting from the first person, and continuously eliminating the mth person until the last one remains [8].

According to the Joseph problem, we can uniquely identify an arrangement of *n* elements in the order of elimination. Given *n* and *m*, we can uniquely obtain a permutation constructed by $(1,2,\cdots,n)$. Write $f_{ysf}(n,m)$. For example, $f_{ysf}(4,3)$, which corresponds to the element sequence of 3, 2, 4, 1, so the elements of the order can be 1, 2, 3, 4 by mapping $f_{ysf}(4,3)$ to replace it with 3, 2, 4, 1.

In order to increase the permutation variables generated by Joseph's traversal mappings, the application of Josephus rings is now augmented by an interval *q* constraint, which results in the randomness of the resulting permutations and increases their key space during the image's encryption. After increasing the interval *q*, the corresponding Joseph-ergodic mapping becomes $f_{ysf}^{1}(n,q,m)$.

2.2. Improved Logistic Mapping

In 1976, American ecological mathematician May proposed a logistic mapping model used to simulate the growth behavior of biological populations. It is very simple in mathematical form, but its dynamic behavior is complicated by its nonlinear chaotic system. In the process of image encryption has a wide range of applications. The equation is:

$$x_{n+1} = ux_n(1-x_n), \tag{1}$$

where *n* and *u* are system parameters. When $n = 1,2,\cdots$ and $3.75 \le u \le 4$, the system is chaotic. In order to expand the encryption key of digital image, many researchers have improved the logistic mapping equation. For example, the improved logistic mapping equation is [14]:

$$x_{n+1} = \left(ux_n(1-x_n)\times 2^k\right) - floor\left(ux_n(1-x_n)\times 2^k\right), k \in Z^+, k \ge 8. \tag{2}$$

Its chaotic map is shown in **Figure 1**. In order to make the encrypted image more secure, the Equation (2) is made the following improvements. The equation is:

$$x_{n+1} = \left(u_1 \log(x_n)\times x_n(1-x_n)\times 6^k\right) - floor\left(u_1 \log(x_n)\times x_n(1-x_n)\times 6^k\right), 5 \le k \le 15. \tag{3}$$

When $5 \le k \le 15$ and $u_1 \in [0,4]$, the system is chaotic. Its chaotic map is shown in **Figure 2**. Compared with the sequence generated by the chaotic mapping in (2), the sequence in (3) is more chaotic and transformable. At the same time, the value range of *k* is increased so that the key space of the encryption algorithm also increases.

After the above improvement, 2.1 effectively increases the substitution variable generated by Joseph's ergodic mapping, and 2.2 effectively enhances the chaos state, transformativeness and the range of *k* of the logistic mapping sequence.

3. Algorithm Description

3.1. Encryption Algorithm Description

At first, the original image is scrambled by using logistic mapping to obtain the encrypted image, then the encrypted image is divided into many blocks. Finally,

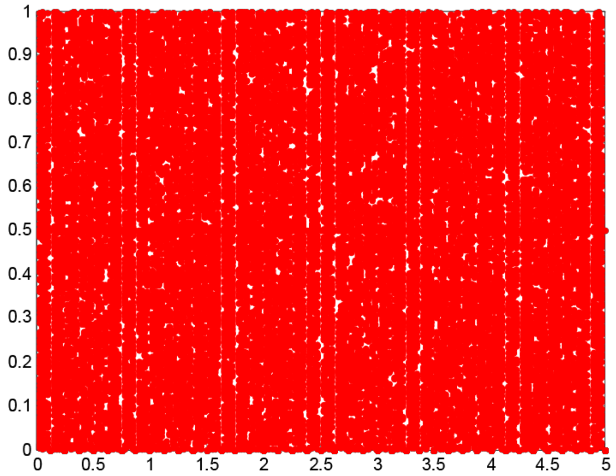


Figure 1. The chaotic map of Equation (2).

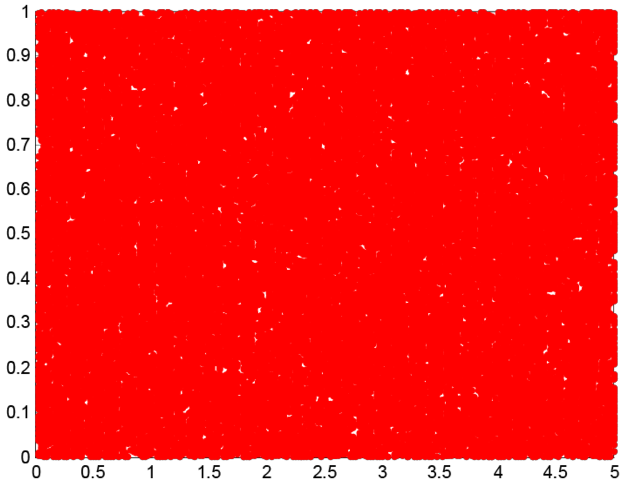


Figure 2. The chaotic map of Equation (3).

the position of the blocked image is scrambled by using the improved Josephus ring to get the encrypted image.

Given a $M \times N$ grayscale image, the encryption steps are described as following:

Step 1: Enter the encrypted grayscale image Q, the size of the image is $M \times N$, let $L = M \times N$.

Step 2: Enter the keys u_1, x_0, k, l, where u_1 is the control parameter of the logistic chaotic map, x_0 is the initial value of the logistic chaotic map, and $x_0 \in (0,1)$, k is the control index of the equation, l is the range of the chaotic sequence converted to an integer and $100 < l < L$. This article take $l = 256$.

Step 3: Generate a L-long chaotic sequence $T = [x_1, x_2 \cdots, x_L]$ by using the formula (3), and then modifies each component x_i of T to obtain the key vector of the sequence $T^1 = [x_1^1, x_2^1, \cdots, x_L^1]$ and the vector T^1 as the image encryption.

Step 4: convert the image Q from $M \times N$ matrix to one-dimensional row vector $B=\left[x_1^2,x_2^2,\cdots,x_L^2\right]$.

Step 5: Exclusive-OR the T^1 and B to obtain another one-dimensional vector $C=\left[x_1^3,x_2^3,\cdots,x_L^3\right]$, and then convert C to an $M\times N$ matrix to obtain the image E^1 encrypted with the improved logistic map.

Step 6: Input m^1,n^1, where m^1 is the pixel of each line after the block, n^1 is the column pixel of each block after the block; and the values of A and B are respectively the factors of M and N. The values of A and B may be the same or different.

Step 7: Partition the encrypted image E^1 to obtain $m^1\times n^1$ matrix of $\left(M/m^1\right)\times\left(N/n^1\right)$ blocks.

Step 8: Enter m, q, where m is the number of the first few to come up with this one, q is the number of intervals.

Step 9: Write $n=\left(M/m^1\right)\times\left(N/n^1\right)$, $C=\left(1,2,\cdots,n\right)$, where $1,2,\cdots,\left(N/n^1\right)$ are the numbering from left to right of $m^1\times n^1$ array in the first row, $\left(N/n^1+1\right),\cdots,2\times\left(N/n^1\right)$ are the numbering of the $m^1\times n^1$ array in the second row from left to right and go on in order .Then all the elements in C are scrambled by the improved Josephian traversal mapping $f_{ysf}^1\left(n,p,m\right)$ to get a sequence C^1.

Step 10: The elements in C^1 (that is, the numbering in step 9) are arranged in a matrix of $\left(M/m^1\right)\times\left(N/n^1\right)$ from left to right in the order of positions in C^1 (Write $X=\left(M/m^1\right)\times\left(N/n^1\right)$, where X is $\left(M/m^1\right)\times\left(N/n^1\right)$ matrix), and then these $m^1\times n^1$ matrix of corresponding number are got into the X to get a disorganized block image.

Step 11: The block image in the tenth step is restored to $M\times N$ image, which is the final encrypted image E.

3.2. Decryption Algorithm Description

Step 1: Input the final encrypted image E in step 11 above.

Step 2: Enter the correct m^1,n^1 to block the encrypted image E.

Step 3: Enter the correct m, q for scrambling the restoration of the block to be restored encrypted image.

Step 4: restoring the restored encrypted block image to an $M\times N$ encrypted image again.

Step 5: Enter the correct key u_1,x_0,k,l, and perform the exclusive-OR operation on the $M\times N$ encrypted image to obtain the decrypted image.

4. Experimental Results and Analysis

4.1. Experimental Platform

PC configuration: Intel (R) Celeron (R) CPU N3450 @ 1.10 GHz 1.10 GHz, memory 4 GB, win 10 64 bit operating system. Through the Matlab R2014a programming to achieve the above encryption algorithm.

4.2. Experimental Results

The experiments selected four grayscale images of lena, baboon, boat and couple, in which the pixel value of the first image was 1024 × 1024 and the pixel values of the remaining images were both 512 × 512. The algorithm of this paper is used to test the selected four images. Figure 3 shows the comparison of plaintext, ciphertext and decrypted images. It can be seen from Figure 3 that the encrypted image has become cluttered and visually distinct from the plaintext image, showing that the algorithm has a good encrypted visual effect and the decrypted image is completely correct, indicating that the algorithm in this paper can correctly implement the role of image encryption and decryption.

4.3. Key Space and Key Sensitivity Analysis

Image encryption algorithm should have enough key space and the sensitivity of key changes, so as to effectively defend against attacks. The key of this algorithm consists of 8 parameters of $u_1, x_0, k, l, m^1, n^1, m, p$, where $u_1 \in (0,4)$, $x_0 \in (0,1)$ and $k \in (5,15)$ are all decimal digits, plus the range of l, m^1, n^1, m and *p*, the key space of this algorithm is more than 10^{37} (calculated with a computer precision of 10^{-15}) and has a good ability to resist attacks. The comparison results with other algorithms are shown in Table 1.

The sensitivity of the key can be divided into the sensitivity of the encryption and the sensitivity of the decryption. In the encryption process, the sensitivity

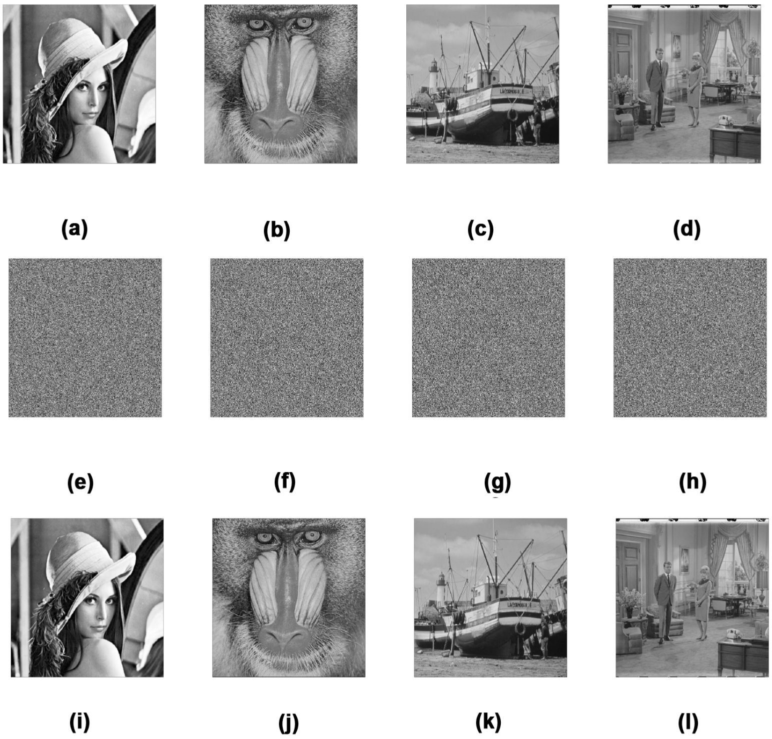


Figure 3. (a) Original lena image; (b) Original baboon image; (c) Original boat image; (d) Original couple image; (e) Encrypted lena image; (f) Encrypted baboon image; (g) Encrypted boat image; (h) Encrypted couple image; (i) Decrypted lena image; (j) Decrypted baboon image; (k) Decrypted boat image; (l) Decrypted couple image.

Table 1. Key space comparison results with other methods.

Methods	Ours	Ref. [9]	Ref. [16]
Key space	10^{37}	2^{106}	1.2×10^{24}

can be reflected by the slight transformation of the key. We use to calculate the rate of change of ciphertext image to reflect the key encryption sensitivity, which is calculated as:

$$CRC = \frac{\sum_{i=1}^{L} Dif\left(E_i, E_i'\right)}{L} \times 100\% \tag{4}$$

where E_i is a ciphertext image encrypted by the initial key, E_i' is a ciphertext image encrypted with a small change of the key, and $Dif\left(E_i, E_i'\right)$ is the number of elements with different pixel values in E_i and E_i'. The following were lena, baboon, boat image as an example.

Figure 4 test the sensitivity of key u_1, Figure 4(a) is the original image of lena, Figure 4(b) is the ciphertext image E encrypted by the keys $u_1 = 3.7$, $x_0 = 0.5$, $k = 9.8$, $l = 256$, $m^1 = 64$, $n^1 = 128$, $m = 3$ and $p = 2$, Figure 4(c) is the encrypted image E' whose key u_1 is changed to 3.70000000000001. By formula (4) calculated the rate of change between the two images was 99.61%. Figure 4(d) is the decrypted image obtained by decrypting E' with the key $u_1 = 3.7$, and Figure 4(e) is the decrypted image obtained by decrypting E' with the key $u_1 = 3.70000000000001$.

Figure 5 test the sensitivity of key x_0. Figure 5(a) is the original picture of baboon, Figure 5(b) is the ciphertext image E encrypted with the key $u_1 = 3.7$, $x_0 = 0.5$, $k = 9.8$, $l = 256$, $m^1 = 32$, $n^1 = 64$, $m = 3$ and $p = 2$. Figure 5(c) is the encrypted image E' whose key x_0 is changed to 0.50000000000001. Through the formula (4) calculated the rate of change between the two images was 99.59%. Figure 5(d) is the decrypted image obtained by decrypting E with the key $x_0 = 0.50000000000001$, and Figure 5(e) is the decrypted image obtained by decrypting E with the key $x_0 = 0.5$.

Figure 6 test the sensitivity of key k. Figure 6(a) is the original picture of the boat, Figure 6(b) is the ciphertext image E encrypted with the key $u_1 = 3.7$, $x_0 = 0.5$, $k = 9.8$, $l = 256$, $m^1 = 32$, $n^1 = 64$, $m = 3$ and $p = 2$. Figure 6(c) is the encrypted image E' whose key k is changed to 9.80000000000001. By formula (4) calculated the rate of change between the two images was 99.61%. Figure 6(d) is the decrypted image obtained by decrypting E with the key $k = 9.80000000000001$, and Figure 6(e) is the decrypted image obtained by decrypting E with the key $k = 9.8$.

Sensitivity analysis of several parameters in the logistic map above, the following parameters m^1, n^1, m, p are used to get on decryption analysis, the experiment chose the classic lena image and only analyzes m^1 and p (the other two parameters n^1 and m were similar to those of m^1 and p).

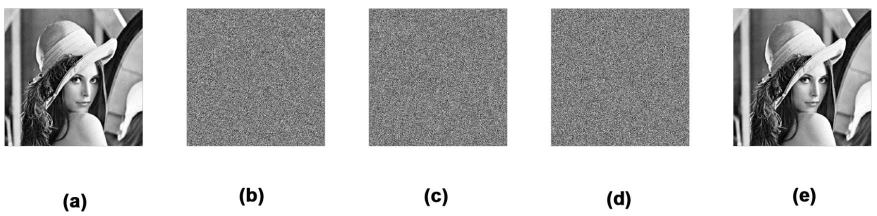


Figure 4. The sensitivity of the key u_1 experimental analysis. (a) Original lena image; (b) Encrypted image E; (c) Encrypted image E'; (d) The wrong key is decrypted; (e) The correct key is decrypted.

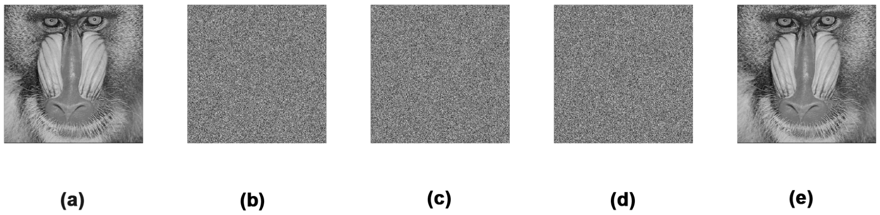


Figure 5. The sensitivity of the key x_0 experimental analysis. (a) Original baboon image. (b) Encrypted image E; (c) Encrypted image E'; (d) The wrong key is decrypted; (e) The correct key is decrypted.

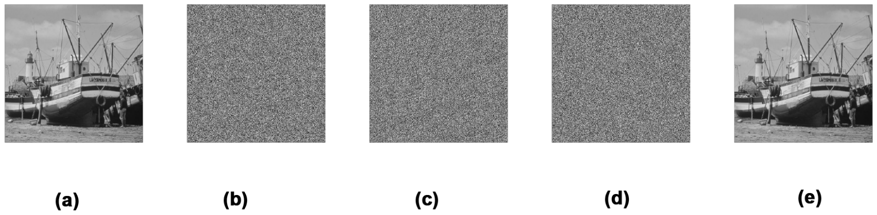


Figure 6. The sensitivity of the key k experimental analysis. (a) Original boat image. (b) Encrypted image E; (c) Encrypted image E'; (d) The wrong key is decrypted; (e) The correct key is decrypted.

Figure 7 test the influences of key m^1 on the decryption process. Figure 7(a) is the original picture of the lena, Figure 7(b) is the ciphertext image encrypted with the key $u_1 = 3.7$, $x_0 = 0.5$, $k = 9.8$, $l = 256$, $m^1 = 64$, $n^1 = 64$, $m = 3$ and $p = 2$, Figure 7(c) is the decrypted image with m^1 changed to 128.

Figure 8 test the influences of key p on the decryption process. Figure 8(a) is the original image of the lena, Figure 8(b) is the ciphertext image encrypted by the key $u_1 = 3.7$, $x_0 = 0.5$, $k = 9.8$, $l = 256$, $m^1 = 64$, $n^1 = 64$, $m = 3$ and $p = 2$, and Figure 8(c) is the decrypted image with p changed to 3.

The experimental results from Figures 4-6 show that the ciphertext changes rate is above 99% even though the key changes slightly in the encryption process. In the process of decryption, even if the key changes slightly, it can not get the correct decryption image. The experimental results from Figure 7, Figure 8 show that when m^1, n^1, m, p are different from the values entered during encryption, only a small portion of small images can be decrypted, however, most other small blocks are not easy to decrypt, which shows that this algorithm has good key sensitivity and encryption effect.

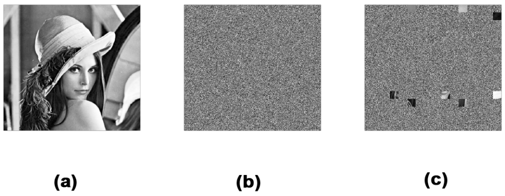


Figure 7. Key m^1 on the decryption process analysis. (a) Original lena image; (b) Encrypted image; (c) m^1 wrongly decrypted image.

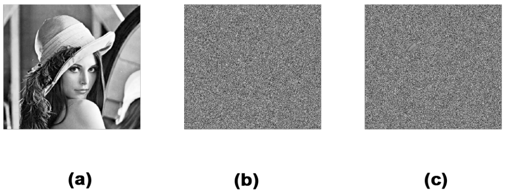


Figure 8. key p on the decryption process analysis. (a) Original lena image; (b) Encrypted image; (c) p wrongly decrypted image.

4.4. Histogram Analysis

Histograms can well reflect the distribution of image pixel values. The smoother the histogram is, the more uniform the pixel values are. Figure 9 shows the histograms of the original image and the encrypted image of the lena and baboon images, respectively.

4.5. Image Encryption Fixed Point Ratio Analysis

According to the literature [3] [20], the fixed point refers to the pixel whose gray value does not change before and after the image is encrypted. The fixed point ratio is the percentage of the fixed point of the image and all pixels, which is calculated as follows:

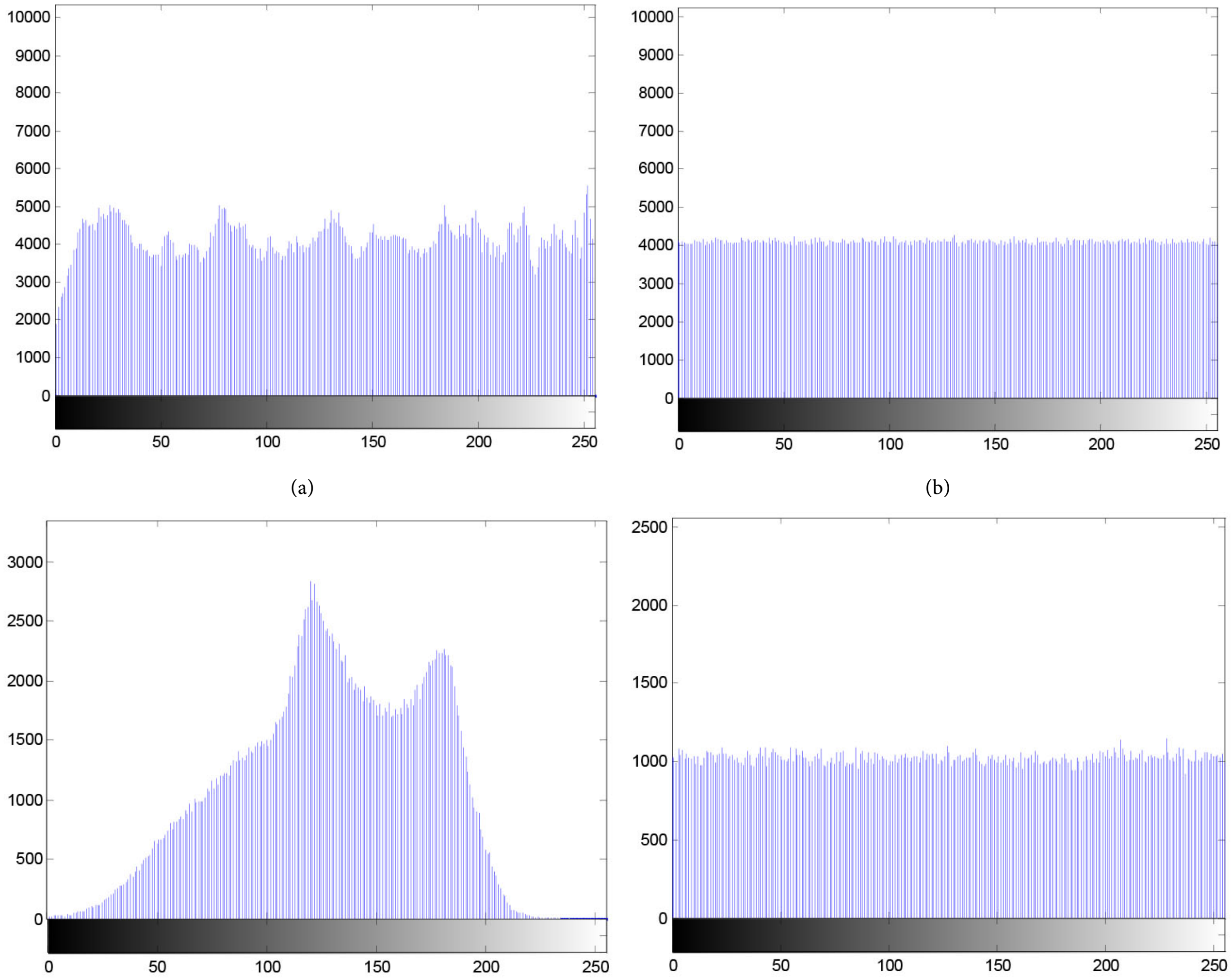
$$BD(G,C)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}f(i,j)}{MN}\times 100\% \tag{5}$$

where $f(i,j)=\begin{cases}1, g_{ij}=c_{ij}\\0, g_{ij}\neq c_{ij}\end{cases}$.

From the formula (5) to calculate the fixed point of the encryption algorithm as shown in Table 2.

4.6 Average Gray Value Change Analysis

After the image is encrypted, the gray value of many pixels will change. The fixed point ratio only reflects the change of the gray level in quantity, but it can not reflect the changed degree of the gray level. Therefore, in order to better evaluate the changed degree of gray-scale of encrypted image, the following gives the average changed value of gray [3] [20]. The formula is as follows:



(a)

(b)

(c)

(d)

Figure 9. Histogram comparison of plaintext image and ciphertext image. Histogram of plaintext lena; (b) Histogram of encrypted lena; (c) Histogram of plaintext baboon; (d) Histogram of encrypted baboon.

Table 2. Encrypted image fixed point ratio analysis table.

Image	All pixels	Fixed point	Fixed point ratio
lena	1,048,576	4014	0.39%
baboon	262,144	1075	0.41%
boat	262,144	1021	0.39%
couple	262,144	974	0.37%

$$GAVE\left(C,G\right)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|c_{ij}-g_{ij}\right|}{MN} \tag{6}$$

where G is a plain text image and C is an encrypted image. According to formula (6) calculate the average gray value of the encryption algorithm changes as shown in Table 3.

Table 3. Average gray value change analysis table.

image	lena	baboon	boat	couple
Average changed value of gray	84.92	71.26	75.05	70.53

4.7. Information Entropy Analysis

Information entropy reflects the distribution of image gray values. The more uniform the gray value of images is, the larger the information entropy of images is. On the contrary, the entropy of information is smaller [20]. Information entropy is calculated as follows:

$$H(G) = -\sum_{i=1}^{L} p(x_i)\log_2(x_i) \tag{7}$$

The information entropy of the original image and the ciphertext image calculated according to formula (7) are shown in Table 4.

4.8. Neighborhood Pixel Correlation Analysis

The correlation of adjacent pixels is used to evaluate the effect of image encryption algorithms in eliminating the correlation of adjacent pixels in a plaintext image. In this paper, 3000 adjacent pixels are randomly selected in the original images and ciphertext images of 4 images. The correlation coefficients of adjacent pixels of the original image and the ciphertext image in the horizontal direction, the correlation coefficients of the adjacent pixels of the original image and the ciphertext image in the vertical direction and the correlation coefficients of adjacent pixels of the original image and the ciphertext image in the diagonal direction are calculated according to the formulas (8) - (11). Table 5 is a comparison table of correlation coefficients between the original image and the encrypted image. In Figure 10, the correlation between the original baboon image and the encrypted image in the horizontal, vertical and diagonal directions is compared.

$$E(x) = \frac{1}{K}\sum_{i=1}^{K} x_i \tag{8}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}\left(x_i - E(x)\right)^2 \tag{9}$$

$$Cov(x,y) = \frac{1}{K}\sum_{i=1}^{K}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{10}$$

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{11}$$

5. Conclusion

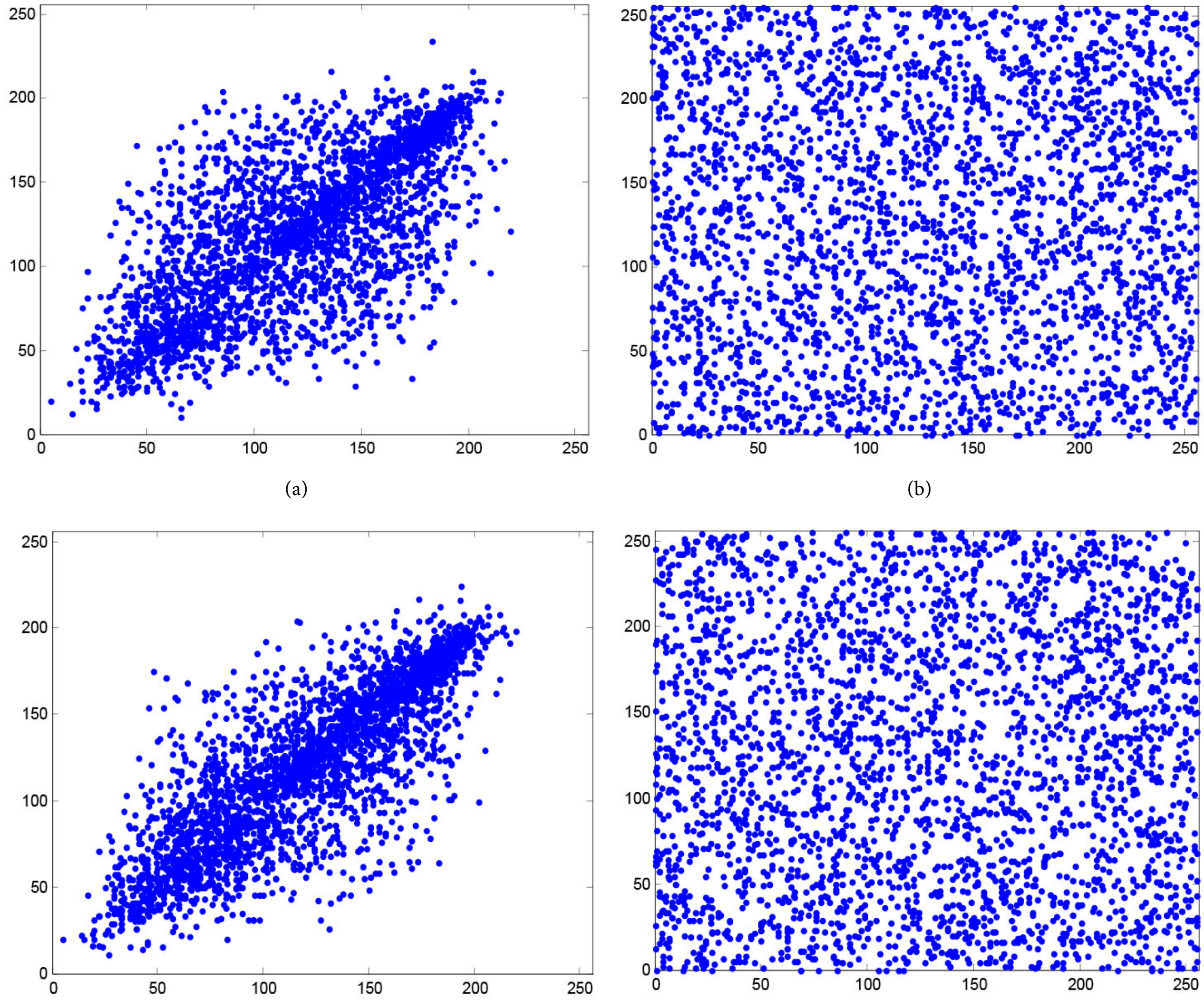
With the rapid development of network technology, how to ensure the security of digital images in storage and transmission has become an important issue in the current information security. The encryption algorithm in this paper is

Table 4. Table of information entropy analysis of original and encrypted images.

image	lena	baboon	boat	couple
The original image	7.9790	7.3713	7.1267	7.2369
Ciphertext image	7.9999	7.9992	7.9991	7.9990

Table 5. Comparison table of correlation coefficient between original image and encrypted image.

Image		lena	baboon	boat	couple
Horizontal correlation coefficient	Original image	0.9991	0.7060	0.9602	0.8284
	Encrypted Image	0.0012	−0.0122	−0.0032	−0.0412
Vertical correlation coefficient	Original image	0.9977	0.8350	0.7954	0.9124
	Encrypted Image	0.0783	−0.0642	−0.0149	0.0261
Diagonal correlation coefficient	Original image	0.9972	0.6983	0.7922	0.7493
	Encrypted Image	0.0372	−0.0064	−0.0016	-0.0339

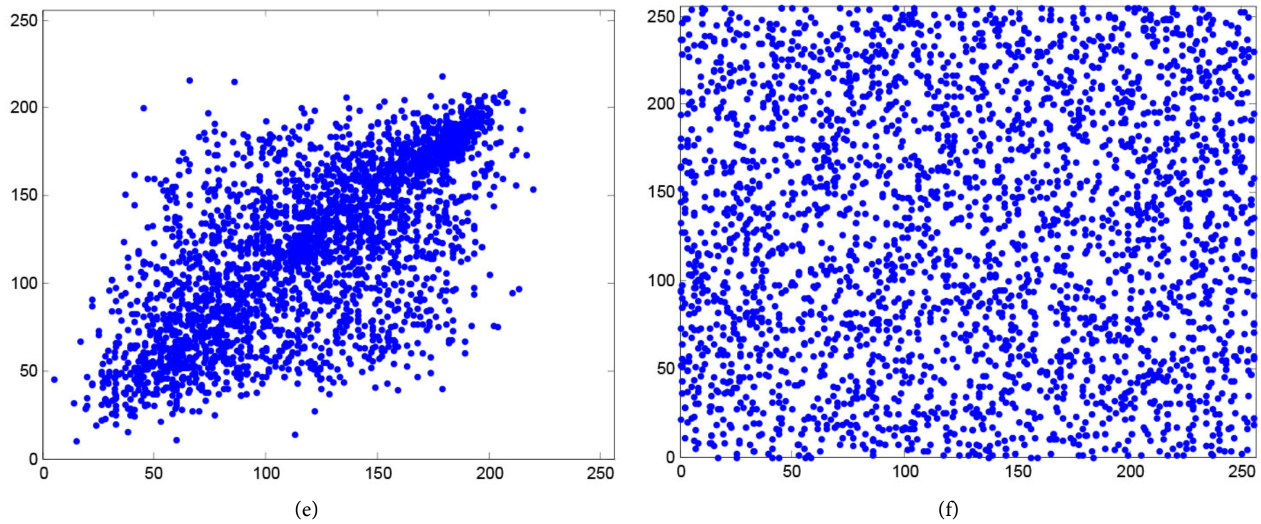


(a)

(b)

(c)

(d)



(e)

(f)

Figure 10. Comparison of the correlation between original baboon image and encrypted baboon image in horizontal, vertical and diagonal directions; (a) Baboon original image horizontal correlation; (b) Horizontal correlation of baboon after encryption; (c) Baboon originalimage vertical correlation; (d) Vertical correlation of baboon after encryption; (e) Baboon original image diagonal correlation; (f) Diagonal correlation of baboon after encryption.

encryption algorithm based on improved Josephus loop and improved logistic mapping to scrambling block. At first, we use logistic mapping to scramble the original image to obtain the encrypted image and then the encrypted image is divided into blocks. Finally, an improved Josephus ring is used to perform the position of the blocked image to get the encrypted image in this paper. By Matlab simulation experiments and the safety of experimental results are analyzed, the results show that the algorithm has the advantages of large key space, high key sensitivity, and can effectively resist the statistical analysis and gray value analysis attacks. So, it has good encryption effect on digital image encryption.

References

[1] Fridrich, J. (1998) Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *Intemational Journal of Bifurcation and Chaos*, **8**, 1259-1284. https://doi.org/10.1142/S021812749800098X

[2] Xu, J.F. and Yang, Y. (2006) Analysis of Scrambling Performance of Encrypted Image. *Neural Computation*, **33**, 110-113.

[3] Guan, Z.H., Huang, F.J. and Guan, W.J. (2005) Chaos-Based Image Encryption Algorithm. *Physics Letters A*, **346**, 153-157.

[4] Xu, B. and Yuan, L. (2014) Research on Image Encryption Algorithm Logistic Chaotic Based on an Improved Digital Mapping. *Computer Measurement & Control*, **22**, 2157-2159.

[5] Li, C.H., Luo, G.C., Qin, K. and Li, C.B. (2016) An Image Encryption Scheme Based on Chaotic Tent Map. *Nonlinear Dynamics*, 1-7.

[6] Li, X., Zhang, G.J. and Zhang, X.Y. (2015) Image Encryption Algorithm with Compound Chaotic Maps. *Journal of Ambient Intelligence & Humanized Computing*, **6**, 563-570. https://doi.org/10.1007/s12652-013-0217-4

[7] Yi, K.X., Sun, X. and Shi, J.Y. (2000) An Image Encryption Algorithm Based on

Chaotic Sequences. *Journal of Computer-Aided Design & Computer Graphics*, **12**, 672-676.

[8] Gou, Y., Shao, L.P. and Yang, L. (2015) Bit-Level Image Encryption Algorithm Based on Josephus and Henon Chaotic Map. *Application Research of Computers*, **32**, 1-7.

[9] Hussain, I. and Gondal, M.A. (2014) An Extended Image Encryption Using Chaotic Coupled Map and S-Box Transformation. *Nonlinear Dynamics*, **76**, 1355-1363. https://doi.org/10.1007/s11071-013-1214-z

[10] El-Latif, A.A.A., Li, L., Zhang, T.J., Wang, N., Song, X.H. and Niu, X.M. (2012) Digital Image Encryption Scheme Based on Multiple Chaotic Systems. *Sensing and Imaging*, **13**, 67-88. https://doi.org/10.1007/s11220-012-0071-z

[11] Khanzadi, H., Eshghi, M. and Borujeni, S.E. (2014) Image Encryption Using Random Bit Sequence Based on Chaotic Maps. *Arabian Journal Forence & Engineering*, **39**, 1039-1047. https://doi.org/10.1007/s13369-013-0713-z

[12] Seyedzadeh, S.M., Norouzi, B., Mosavi, M.R. and Mirzakuchaki, S. (2015) A Novel Color Image Encryption Algorithm Based on Spatial Permutation and Quantum Chaotic Map. *Nonlinear Dynamics*, **81**, 1-19. https://doi.org/10.1007/s11071-015-2008-2

[13] Zhu, H.G., Lu, X.J., Zhang, X.D. and Tang, Q.S. (2014) A Novel Image Encryption Scheme with 2D-Logistic Map and Quadratic Residue. *Journal of Northeastern University* (*Natural Science*), **35**, 20-23.

[14] Liu, R. (2015) New Algorithm for Color Image Encryption Using Improved 1D Logistic. *Open Cybernetics & Systemics Journal*, **9**, 210-215. https://doi.org/10.2174/1874110X01509010210

[15] Elgendy, F., Sarhan, A.M., Eltobely, T.E., El-Zoghdy, S.F., El-Sayed, H.S. and Faragallah, O.S. (2015) Chaos-Based Model for Encryption and Decryption of Digital Images. *Multimedia Tools & Applications*, 1-25.

[16] Pisarchik, A. and Zanin, M. (2008) Image Encryption with Chaotically Coupled Chaotic Maps. *Journal of Physics D*, **237**, 2638-2648. https://doi.org/10.1016/j.physd.2008.03.049

[17] Chai, X. (2017) An Image Encryption Algorithm Based on Bit Level Brownian Motion and New Chaotic Systems. *Multimedia Tools and Applications*, **76**, 1159-1175. https://doi.org/10.1007/s11042-015-3088-1

[18] Norouzi, B. and Mirzakuchaki, S. (2017) Breaking a Novel Image Encryption Scheme Based on an Improper Fractional Order Chaotic System. *Multimedia Tools and Applications*, **76**, 1817-1826. https://doi.org/10.1007/s11042-015-3085-4

[19] Yang, D., Wang, J. and Chen, S. (2017) An Encryption Algorithm Keeping Data Length Unchanged Based on Modified Logistic Map. *Computer Applications and Software*, **34**, 293-298.

[20] Wang, Y., Zhu, W. and Zhan, X. (2006) Study on Scrambling Capability Based on Image Encryption. *Computer Engineering and Design*, **27**, 4729-4731.