Journal of Applied Mathematics and Physics, 2020, 8, 1814-1825
https://www.scirp.org/journal/jamp
ISSN Online: 2327-4379
ISSN Print: 2327-4352

Image Encryption and Decryption Based on Chaotic Algorithm

Yue Hu*, Ruyue Tian

School of Mathematics and Physics, China University of Geosciences, Wuhan, China
Email: *2587607122@qq.com

How to cite this paper: Hu, Y. and Tian, R.Y. (2020) Image Encryption and Decryption Based on Chaotic Algorithm. *Journal of Applied Mathematics and Physics*, **8**, 1814-1825.
https://doi.org/10.4236/jamp.2020.89136

Received: August 14, 2020
Accepted: September 12, 2020
Published: September 15, 2020

Abstract

This paper analyzes the problems in image encryption and decryption based on chaos theory. This article introduces the application of the two-stage Logistic algorithm in image encryption and decryption, then by information entropy analysis it is concluded that the security of this algorithm is higher compared with the original image; And a new image encryption and decryption algorithm based on the combination of two-stage Logistic mapping and *M* sequence is proposed. This new algorithm is very sensitive to keys; the key space is large and its security is higher than two-stage Logistic mapping of image encryption and decryption technology.

Keywords

Chaos Algorithm, Image Encryption and Decryption, Two-Stage Logistic Mapping, *M* Sequence

1. Introduction

The issue of how to protect the security of private information has aroused widespread concern. In April 2016, the European Union promulgated the "General Data Protection Regulation", which provides reference application standards for people's privacy protection [1] [2] [3]. First, Fridrich explored the two-dimensional standard Baker symmetric image encryption algorithm based on chaotic mapping and proposed [4], and has become a key research object of data encryption technology. In 2000, YIT used a chaotic sequence in the DCT domain to generate a key for encrypting [5]. Based on the research of chaos theory and chaotic cryptography, many image encryption algorithms based on one-dimensional chaos, coupled chaos and multi-dimensional chaos have been proposed [6] [7] [8] [9] [10]. In 2015, Fengming Guo and Li Tu used chaotic

sequences as the key to secure communication. It has the advantages of large randomness, good confidentiality, and large key space. In 2016, Dan Cai put the Logistic chaotic mapping into three segments, proposed a piecewise tangent method and performance analysis about it, but did not make it applied in image encryption [11].

Logistic chaotic map has a simple structure and good performance. It is currently a widely used chaotic map. In order to better improve the performance of Logistic mapping, some scholars have proposed an improved Logistic mapping on this basis [12]. Compared with the original map, this improved map can enter the chaotic state earlier, and the correlation characteristics are more ideal.

However, this improved Logistic mapping still has some shortcomings in sequence ergodicity and randomness. We hope that this method can be improved to find a safer and faster encryption algorithm.

2. Related Basic Theories

2.1. Lyapunov Exponent

The Lyapunov exponent represents the numerical characteristics of the average exponential divergence rate of adjacent trajectories in phase space. It is one of the features used to identify several numerical values of chaotic motion. The Lyapunov index calculation formula in the form of

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{n=0}^{N-1} \ln \left| \frac{\mathrm{d}f\left(x_n, u\right)}{\mathrm{d}x} \right| \tag{2.1}$$

When $\lambda > 0$, the system motion will enter a chaotic state, the corresponding map is called a chaotic map, and the system diverges along the trajectory;

When $\lambda < 0$, the movement state of the system will tend to be stable and insensitive to the initial state of the system at this time, the system converges along the direction of the trajectory;

When $\lambda = 0$, the system is in a stable state, neither converging nor diverging.

Whether the system is a chaotic system can be judged by the value of Lyapunov exponent in the dynamic system and the state of the system trajecto.

2.2. Cryptography Theory

Shannon's information theory has proved that only the "one word, one password" cryptosystem is a completely secure secret system. Only by processing the plain text of the encrypted message through this key can each bit after encryption be made. The ciphertext is not regular. It is precisely because of this ciphertext that there is no law to follow that will prevent the attacker or the decipherer from finding the law from all kinds of information they already know, so that they have no way to decrypt the encrypted ciphertext, so as to ensure the security of the password system.

But the above statement only exists in theory, and the keys we use in actual encryption systems are pseudo-random sequences generated by software or hard-

ware. This generated pseudo-random sequence is always no matter how long it is. It is periodic, not really random. Periodicity means that it has certain rules to follow, but since the period of chaotic systems is infinite, we can study cryptography based on chaotic algorithms.

2.3. The Application of the Chaos Theory in Cryptography

Existing research shows that the chaotic sequence generated by the chaos system is a nonlinear sequence, its structure is complex and difficult to analysis and forecast, it also has good randomness, correlation and complexity, so it can be as a chaotic encryption key sequence. For "a word a secret" encryption algorithm, chaotic sequence is a good key sequence, it can serve as a kind of practical password system.

Chaos is a complex dynamic behavior produced by a nonlinear system. Due to its extreme sensitivity to initial conditions, chaotic systems can generate a large number of uncorrelated chaotic sequences with pseudo-random characteristics. The basic principle of chaotic encryption is to use the chaotic sequence generated by the chaotic system to encrypt the plaintext to obtain the ciphertext. After transmission, the receiver constructs the same chaotic system as the sender through chaotic synchronization, and finally extracts the plaintext from it to decrypt it. It is this extremely sensitive dependence on initial value conditions and parameters that make chaos occupy an extremely important position in secure communication systems. Compared with traditional ciphers, chaotic sequences have many excellent cryptographic features, such as being difficult to be attacked and extremely difficult to crack. These characteristics have greatly improved the security performance of encryption and decryption work.

2.4. Chaos Encryption Principle

Chaotic encryption with traditional cryptography have a lot in common, the chaos encryption password can be divided into chaos sequence and chaotic block cipher.

After dealing with the chaos system formed by the sequence of code with high efficiency, can make clear statistical characteristics were disrupted and transmission error is zero, so for now using the password in the form, sequence password has a very important position [13].

Chaotic block ciphers are more widely used in real life. Because block ciphers are easier to standardize, in ordinary digital communication systems, information is first divided into blocks before being transmitted, and block ciphers are easier to synchronize, so this style of cipher is more widely used than chaotic sequence ciphers. Chaotic packet encryption is a kind of encryption method that uses plain text or key as the initial condition or parameter, and forms cipher text after many iterations or reverse iterations.

Chaotic mapping in the application of the block cipher is by using the iterative nature of chaos for rapid scrambling image data [14]. In general, when designing block ciphers, it is mainly to iterate the plaintext information that needs to be

encrypted many times, so as to achieve the effect of completely scrambling the plaintext messages. The following will introduce two types of chaotic block ciphers: image encryption and decryption based on two-stage logistic mapping and a new image encryption and decryption algorithm based on the combination of two-stage Logistic mapping and M sequence.

3. Image Encryption Technology

3.1. Image Encryption and Decryption Algorithm Based on Two Sections of Logistic Mapping

3.1.1. Overview of the Logistic Mapping

Chaos theory is widely used in data encryption. Among them, Logistic chaotic mapping is one of the most commonly used models. The Logistic equation, also known as the wormhole model [14], is an American ecologist May R. It was proposed in 1976. At that time, the Logistic equation was used to analyze the relationship between the number of individual insect populations and environmental factors. It was a particularly simple but important one-dimensional nonlinear equation. The Logistic equation is shown in 3.1.

$$x_{k+1} = \gamma x_k \left(1 - x_k\right) \tag{3.1}$$

Among them $x_k \in [0,1], k = 0,1,\cdots,n$, γ is the branch parameter, $\gamma \in (0,4]$.

If the branch parameter γ take different values, the system 3.1 will show different characteristics. In the ever-increasing branch parameters γ, the system will continue to experience period-doubling bifurcations and eventually reach the state of chaos [15].

Logistic mapping Lyapunov index spectrum has obtained by simulation, as shown in Figure 1.

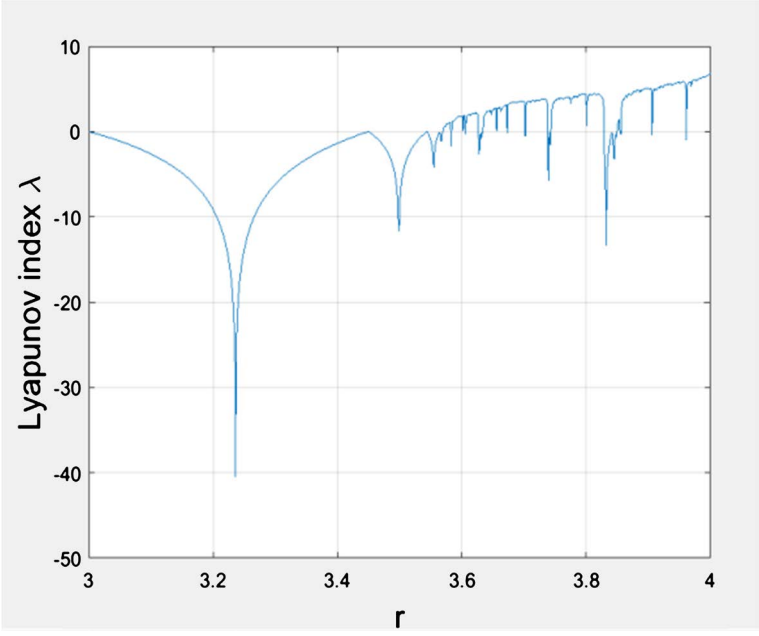

Figure 1. Logistic mapping Lyapunov index spectrum.

From Figure 1 we can see, when the parameters $\gamma > 3.56$, Lyapunov index started to be positive, system started to cycle times. along with the continuously raised large parameter γ, positive Lyapunov index increased gradually, system in the phase space trajectory for the dispersion, system gradually into chaotic state.

Logistic chaotic map has simple expression and excellent performance, and is one of the most commonly used chaotic maps. In most of the related algorithms, People take advantage of the simple structure and convenient implementation of one-dimensional Logistic chaotic mapping. Although Logistic maps have the advantages of cryptography such as randomness, due to their small key space and low sequence complexity coefficient, the encrypted cryptosystem is less secure. Although high-dimensional chaotic mapping can make up for these defects to a certain extent, the amount of calculation is particularly complicated. Therefore, many scholars are looking for ways to improve the small key space and low sequence complexity of Logistic mapping [16].

3.1.2. Overview of Two-Stage Logistic Mapping

In this paper, the two-stage Logistic chaotic map proposed by Xuefeng Zhang and Jiulun Fan is adopted [12] and applied to image encryption.

Two-stage Logistic mapping is defined as:

$$x_{k+1} = \begin{cases} 4\gamma x_k (0.5 - x_k) & 0 \le x_k < 0.5, \\ 1 - 4\gamma x_k (x_k - 0.5) & 0.5 \le x_k \le 1. \end{cases}$$

Among them, the initial value $x_0 \in (0,1)$, $\gamma \in [0,4]$.

The Lyapunov exponent spectrum of two-stage Logistic map was obtained through simulation, as shown in Figure 2.

It can be clearly seen from Figure 2 that Lyapunov exponent appeared positive

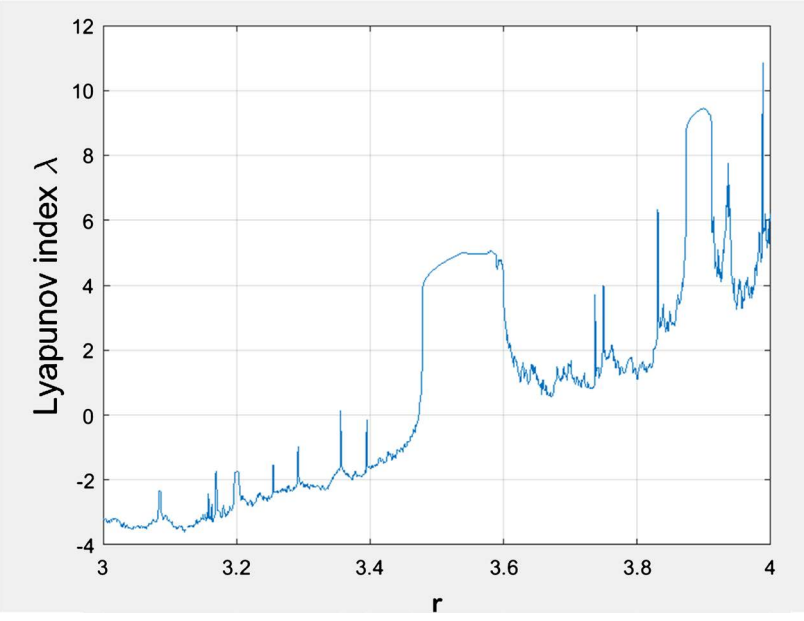

Figure 2. Two-stage Logistic map.

value before $\gamma = 3.5$, and with the continuous increase of parameters, the positive Lyapunov exponent became more and more, so the system soon entered a chaotic state.

By analyzing Figure 1 and Figure 2 and comparing the Lyapunov index spectrum of the original Logistic map and the improved two-stage Logistic map, it can be concluded that the improved mapping has better ergodicity, larger key space, and enters into chaotic state earlier than the original mapping. Therefore, the two-stage Logistic map is more suitable for image encryption.

3.1.3. Image Encryption and Decryption Technology of Two-Stage Logistic Map

A. Solving steps

1) Matlab pretreatment

First, reading the color image data stored on the PC's hard drive, so in Matlab it enters the system as a matrix. Then, the original image will be converted into gray image (this paper only researches gray image encryption algorithm). And display the image and image histogram (the purpose is to be able to observe change of image histogram before encryption and after decryption, it can be easy to clear and intuitive analysis of the image encryption and decryption processing effect).

2) Display the image and histogram of the image before encryption

3) Image encryption

i) Selecting two-stage Logistic mapping and making it chaotic, using it as the key for image encryption processing algorithm. Setting the parameters of the selected chaotic map: taking $\gamma = 3.99, x_0 = 0.41$.

ii) Cutting the image into N whole pieces (the parts that do not satisfy the whole piece are filled with zero elements).

iii) Scrambling the pixel position of the image.

iv) One diffusion transformation after one scrambling transformation.

v) Skipping to Step iii) and looping through Steps iii) and iv).

4) Displaying the encrypted image and image histogram

5) Image decryption

This step is the exactly opposite of the encryption process, but the keys (that is the mixed and scrambled parameters) must be exactly the same.

B. Experimental simulation

In Matlab, the image encryption and decryption technology of two-stage Logistic mapping is used to encrypt and decrypt a digital image. To make it chaotic, we take $\gamma = 3.99, x_0 = 0.41$. The experimental results are shown in Figure 3.

C. Information entropy analysis

For image encryption, if the information entropy is higher, the grayscale distribution in the image will be more symmetrical, the attacker will get less relevant image information from the grayscale distribution, and the image encryption technology will be more secure.

According to the experimental results in Figure 4, it can be clearly seen that

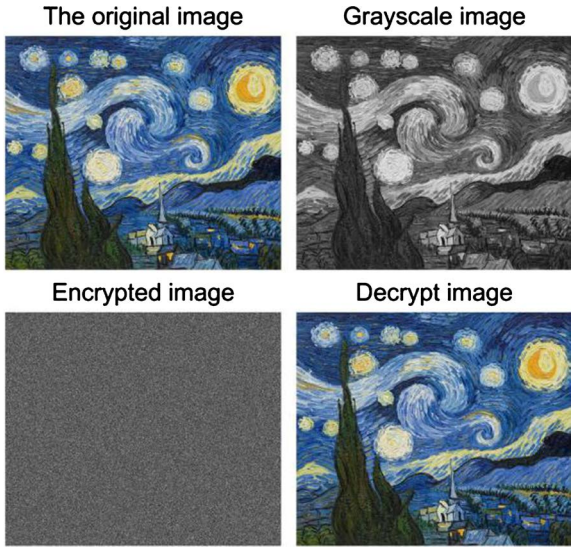

Figure 3. Results of two-stage Logistic algorithm.

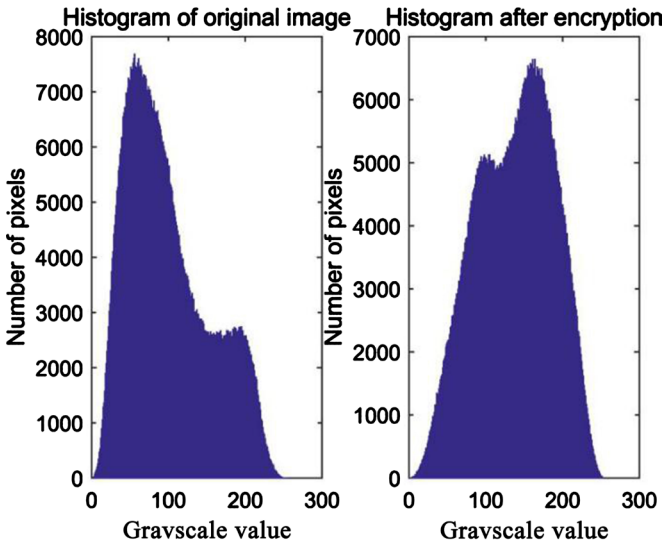

Figure 4. Histogram analysis.

compared with the original image histogram, the image histogram after encryption processing is more symmetrical. Therefore, the image encrypted by two-stage Logistic mapping encryption technology has better concealment in the transmission process.

3.2. Image Encryption and Decryption Algorithm Based on the Combination of Two-Stage Logistic Map and *M* Sequence

3.2.1. Overview of *M* Sequence

In this paper, the *M* sequence transformation in [17] is adopted, which can be used to effectively shuffle the position of the image. The *M* sequence transformation in this paper is very different from the *M* sequence used in other literatures for image encryption. It uses the ergodic property of shift register state in the *M* sequence generator for position displacement. At the same time, the pseudo

random property of M sequence is used to realize image position scrambling. Image replacement is to change the value of each pixel in the image so that the image histogram of the replaced image is similar to that of the image composed of random sequences. This method can effectively disorganize the image, and further reduces the correlation of the image after the replacement processing, thus better protect the image data.

Although M sequence transformation has many excellent encryption features, from the perspective of security analysis, this sequence cipher is easy to be cracked under known plaintext attack, resulting in information leakage, so M sequence transformation cannot be used as a key directly. Therefore, on the basis of the encryption algorithm of M sequence transformation, combined with the nonlinear method that is the two-stage Logistic mapping algorithm mentioned above, they can give full play to the superiority of the key. On the premise of improving security, this paper proposes a new image encryption and decryption algorithm based on the combination of two-stage Logistic map and M sequence.

3.2.2. Image Encryption and Decryption Technology Combining Two-Stage Logistic Map with *M* Sequence

A. Solving steps

Encryption process:

1) Enterring the image to be encrypted. Matrix $f(i,j)$ is used to represent the image, where $i=0,1,\cdots,M-1$; $j=0,1,\cdots,N-1$. Let the number of iterations be a.

2) Input the initial value x_1, x_2 and branch parameter γ_1, γ_2 of the two-stage Logistic chaotic map, and use Formula (2) to iterate the two-stage Logistic chaotic map $MN+1$ times, so as to generate Two different matrices $g_1(i,j)$ and $g_2(i,j)$, among them $0 \le i \le M-1$, $0 \le j \le N-1$.

3) Replacing the gray value of the image; The image $f(i,j)$ is replaced with the gray value of the image point by point according to formula (3), another image matrix can be obtained, denoted as $f_1(i,j)$, where L is the gray level of the image.

$$f_1(i,j)=\left(f(i,j)+ig_1(i,j)+jg_2(i,j)\right)\bmod(L)$$

4) Randomly selecting a pair of parameters x_0', y_0', and imaging displacement position processing: according to the chapters mentioned before m transformation of image matrix $f_1(i,j)$ for replacement operation processing, so acquiring another image matrix $f_2(i,j)$.

5) Carrying out a iteration for 3) and 4), and finally obtaining the encrypted image.

Image decryption is the reverse operation of the encryption process, and the same key is used, so this article will not be described too much.

B. Experimental simulation

In MATLAB, a digital image is encrypted and decrypted using the image encryption and decryption technology combining two-stage Logistic mapping and

M sequence. Among them $x_1 = 0.41$, $x_2 = 0.87$, $\lambda_1 = 3.99$, $\lambda_2 = 3.8$, $x_0' = 10$, $y_0' = 2$, $\gamma = 1$. The experimental results are shown in Figure 5.

C. Performance analysis

1) Sensitivity analysis

In the experiment in Figure 6 and Figure 7, on the premise that all other parameters and initial values are the same, an initial value or parameter of the chaotic system is changed, and the simulation results cannot restore the original encrypted image correctly. This indicates that the algorithm combining two-stage Logistic map with M sequence is particularly sensitive to the initial value and system parameters. Therefore, even if the attacker knows some of the initial values and parameters, the image cannot be decrypted and restored correctly when the exact key used for encryption is not known.

2) Information entropy analysis

According to the experimental results in Figure 8, it can be clearly seen that compared with the histogram of the original image, the image histogram after

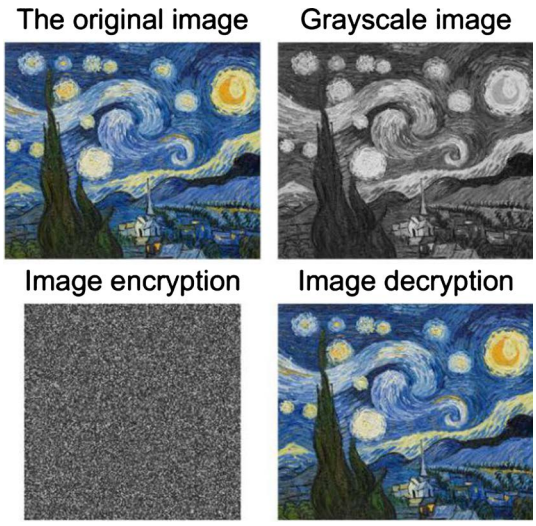

Figure 5. Image encryption and decryption results.

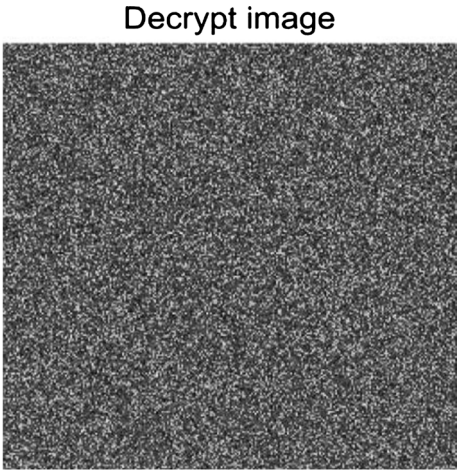

Figure 6. $\lambda_1 = 3.9900001$.

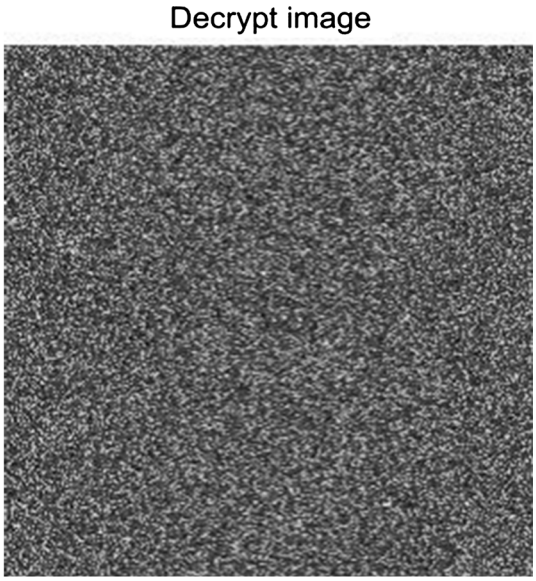

Figure 7. $x_1 = 0.4100001$.

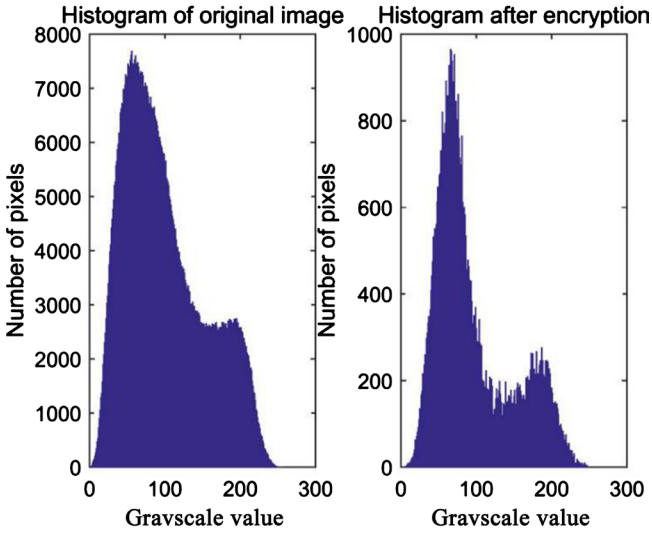

Figure 8. Histogram comparison.

encryption processing is more symmetrical. Compared with the previous two-stage Logistic algorithm encryption and decryption technology is also more secure. Therefore, the image encryption and decryption technology combined with two-stage Logistic mapping and *M* sequence has better concealment in the transmission process.

4. Conclusions

This paper introduces the application of two-stage Logistic algorithm in image encryption and decryption and verifies that it is securer than the original image through information entropy. This paper proposes a new image encryption and decryption algorithm based on the combination of two-stage Logistic map and *M* sequence. In summary, this algorithm has the following advantages:

1) The state of the shift register in the *M* sequence generator is ergodic (except the zero state), and the *M* sequence transformation used in image position displacement can achieve very good effect quickly.

2) This algorithm is highly sensitive to the key, and is securer than the image encryption and decryption technology of two-stage Logistic mapping.

3) Due to the introduction of positional parameters in the replacement of image pixel values, making the initial values have parameter sensitivity, overcoming the shortcomings of *M* sequence transformation, and the image encryption algorithm designed in this paper meets the requirements of modern cryptosystems.

4) The speed of two-stage Logistic mapping into chaos is relatively fast, which makes the key space huge.

Acknowledgements

I would like to acknowledge Professor Zhouchao Wei for his kindly help and comments. I would like to acknowledge funding of the Undergraduate Innovation and Entrepreneurship Program. Project number is 201910491046.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Zheng, M.Y., Xu, D.X., Jiang, L.S., Gu, C.J., Tan, R. and Cheng, P. (2019) Challenges of Privacy-Preserving Machine Learning in IoT. *Proceedings of the* 1*st International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things*, New York, November 2019, 1-7. https://doi.org/10.1145/3363347.3363357

[2] Bertino, E., Choo, K.K.R., Georgakopolous, D. and Nepal, S. (2016) Internet of Things (IoT): Smart and Secure Service Delivery. *ACM Transactions on Internet Technology*, **16**, Article No. 22. https://doi.org/10.1145/3013520

[3] Panah, A.S., Yavari, A., Van Schyndel, R.G. and Geogako, D. (2019) Context-Driven Granular Disclosure Control for Internet of Things Applications. *IEEE Transactions on Big Data*, **5**, 408-422. https://doi.org/10.1109/TBDATA.2017.2737463

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

[5] Yi, K.X., Sun, X. and Shi, J.Y. (2000) An Image Encryption Algorithm Based on Chaotic Sequences. *Journal of Computer Aided Design and Computer Graphics*, **12**, 672-676.

[6] Pareek, N.K., Patidar, V. and Sud, K.K. (2005) Cryptography Using Multiple One Dimensional Chaotic Maps. *Communications in Nonlinear Science and Numerical Simulation*, **10**, 715-723. https://doi.org/10.1016/j.cnsns.2004.03.006

[7] Pareek, N.K., Patidar, V. and Sud, K.K. (2006) Image Encryption Using Chaotic Logistic Map. *Image and Vision Computing*, **24**, 926-934. https://doi.org/10.1016/j.imavis.2006.02.021

[8] Tong, X.J. and Cui, M.G. (2009) Image Encryption Scheme Based on 3d Baker with Dynamical Compound Chaotic Sequence Cipher Generator. *Signal Processing*, **89**, 480-491. https://doi.org/10.1016/j.sigpro.2008.09.011

[9] Wang, X.-Y. and Yu, Q. (2009) A Block Encryption Algorithm Based on Dynamic Sequences of Multiple Chaotic Systems. *Communications in Non-Linear Science and Numerical Simulation*, **14**, 574-581. https://doi.org/10.1016/j.cnsns.2007.10.011

[10] Pisarchik, A.N. and Zanin, M. (2008) Image Encryption with Chaotically Coupled Chaoticmaps. *Physics D*: *Nonlinear Phenomena*, **237**, 2638-2648. https://doi.org/10.1016/j.physd.2008.03.049

[11] Cai, D., Ji, X., Shi, H. and Pan, J. (2016) Improved Piecewise Logistic Chaotic Mapping Method and Its Performance Analysis. *Journal of Nanjing University* (*National Academy*), No. 5, 809-815. (In Chinese)

[12] Deng, L. (2005) Chaotic Synchronization and Its Application in Secure Communication. Chongqing University, Chongqing. (In Chinese)

[13] Huang, R. (2000) Chaos and Its Application. Wuhan University Press, Wuhan. (In Chinese)

[14] Yin, X. (2008) Embedded Ranging System in Ism Ban. *Electronics Letters*, **44**, 1043. https://doi.org/10.1049/el:20081157

[15] Pang, Z. (2017) Digital Image Encryption and Decryption System Based on Chaos Algorithm and Matlab Simulation. Master's Thesis, Kunming University of Science and Technology, Kunming.

[16] Ni, Y. (2017) Research on Adaptive Image Encryption Algorithm Based on Segmented Logistic Chaotic Mapping. Master's Thesis, Anhui University, Hefei.

[17] Liu, J., Huang, X., Zhu, C. and Lu, W. (2007) Image Encryption Algorithm Based on M Sequence Transformation and Chaotic Mapping. *Journal of Electronics and Information Technology*, No. 6, 1476-1479. (In Chinese)