ISSN: 2688-8653

Image Encryption Algorithm based on Hyperchaotic Lorenz System

Jiaming Zhao, Wenyu Zhang

School of computer and software engineering, Liaoning University of science and technology, Anshan, Liaoning, 114051, China

Abstract

With the advent of the Internet era, more and more information interaction needs to be transmitted through the network, such as video, audio, pictures and so on. Image has many advantages, such as intuitive, simple and so on, which makes it the most widely spread way at present. However, with the rapid development of science and technology, more and more malicious attacks such as information theft have become a common phenomenon. Therefore, information security has become a research field concerned by many scholars. Image encryption has been widely studied, mainly committed to designing a more secure and efficient image encryption algorithm. Most of the traditional image encryption algorithms are easy to be decoded after "violent" attacks. Later, researchers found that the combination of chaotic mapping and image encryption can give full play to many excellent attributes of chaotic system to ensure that the cryptosystem is not easy to be attacked by malicious attacks. Therefore, image encryption algorithm based on chaos has become the first line of cryptography research. Firstly, this paper introduces cryptography and classical diffusion and scrambling algorithms, and then designs a chaotic image encryption algorithm using hyperchaotic Lorenz system. Finally, the indexes of the algorithm are analyzed to prove that the algorithm proposed in this paper has high security.

Keywords

Chaos; Cryptography; Image Encryption.

1. Introduction

In this era of information explosion, due to the rapid development of the network, more and more information is transferred from traditional carriers to new carriers, such as text, data and other information recorded on paper, which are collected, saved, edited and transmitted by computers [1-3]. In the Internet era of the 21st century, more people will access the Internet through computers to obtain information; According to the 43rd statistical report on China's Internet Development released by China Internet Network Information Center, the number of Internet users in China had reached 1.011 billion by October 2012. In this huge scale and the prevailing situation of the Internet, a large number of important image information in private and special fields need to be transmitted through the Internet. The leakage of personal privacy information is everywhere, and there is a growing trend of development. In the Internet era, it is very important to protect personal privacy and the security of information in special fields [4-7]. Therefore, the key problems to be solved include: how to ensure that the image is not "stolen" and the integrity of image transmission.

2. Chaotic Image Encryption Algorithm

2.1. Cryptography

Cryptography is a subject that encrypts and decrypts information. The purpose of cryptography is to convert the transmitted information into an unavailable format on the transmission medium, so that the information can only be recognized by authorized persons. Passwords are divided into two categories: substitution passwords and substitution passwords. Only using simple substitution and replacement can not make the encryption system achieve the desired effect. Therefore, in recent years, many scholars [8-11] have developed new algorithms to encrypt information.

There are many categories of cryptographic technology, which are widely used in many fields. Any cryptographic technology is not independent, but interrelated and complementary to each other, forming a very rich framework, just like a huge jigsaw puzzle. Basic cryptographic techniques include the following:

(1) Symmetric password: it has the same key for encryption and decryption. The common ones are des, idea, blowfish, cast-256, Mars, etc. According to different processing objects, symmetric algorithms can be divided into stream cipher and block cipher.

(2) Asymmetric key: asymmetric cryptography refers to that different keys can be used for encryption and decryption, also known as public key cryptography. Public key cryptography was produced in the 1970s. This method has brought a very important change in the field of cryptography. The security systems in modern computers and networks depend on public key cryptography to a great extent.

(3) One way hash function: one way hash function is a key technology to transform complex messages into hash values, which can be used for message guarantee and availability.

(4) Message authentication code: message authentication code is a verification technology that can identify whether the message content sent by the other party in communication is fabricated and whether it is true or false. It can be used to check the integrity of the message and verify the message content.

(5) Digital signature: digital signature is a series of numbers that can only be generated by the message sender. This series of numbers cannot be forged by others.

(6) Pseudo-random number generator: the pseudo-random number generator is composed of one-way hash function and cryptography, which can produce a highly unpredictable bit sequence.

2.2. Classical Diffusion and Scrambling Algorithms

Shannon proposed two basic principles, which are the main basis for supervising the key design process in the field of cryptography. These two basic principles are diffusion and scrambling.

Diffusion algorithm: in the image encryption algorithm, the diffusion processing method aims to not change the original pixel position of the encrypted image, and change the gray value of each pixel of the encrypted image. Common diffusion algorithms are as follows:

(1) Diffusion algorithm based on XOR operation.

(2) Diffusion algorithm based on modulo addition.

(3) Diffusion algorithm based on modulo addition and cyclic left (right) shift.

(4) Diffusion algorithm based on Galois field (addition field, subtraction field, multiplication field and division field) operation.

Scrambling algorithm: scrambling is to disrupt the "coordinate" order of encrypted image pixels and ensure that the pixel values do not change. Commonly used scrambling algorithms include the following three types:

(1) Line scrambling and rank scrambling are adopted for the two-dimensional image matrix, or the scrambling of rows and columns is staggered.

(2) The two-dimensional image is represented in the form of one-dimensional vector, and the position is scrambled. This one-dimensional vector is usually expressed in the form of rows and columns.

With the help of scrambling matrix, the position of each pixel of two-dimensional image is changed.

2.3. Chaotic Image Encryption

2.3.1. Hyperchaotic System Lorenz

Lorenz proposed Lorenz equation based on the chaotic attractor discovered in the middle of the 20th century, also known as Lorenz system. Lorenz chaotic system belongs to high-dimensional nonlinear dynamic system, and its definition is shown in formula (1):

$$\begin{cases} \dot{x} = a\left(y - x\right) + w \\ \dot{y} = cx - y - xz \\ \dot{z} = xy - bz \\ w = -yz + rw \end{cases} \tag{1}$$

Where, a=10, b=8/3, $-1.52 \le r \le -0.06$, equation (1) is in hyperchaotic state.

2.3.2. Image Encryption based on Chaotic System

In recent years, researchers have highly integrated chaotic system with the field of image encryption through its initial value sensitivity and similar properties of cryptography. Based on Lorenz chaotic system and common image encryption models, 256 images are encrypted on windows10 platform by using matlabr2018 × 256 images are encrypted and analyzed experimentally. The encryption process is shown in Figure 1:

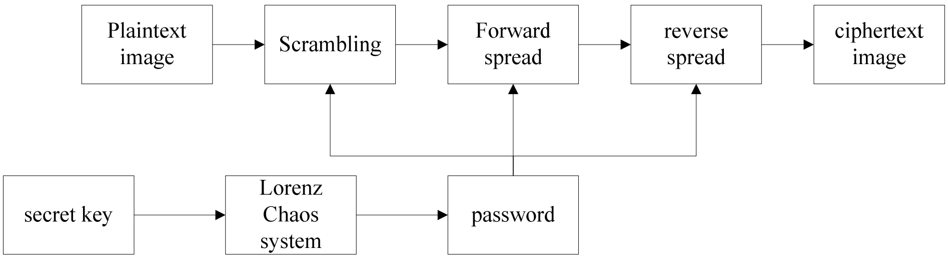


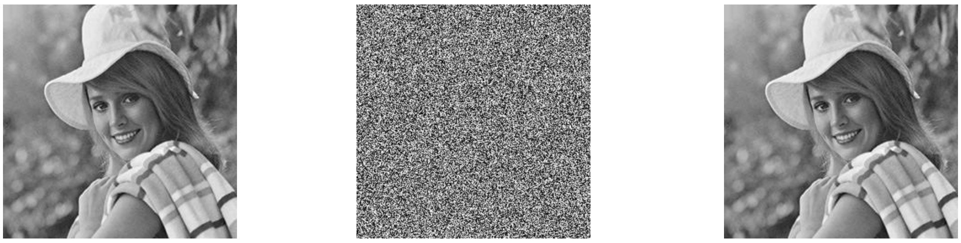
Figure 1. Image encryption process

Firstly, the key is input into the chaotic system, and the chaotic sequence generated by the system through iteration is used as the password. Then, the password is used to scramble the plaintext image pixels, forward diffusion and reverse diffusion, and finally generate the encrypted ciphertext. The diffusion process of the algorithm adopts the diffusion algorithm of XOR operation, while the scrambling process adopts the scrambling algorithm of scrambling the position of the vector after expanding the two-dimensional image into one-dimensional row vector or one-dimensional column vector.

3. Experimental Results and Index Analysis

3.1. Experimental Results

In this paper, the simulation experiment of image encryption algorithm is proposed. The software environment is Matlab2018 and the operating system is Windows10. The gray image with size of 256*256 is used in this paper. Firstly, the encryption algorithm is used to encrypt the image, and then the ciphertext image is decrypted through the given key and decryption algorithm. The experimental results are shown in Figure 2:



Linda Original image Linda ciphertext image Linda decrypts the image

Figure 2. Linda Cipher text image

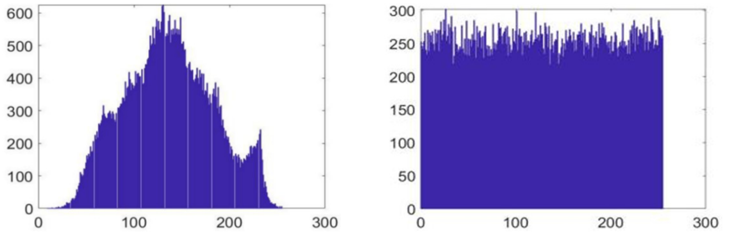
3.2. Index Analysis

The security of image encryption algorithm is often judged by six indexes, which are encryption and decryption time, key space, ciphertext statistical characteristics, ciphertext sensitivity, plaintext sensitivity and information entropy.

1. Encryption and decryption time: in order not to lose generality, the unified encryption and decryption size in this paper is 256 × 256 8 images for 100 times, and calculate the average encryption time. The algorithm encryption time of this chapter is 1.0990s, and the decryption time is 1.2368s.

2. Key space: refers to the set of legal keys in the key system. When the key length is r, the key space has 2 elements to the power of R. In this chapter, the set of parameters and initial values used in the image encryption algorithm based on Lorenz chaotic system is the key space,Its size is $2.56*10^{59}$,In theory,The key space is 2^{100}, which can resist some "violent" attacks. The algorithm key space in this chapter is greater than 2^{100}, which can resist exhaustive attacks.

3. Statistical characteristics of ciphertext: it refers to analyzing the statistical characteristics of ciphertext images by comparing the evaluation indexes such as plaintext and ciphertext histogram. Researchers generally believe that a good image encryption algorithm should reduce the correlation between two adjacent pixels in the encrypted image. The plaintext histogram in this paper is shown in Figure 3.



Linda plaintext histogram Linda ciphertext histogram

Figure 3. Linda Ciphertext histogram

4. Key sensitivity analysis:

Key sensitivity, KS is an evaluation index for testing the ability to resist illegal decryption. It refers to the difference obtained when fine-tuning parameters: the difference is reflected through ciphertext. If there are significant differences between the two ciphertext images, the cryptosystem is said to have strong key sensitivity; On the contrary, the KS effect is poor.

The difference between the two images is judged by the following indicators: nPCR and uaci. In this chapter, two images with the same dimension are recorded as P1 and P2, and the image size is M * N. NPCR is to compare the percentages of pixels with different corresponding positions in two images. The theoretical expectation of NPCR is 99.6094%. The calculation formula is as follows:

$$NPCR(P1,P2)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|\,Sign(P1(i,j)-P2(i,j))\,|\times 100\%$$

UACI refers to calculating the average value of the ratio of the pixel points at all corresponding positions and the ratio of the maximum difference (the maximum difference is 255) by comparing the difference of the pixel points at the corresponding positions in two images and recording their ratio. The theoretical expectation of uaci is 33.4635%. The calculation formula is as follows:

$$UACI(P1,P2)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|\,P1(i,j)-P2(i,j)}{255-0}|\times 100\%$$

The sensitivity analysis of algorithm key in this chapter is shown in Table 1:

Table 1. Key sensitivity analysis

algorithm	Algorithm in this paper	Ref [56]	Ref [57]	Theoretical value
NPCR(%)	99.4099	99.6049	99.6212	99.6094
UACI(%)	33.3990	33.4656	33.4706	33.4635

5. Text sensitivity analysis:

Explicit sensitivity (ES) refers to the use of the same key to obtain the corresponding ciphertext image difference when the image encryption system encrypts the plaintext images with slightly changed pixel values. Comparing the difference between two ciphertext images, when the difference between the two ciphertext images is very different, the image cryptosystem is said to have good es; If the difference between two ciphertext images is small, the image encryption system is said to have weak es, and this kind of image encryption system is usually unable to resist selective plaintext attack or known plaintext attack,

The sensitivity analysis of algorithm plaintext in this chapter is shown in Table 2.

Table 2. Plaintext sensitivity analysis

algorithm	Algorithm in this paper	Ref [56]	Ref [57]	Theoretical value
NPCR (%)	99.2174	99.5926	99.6098	99.6094
UACI (%)	33.5535	33.3386	33.4537	33.4635

6. Information entropy: it reflects the uncertainty of ciphertext image information, and its calculation formula is as follows:

$$H=-\sum_{0}^{i=0}p(i)\log_2 p(i)$$

Where i is the gray level of the image, and p(i) represents the probability of occurrence of gray value i.

The information entropy of plaintext and ciphertext used in this chapter is 7.5372 and 7.9976. For 256 * 256 pictures, the theoretical value of information entropy is 8. The difference between the information entropy of each ciphertext image and the theoretical value is small, which proves that it has a good information entropy.

4. Conclusion

This paper proposes an image encryption algorithm based on hyperchaotic Lorenz system, and introduces cryptography and classical diffusion scrambling algorithm. Through the index analysis, it is concluded that the image encryption algorithm in this paper has high security and is not easy to be attacked by exhaustive method and other malicious acts, but the plaintext sensitivity needs to be further improved.

References

[1] ALLEN J. Short Term Spectral Analysis,Synthesis,and Modifification by Discrete Fourier Transform [J]. IEEE Transactions on Acoustics Speech &amp; Signal Processing. 1977,25(3):235-238.

[2] Lian S, Sun J, Wang Z. A block cipher based on a suitable use of the chaotic standarmap[J]. Chaos Soliton Fract. 2005, 26(1): 117-129.

[3] Li C , Shang X , Zhang L , et al. Pipeline Defect Detection Cloud System Using Role Encryption and Hybrid Information[J]. Computers, materials and continuum (English), 2019 (9): 16.

[4] Jiang Wenchao, Lin Dexi, Guo chumou, et al A new text encryption and decryption algorithm with customizable encryption strength [M] Computer science and exploration. 2017.11 (9): 1439-1450.

[5] Liu Wenhao, sun Kehui, Zhu congxu A hyperchaotic digital speech encryption algorithm for mobile communication [J] Journal of cryptography, 2017,4 (1): 85-98.

[6] Hamidouche W, Farajallah M, Sidaty N, et al. Real-time selective video encryption based on the chaos system in scalable HEVC extension[J]. Signal Processing Image Communication. 2017, 58:73-86.

[7] Guesmi R, Farah M A B, Kachouri A, et al. A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2[J]. Nonlinear Dynamics. 2016,83(3):1-14.

[8] Liu Yipeng, Guo Jiansheng, Cui Jingyi Design of secure amplification scheme for efficient short seed quantum key distribution [J] Journal of optics. 2017,37 (2): 273-282.

[9] Huang Biao, Huang Yongmei, Peng Zhenming Reference pulse phase attack and detection for continuous variable quantum key distribution [J] Journal of optics. 2019,39 (11): 327-333.

[10] Sun Ying, Zhao Shanghong, Dong Chen Passive measurement equipment independent quantum key distribution based on parametric down conversion light source [J] Journal of optics. 2015,35 (12): 267-273.

[11] Huang D, Fang J, Wang C, et al. A 300-MHz Bandwidth Balanced Homodyne Detector for Continuous Variable Quantum Key Distribution[J]. Chinese Physics Letters. 2013, 30(11):468-477.