International Core Journal of Engineering Volume 7 Issue 7, 2021
ISSN: 2414-1895 DOI: 10.6919/ICJE.202107_7(7).0060

Summary of Chaotic Image Encryption

Yilin Han, Ye Tao*, Wenyu Zhang

School of Computer and Software Engineering, University of Science and Technology Liaoning, Anshan, 114051, China.

Abstract

In order to further study image encryption based on chaos. Firstly, this paper introduces the core disciplines--cryptography in the field of information security and expounds the definition of chaos. Then the encryption flow and shortcomings of the traditional chaotic image encryption algorithm are analyzed. Besides the research status of chaotic image encryption and the achievements and problems in the application of chaos in image encryption are described. Finally, the future development prospect of chaotic image encryption technology and the significance of improving the security of image encryption algorithm are explained.

Keywords

Cryptography; Chaos; Image Encryption.

1. Introduction

Since ancient times, information security has been a sensitive and important topic for people. At the same time, it has always been the focus of the military and diplomatic departments of various countries. Especially since entering the 21st century, with the rapid development of science and technology, the development of computer network technology in China is very rapid [1]. Multimedia communication technology has also become a hot topic in the development of science and technology. In this era of information globalization, digital multimedia can easily copy, store and communicate through the network. Because of the large-scale use of digital images on the Internet, especially when digital images have important confidential information, it is necessary to encrypt them before the channel transmission is not guaranteed to be very secure [2]. And because some of the information involves personal privacy, copyright and other security reasons, users do not want this information to be viewed by unauthorized people. Therefore, ensuring information security is essential. Data encryption technology is the basis of information security, many other information security technologies are based on data encryption technology. In the image, text, data, audio and many other multimedia carriers, image information can cover more information more comprehensively than text, audio and so on. At the same time, if the image is made into the form of video, it can better transmit and express information. Therefore, digital image information security becomes an important part of information security, reliable and secure image processing has become one of the important research directions. Each image we see is thought to consist of discrete pixels, if a picture is constantly magnified, we can see a small square, which combines to form the image we usually see. If we regard the image as a two-dimensional matrix, then image encryption is to transform the matrix to achieve the purpose of encryption. In the current research on image encryption, most of the research on image protection is to use ciphertext at the transmission and receiving end, and then decrypt it by key [3]. The two most common methods of image encryption include confusion and diffusion. Confusion refers to disrupting the original position of the pixel value in the binary matrix.Common methods include sorting, cyclic shift, Arnold transformation, magic square transformation and so on. Diffusion refers to a small change in the pixel value in the initial image, which will bring great changes to the pixels of the whole image.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202107_7(7).0060

However, due to the large amount of data, high redundancy and high correlation of data points, the traditional encryption method has low efficiency and poor security. However, the characteristics of chaotic mapping, such as initial value sensitivity, ergodicity, short-term predictability and long-term unpredictability, are widely used in digital image encryption.

2. Cryptography

As the foundation of information security, cryptography is also the core technology of information security [4]. Conventional cryptography is mainly focused on text encryption, its typical encryption methods are DES, IDEA, AES and other classical algorithms [5-7]. The basic requirements of modern information security include: confidentiality, integrity, availability and non-repudiation of information. And the encryption methods we now use include:

1 Symmetrical encryption: Is encryption and decryption can use the same key cryptographic technology [8]

2 Asymmetric encryption: It is used to solve the problem that the key may be intercepted by a third party in symmetric encryption. It is divided into public key and private key. The public key domain is a pair of private keys. If the data is encrypted with a public key, only the corresponding private key can be decrypted. The key of encryption and decryption is different.

3 Hash function: Is a one-way function. Is generally used to verify the integrity of certain data.

4 Digital signature: It is a combination of hash and asymmetric encryption, which has great advantages for verifying the integrity and non-repudiation of information.

3. Traditional chaotic image encryption

Chaos originated in 1961, when meteorologists Lorenz a calculation for weather prediction.In this experiment, he abandoned the initial values of a set of data and then brought them back into computer operations but there is a big gap between the results and the calculation after the initial value is fully input. This phenomenon began to attract Lorenz attention, and in 1963 he completed the establishment of the Lorenz equation, which is now considered the first mathematical description of chaos [9]. This phenomenon began to attract Lorenz attention, and in 1963 he completed the establishment of the Lorenz equation, which is now considered the first mathematical description of chaos [10]. This phenomenon is widely found in nature, such as changes in the ocean, changes in the atmosphere, changes in stocks, etc [11]. Chaos is characterized by its sensitivity to initial conditions, good pseudo-randomity and divergence of motion trajectories. It is consistent with the requirement of cryptography for encryption, combining with the birth of chaotic cryptography [12-16]. Because the principle of chaos is of great help to the encryption of digital images, it has been widely used in digital image encryption.

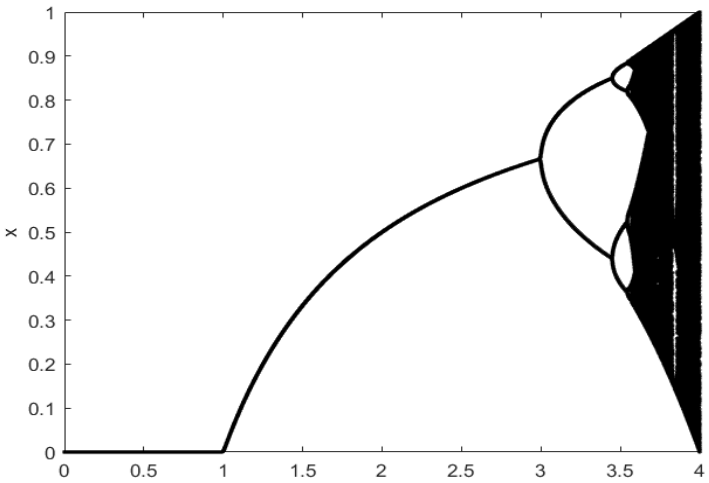


Figure 1. Logistic Mapping Forked Images

ISSN: 2414-1895 DOI: 10.6919/ICJE.202107_7(7).0060

3.1 Logistic chaos mapping:

Logistic mapping, also known as worm mapping, is a parabolic mapping [17]. It has a good encryption effect. And the statistical characteristics of the original image can be hidden well, and the attack based on image pixel value has a good defense function.

Logistic mapping bifurcation images are shown in Figure 1.

Encryption process of chaotic Logistic mapping:

The original image waiting to be encrypted is fed into a chaotic sequence by the encryption key, Through a series of encryption algorithms designed by chaotic system, image encryption is realized. By inputting the decryption key into the system, the decryption image of the encrypted image can be obtained by reverse operation encryption process as shown in figure 2.

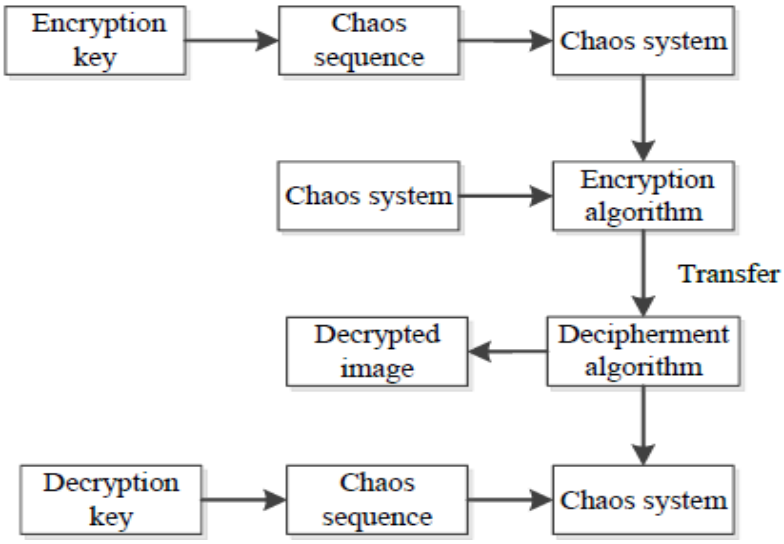


Figure 2. Encryption flow of chaotic Logistic mapping

3.2 Image encryption based on grayscale replacement

Taking into account the good randomness of the sequence generated by iterative calculation of chaotic systems, in 1990, Matthews presented an image encryption algorithm based on one-dimensional Logistic chaotic mapping. The algorithm uses Logistic mapping to set different initial conditions to generate chaotic sequences. The pixel gray value of digital image is replaced by stream cipher structure to encrypt digital image. Then the decryption key is input into the system, and the decryption image of the encrypted image can be obtained by reverse operation encryption process.

R, G, B part of the digital image, using S box transformation for preprocessing. The two-dimensional matrix of the initial gray value of the image is obtained and converted into the one-dimensional matrix required by the encryption algorithm [18]. The encryption process is shown in figure 3.

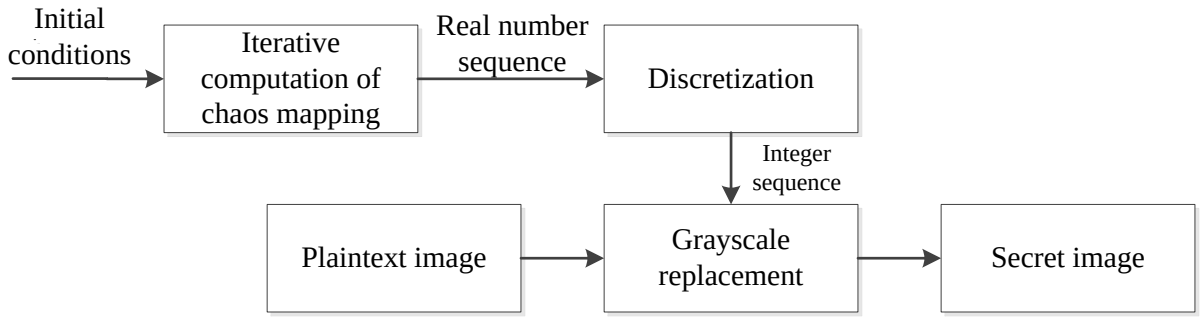
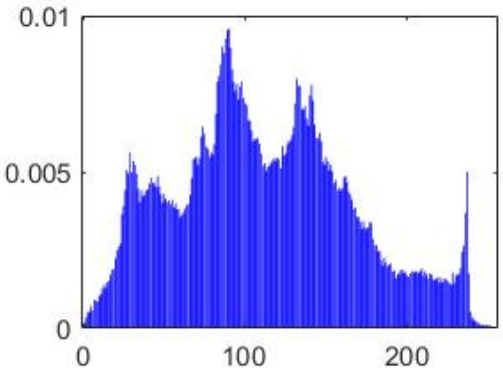


Figure 3. Image Encryption Process Based on Grayscale Replacement

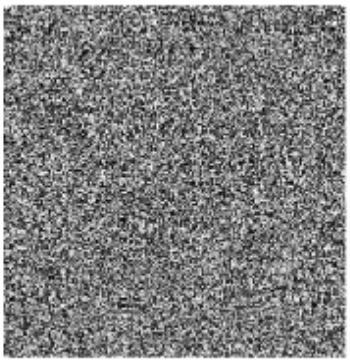
ISSN: 2414-1895 DOI: 10.6919/ICJE.202107_7(7).0060

The encryption effect diagram is shown in figure 4.

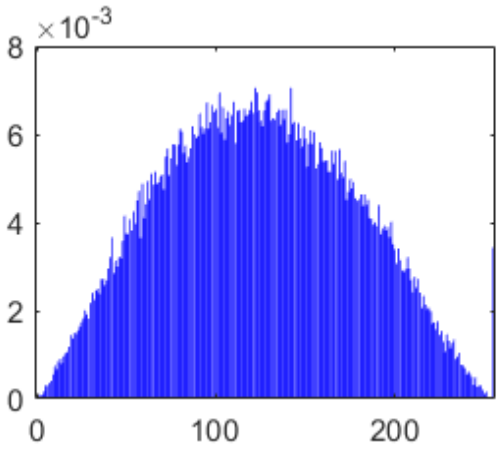
(a) Original image



(b) Histogram of the original image



(c) Encrypted images



(d) Image histogram after encryption

Figure 4. Encryption Effect

Due to the limitation of the accuracy of the computer, the chaotic sequence generated by eventually degenerate into periodic sequence, which may lead to some security problems. In addition, image encryption of stream cipher mechanism can not resist known plaintext and selected plaintext attacks. But because the encryption algorithm can scramble the pixel gray value of the original image, therefore, this encryption operation can be used as a basic operation of image encryption to design complex image encryption algorithm.

3.3 Image encryption based on pixel scrambling

A typical pixel scrambling encryption technique is scrambling encryption based on Arnold mapping. Arnold chaos mapping is also called cat mapping. Aronld can change the pixel position or value of a two-dimensional image, will turn the image into a completely different image. Aronld mapping is the scrambling of pixels by changing the location of elements. In addition, the principle of this mapping is very simple and easy to implement, so it is widely used in digital image encryption technology.

The transformation of the Aronld is to do the x axis direction staggered transformation according to the order, then the y axis direction staggered transformation, the final mode operation is equivalent to the cutting backfill operation. The Aronld inverse transformation method makes the recovery of Aronld transform scrambled image no longer need to calculate the period of image transformation, and can be restored to any secondary scrambling effect of image. The recovery efficiency of the image is greatly improved.

However, due to the periodicity of scrambling transformation, the encryption algorithm can not provide a very efficient guarantee for image security. At the same time, the image encryption process

ISSN: 2414-1895 DOI: 10.6919/ICJE.202107_7(7).0060

of scrambling operation is also a linear operation, so the image encryption technology is the same as the image encryption algorithm of gray level transformation, which can not effectively resist the attacks of known plaintext and selected plaintext.

3.4 Cyclic Iteration Image Encryption

Shannon showed in his paper in 1949 that confusion and diffusion are the basic principles for cryptographic security. For example, many modern cryptographic algorithms, such as DES,AES, use cyclic processes, and each round of encryption contains two basic operations: replacement and scrambling. In recent years, many researchers have used cyclic iterative design block cipher systems, A variety of cyclic iterative image encryption algorithms based on different chaotic systems are designed [19].

Its basic structure is shown in figure 5.

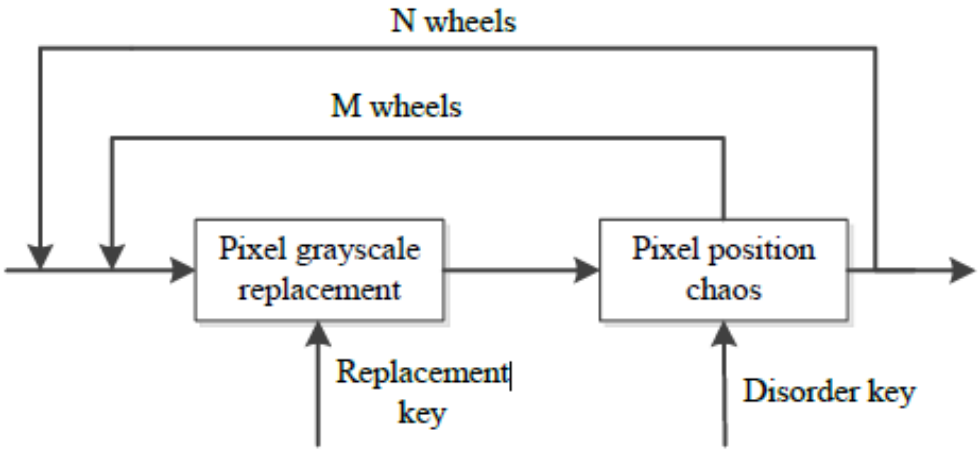


Figure 5. Basic structure of cyclic iterative image encryption

The key technologies involved in encryption algorithm:

1 Wheel key generation technology.

2 Chaos pseudorandom sequence generation technology.

3 Encryption feedback mechanism.

4. Research status of chaos image encryption

Digital images are much larger than text data and have some correlation with adjacent data. In addition, with the development of science and technology, people's demand for timely communication is constantly improving. Therefore, the traditional chaotic image encryption algorithm may play a certain role in images, but it can not fully meet the needs of human beings.

4.1 Color image encryption algorithm based on chaos theory and DNA dynamice encoding

Nowadays, with the development of science and technology, more and more researchers devote themselves to the study of DNA cryptography. Because DNA molecules can process data in parallel and store a large amount of data, low energy consumption and rich resources, it has a unique advantage to encrypt and store data by using its characteristics. And gradually become an important research direction in the field of information security. Its advantages over traditional cryptography are:

1 DNA small molecular size to achieve nano-level storage;

2 DNA sequence parallel operation, improve operation speed;

3 DNA mixed encryption, detection difficulty increased, security is reliable protection.

The encryption process is shown in figure 6.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202107_7(7).0060

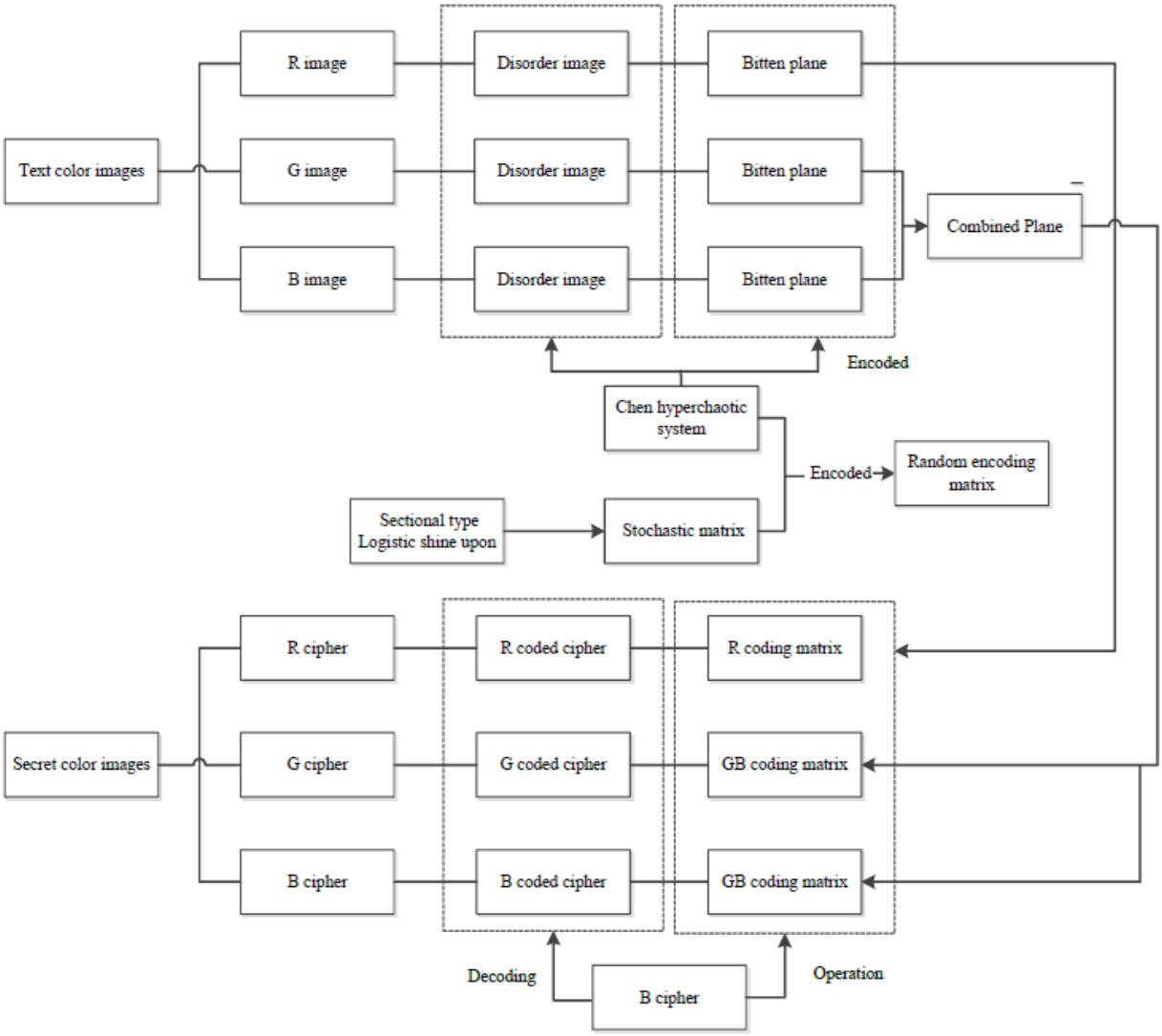


Figure 6. Flowchart of Color Image Encryption Based on Chaos Theory and DNA Dynamic Encoding

Encryption ideas:

Color images of 256×256 are selected as encrypted images, which is decomposed into three grayscale images: R channel component, G channel component and B channel component, R, G, B three channels are then scrambled, where each gray image has the same scrambling process. And then merge the DNA encoding of the channel image, And then merge the DNA encoding of the channel image, by using random matrix and ciphertext DNA each channel, finally, the encrypted image is obtained. Then the decryption key is input into the system, and the decryption image of the encrypted image can be obtained by reverse operation encryption process.

Performance analysis of the encryption algorithm:

After the plaintext image is encrypted by the encryption algorithm, the encrypted image is similar to noise, which can not be recognized and hides the original information. There is no correlation between ciphertext and original plaintext, so the encryption algorithm has good encryption effect. The key decrypted image is consistent with the plaintext image, which indicates that the encrypted image can be completely restored without interference [20]. And the encryption algorithm is sufficient to resist exhaustive attacks. At the same time, the encryption algorithm takes the initial value of the system as the encryption key, changes the initial value of the system relatively, then uses a single key to change slightly, and the other keys remain unchanged to decrypt. It can be seen that only a slight change of a single key can not restore the original plaintext image, and each group of key decrypted images are different from each other, so the encryption algorithm has high key sensitivity.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202107_7(7).0060

4.2 An image encryption algorithm based on chaos mapping and AES

AES full name is Advance Encryption Standard,it is the most widely used algorithm in symmetric cryptography, and its appearance is mainly to replace the DES encryption algorithm. AES encryption algorithm has attracted the attention of many scholars in the field of image encryption, and new image encryption algorithms related to AES have been proposed. Among the problems of image encryption, AES encryption algorithm has complex replacement and scrambling structure, and the overall encryption effect is better.However, it has the defects of small key space, fixed S box and wheel key space, which makes its overall security decrease. Therefore, some researchers have proposed an image encryption algorithm based on improved Henon mapping and AES to improve the overall security of AES encryption algorithm.

Encryption ideas:

1 First of all, thinking Henon mapping has the characteristics of hyperchaotic. Hyperchaotic systems have more than two positive Lyaponuv indices, which have excellent pseudo-randomity and huge key space [21]. Therefore, the hyperchaotic sequence is obtained by using four-dimensional Henon mapping as the key source to design AES encryption algorithm to solve the problem of small key space in AES encryption algorithm.

2 By using the average value of plaintext image pixels as parameters to import the thinking Henon mapping to intercept four groups of chaotic sequences, the correlation characteristics of plaintext image are introduced to improve the ability of image encryption algorithm to resist plaintext image attack and ciphertext image attack.

3 The four sets of chaotic sequences are used as training samples of specific neural networks to obtain four sets of nonlinear chaotic sequences with randomness and disorder, which are used as the target keys of AES encryption algorithms to improve the randomness of the keys of the AES algorithms.

4 The four sets of chaotic sequences are generated into two sets of S boxes and wheel keys, and the final ciphertext images are obtained by two rounds of AES encryption to solve the problem that the S boxes and wheel keys are fixed in the encryption algorithm.

5 The decryption key is input into the system, and the decryption image of the encrypted image can be obtained by reverse operation encryption process.

The encryption process is shown in figure 7.

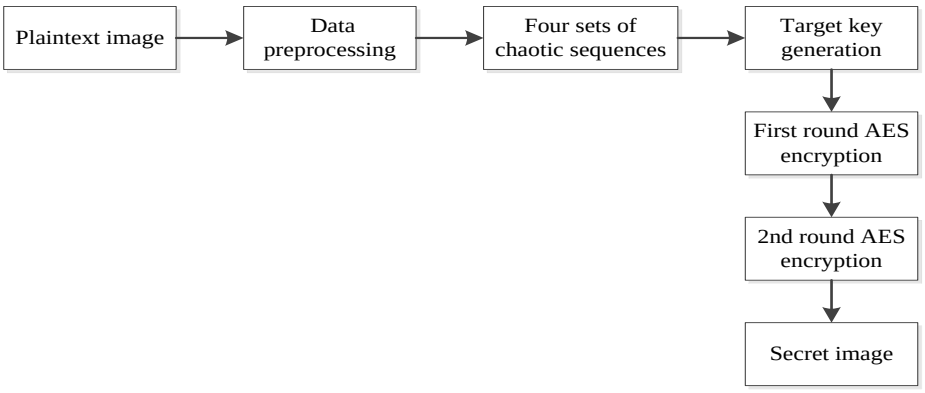


Figure 7. Flowchart of Image Encryption Based on Chaos Mapping and AES

Performance analysis of the encryption algorithm:

1 Histogram analysis: Histogram refers to the data analysis of the gray histogram of the image, and the concealment of the image is judged by analyzing the fluctuation of the gray pixels at all levels in the image. Safe and efficient ciphertext images will have a very uniform distribution histogram. By observing the histogram of the encrypted image using the algorithm, it is found that the distribution of gray pixel values at all levels of the histogram is very uniform and has good hiding ability.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202107_7(7).0060

2 Statistical analysis: By testing the correlation of pixels between adjacent pixels in the plaintext image and ciphertext using the encryption algorithm in vertical, horizontal and diagonal directions, it is found that the algorithm has very strong ability of anti-statistical analysis and has very good encryption effect.

3 Secret attack analysis: It means that the attacker does not know the encryption algorithm, only the intercepted ciphertext information is used to analyze and obtain the key required by the plaintext or encryption algorithm. In this encryption algorithm, the ciphertext image is closely related to the chaotic sequence generated by the key, and the hyperchaotic sequence has very strong nonlinearity and randomness, so it is difficult to crack the image encryption algorithm only by ciphertext image.

4 Key space analysis: The key of image encryption algorithm in this paper is double precision type, and the effective size of key data can reach 16 bits. Key space can reach 1060 than the traditional AES encryption algorithm has a huge key space, can effectively resist exhaustive attacks.

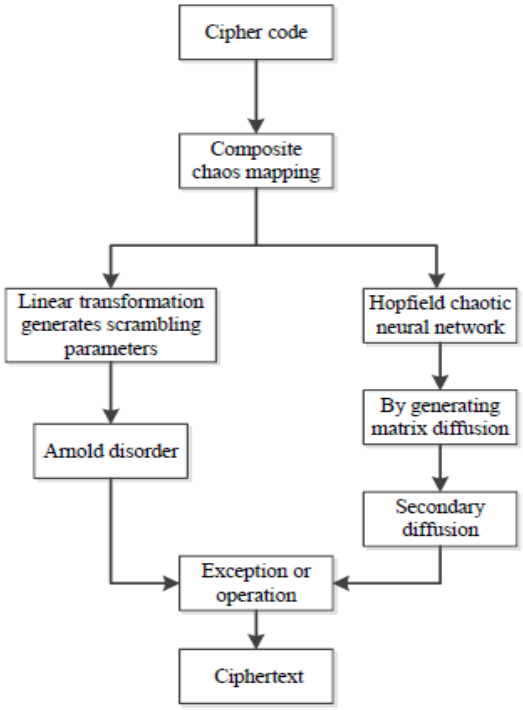


Figure 8. Image encryption flow based on Hopfield neural network

4.3 Image encryption algorithm based on Hopfield neural network

In recent years, with the development of artificial intelligence, neural networks with chaotic characteristics [22-24] have been paid attention to and become a new focus in the process of image encryption. Hopfield neural network and learning algorithm were first proposed by American physicist Hopfield in 1982. It is mainly used to simulate and analyze the neural network of organisms to find out the principle of memory between neurons. At the time of Hopfield neural network,: discrete neural network and continuous neural network. Discrete neural networks are mainly used for associative memory, while continuous neural networks are currently used to deal with optimization problems. The discrete neural network is suitable for the diffusion process of encryption. The encryption algorithm uses discrete neural networks.

The neural network is mainly divided into serial asynchronous and parallel synchronous. Parallel synchronization means that after some or all neurons change, the state of the next moment changes according to the corresponding rules. Serial synchronization means that at any time, after one neuron changes its state, other neurons change according to the influence and rules of its connected relationship. Whether serial asynchronous or parallel synchronous, the evolution steps are: Initialize

ISSN: 2414-1895 DOI: 10.6919/ICJE.202107_7(7).0060

the network, change the neuron, get the output of this round, judge whether the system is stable or not, and bring it into the next round of input. The encryption algorithm uses parallel synchronization mode.

The encryption process is shown in figure 8.

Performance analysis of the encryption algorithm:

1 Violent attacks: In this encryption algorithm, the key thinks that the non-integer key has the accuracy of 10-14, so its key space should be more than 2100, which has reached the theoretical non-violent cracking.

2 Key sensitivity: A good algorithm, its ciphertext must be highly sensitive to the key, so that the attacker can not be decomposed by fuzzy key attack. The experimental data show that in this encryption algorithm, when the key is changed in the minimum order of magnitude, the result of decrypted image can be completely different, and the information obtained can not express plaintext. So the sensitivity of the encryption algorithm is qualified.

5. Development prospect of chaos image encryption

Chaos image encryption, after years of development has achieved a lot of scientific research results. But because of the late start, still in many aspects of development immature. First of all, in the current research results, most encryption algorithms are aimed at single or double images, how to simultaneously encrypt multiple images or even extend to video, It is an important research direction in the future to design a more secure and efficient encryption algorithm. At the same time, with the progress of the times, the amount of image data is increasing, and the requirements of timely communication are constantly improving, so the design of efficient and secure encryption algorithm is also the most important. In addition, the current encryption algorithms are mostly theoretical, and have not been well applied in practice. How to ensure that the algorithm is practical and safe in practical application, including the design of hardware and software, this work also takes a long time.

In the aspect of neural network, in recent years, the role of neural network in network communication is becoming more and more important. It has been more and more applied in network confidential communication, and the scope of application has become more and more extensive, involving various fields in social work. In network security communication, neural network provides a new way of thinking and realization in the field of secure communication. In the future, the theory and application of neural network will be more comprehensive and in-depth. As the most valuable and potential new technology, neural network will play a key role in the development of cryptographic technology in network communication. Cryptographic technology as an important technology of confidential communication will also benefit here.

6. Conclusions

Nowadays, with the development of science and technology, the computing ability of computer is improving, and the speed and security of image encryption and decryption are also improving. But whether in the military field or in our daily life, image encryption has always been a technology that people continue to study and explore. With the continuous development of science and technology and the continuous exploration in the field of chaos, image encryption technology based on chaos will have a broader development prospect.

Acknowledgments

This research is supported by Liaoning University of Science and Technology 2020 National College students Innovation and Entrepreneurship training Program. This project is named as the research of image encryption algorithm based on chaos and deep learning and the project number is 202010146005.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202107_7(7).0060

References

[1] X. W. Zhang,“ Analysis on the Development Model of Computer Network Technology,” J.Technology diffusion, p. 125–126, Apr. 2010.

[2] Murilloescobar M A, C CruzHemandez, F Abundizperez, et al,“A RGB image encryption alogrithm based on total plain image charateristics and chaos,” J. Signal Processing, p. 119–131, 2015.

[3] KOSE U, ARSLAN A,“Design and Development of a Chaos-Based Image Encryption System,” J. Chaos.Complexity and Leadership, p. 22–28, 2012.

[4] Y. L. Mou,“It is impossible for the correlation key of lightweight packet cipher to be analyzed,” Xi'an: Xidian University, 2017.

[5] BIHAM E, SHAMIR A,“Differential cryptanalysis of DES-like crytosystems,” J. Journal of Cryptology, p. 3–72, Apr. 1991.

[6] LAI X, MASSEY JL,“A Proposal for a New Block Encryption Standard,” M. 1991.

[7] FELDHOFER M,DOMINIKUS S, WOLKERSTOREFR J,“Strong Authentication for RFID Systems Using the AES Algorithm,” J. Ches, p. 357–370, 2004.

[8] Standaert F, Pereira O, Yu Y,“Leakage-Resilient Synmetric Cryptography under Empirically Verifiable Assumptions,” J. Lecture Notes in Computer Science, p. 335–352, 2013.

[9] LORENZ N,“The essence of chaos,”J. Physics Today, p. 862–863, 1993.

[10] Jain M, Kumar A, Choudhary R C,“Improved diagonal queue medical image steganography using Chaos theory, LFSR, and Rabin cryptosystem,”J. Brain Informatics, p. 95–106, 2017.

[11] Jian L I, Xiang D Y,“Recent Development of Chaos Theory in Topological Dynamics,”J. ActaMathematica Sinica English, p. 83–114, 2016.

[12] CHEN X, HU C J,“Adaptive medical image encryption algorithm based on multiple chaotic mapping,”J. Saudi Journal of Biological Sciences, p. 1821–1827, 2017.

[13] DOU Y, LIU X, FAN H, et al,“Cryptanalysis of a DNA and chaos based image encryption algorithm,”J. Optik, p. 145, 2017.

[14] FU X, LIU B, XIE Y Y, et al,“Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos,”J. IEEE Photonics Journal, p. 1–15, 2018.

[15] LIU H, KADIR A, SUN X,“Chaos-based fast colour image encryption scheme with true random number keys from environmental noise,”J. Iet Image Processing, p. 324–332, 2017.

[16] QI Y, WANG C,“A New Chaotic Image Encryption Scheme Using Breadth-First Search and Dynamic Diffusion,”J. Iet Image Procession and Chaos, 2018.

[17] M. S. Yan,“Design and Analysis of MIMO Radar Orthogonal Waveform Based on Chaos Sequence,”D. Nanchang: Nanchang University,2018.

[18] H. M. Li, C. J. Li,“Research on Image Encryption Algorithm Based on Chaos Theory,”J. Journal of Changchun Normal University (Natural Science Edition),p. 43–47, Feb. 2018.

[19] Z. M. Li,“Research on Digital Image Encryption Based on Chaos and Neural Network,” D. Dalia:Dalian University of Technology, 2019.

[20] L. L. Cheng,“Research on Digital Image Encryption Algorithm Based on Chaos Theory,” D. Anhui:Anhui University, 2018.

[21] Y. Wang, J. Yang, Y. Wang,“The Improved Image Encryption Algorithm for Henon chaotic System Combined with AES,”J. Computer engineering and applications, p. 180–186, 2019.

[22] PENG J, ZHANG D,LIAO X,“A Digital Image Encryption Algorithm Based on Hyper-chaotic Cellular Neural Network,”J. p. 269–282, 2009.

[23] KUMAR S, AID R,“Image encryption using wavelet based chaotic neural network; International Conference on Advances in Computing,” C. 2016.

[24] ZHAO G M, GUO-DONG L I,“On Application of Image Encryption Technology Based on Chaotic of Cellular Neural Network,”J. Journal of Mianyang Normal University, p. 151–158, 2014.