Journal of Computing and Electronic Information Management

ISSN: 2413-1660

Summary of image encryption technology based on chaos

Jiaming Zhao, Ye Tao*, Wenyu Zhang
School of Computer and Software Engineering, University of Science and Technology Liaoning, Anshan City, Liaoning Province, 114051, China

*Corresponding author: Ye Tao, Email:taibeijack@163.com

Abstract: This article first gives a brief introduction to the huge and complex information processing system-cryptosystem, Summarizing the shortcomings of traditional image encryption algorithms. It analyzes how to improve the traditional encryption algorithm. Then it explained the current development of research work on image encryption algorithms. The cryptosystem constructed by the neural network is explained. And the research results and general problems that have been achieved by the application of chaos in the field of image encryption. Finally, the development trend of image encryption technology based on chaos and the importance of improving the security of image encryption algorithms are explained.

Keywords: Chaos; image encryption; encryption algorithm; neural network.

1. Introduction

In this age of information explosion,Information security has become a topic of discussion. As people pay more and more attention to privacy and protection of important information, The importance of cryptography is increasing [1]. Therefore, cryptography has become a very popular topic, Finding a more secure and efficient encryption method has become particularly important. In the field of information security, most information carriers are expressed in the form of images. At present, the more common methods of enhancing image security include image pixel spatial scrambling, gray value transformation, double change of spatial position and gray value, However, these are encrypted only by pixel transformation, which is particularly easy to be statistically analyzed and then cracked. Although the traditional encryption method can be used for image encryption, the work efficiency is not low and it is easy to be deciphered, so it is very necessary to find a more secure and more efficient image encryption technology [2]. Many excellent properties of chaotic maps, such as pseudo-randomness and initial value sensitivity, are necessary for the realization of

cryptosystems. Therefore, chaos-based encryption algorithms have become the front line of cryptography research.

Although many chaotic encryption algorithms have been proposed, many practices have found that most schemes are not secure enough. Because chaotic mapping parameters and steady-state simulation accuracy will be greatly limited, chaotic sequences have some shortcomings, including large-area linearity and strong correlation. There are strong limitations to using only pseudo-random sequences excited by chaotic sequences for encryption [3]. The limited accuracy of the computer system is likely to lead to a short period of chaotic sequences and poor randomness. Nowadays, a large part of existing chaotic encryption technologies are based on one-dimensional or two-dimensional chaotic control systems, and these technologies are easily attacked by phase space reconstruction methods. There are many other insecure and inefficient situations in chaotic encryption. Therefore, people apply the neural network theory to the chaotic encryption method. After experimental analysis, it is found that this method strengthens the encryption effect, improves the encryption efficiency, and improves information security.

2. Cryptography

Encryption and decryption involve many aspects such as information confidentiality, availability, authentication, etc., and the related technologies derived from this are always related to the safety of personal property in people's daily lives. Password-related technologies are so indispensable, but they are so bland, people rarely pay attention to their existence, and very few people understand why people need them and how they work. Regarding cryptographic technology, most people are in a state of "neither knowing nor knowing why". There are many types of cryptographic technologies. They are used in many fields. Each cryptographic technology does not exist independently. Instead, they are related to each other and complement each other to form a very large framework, just like a huge one. The basic cryptographic techniques are as follows:

Symmetric password

Symmetric password has the same encryption and decryption keys, common ones are DES, IDEA, Blowfish, CAST-256, Mars, etc. [4]. Symmetric algorithms can be divided into two types according to different processing objects, one is stream ciphers and the other is block ciphers [5].

Public key password

Asymmetric password refers to the method of using different keys for encryption and decryption, also known as public key password. Public key cryptography emerged in the 1970s, and this method triggered a major revolution in cryptography. The security

systems in modern computers and the Internet largely rely on public key cryptography.

One-way hash function

One-way hash function is a key technology that transforms a longer message into a hash value, which is used to ensure the availability of the message.

Message authentication code

Message authentication code is a kind of authentication technology that can identify whether the message sent by the communication object is fabricated, and is used to verify the integrity of the message and authenticate the message.

Digital signature

Digital signature is an authentication technology that can authenticate third-party messages and prevent the communication object from denying it.

Pseudo-random number generator

Pseudo-random number generator is a technology that can generate unpredictable bit sequences, which is composed of technologies such as cryptography and one-way hash function.

3. Image encryption technology

Digital images are one of the most popular multimedia forms in today's society, and they are widely used in many fields such as economy, education, politics, and national defense. In some special fields, such as military, commercial and medical, digital images have important confidentiality requirements.

In order to make the digital image highly confidential, in actual operation, the two-dimensional image is generally converted into relatively simple one-dimensional data, and the existing encryption algorithm is used to encrypt the image. Unlike ordinary encryption technologies, images and videos are temporal, spatial, and visually perceptible, and can also be lossy compressed. These unique features make the encryption algorithm of image design more efficient and secure.

Since the 1990s, researchers have fully utilized these key features to propose many types of encryption algorithms. At present, image encryption technology can be divided into two categories, namely, airspace image encryption technology and compressed image encryption technology. The purpose of the pixel scrambling based on the spatial domain is to quickly disturb the pixel position, simply destroy the original local correlation and spatial order of the image, so that people can not see the original image and turn the image into a Noise-like form.

Image encryption technology is about the reason why images can be compressed because there is redundancy in the data. The redundancy of image data is mainly manifested in the following points. Spatial redundancy caused by the correlation between adjacent pixels in the image; Temporal redundancy caused by the correlation

between different frames in the image sequence; Caused by the correlation of different color planes or spectral band Spectrum redundancy. The purpose of data compression is to reduce the number of bits required to represent data by removing these data redundancy. For example, the image-based encryption technology is based on the visual redundancy of the image. After obtaining the preliminary encrypted image, it is hidden into another carrier image. The gray value of each pixel is distributed between 0 and 255 [6], which can be converted into a binary number to represent, by modifying the least significant bit to achieve image hiding. Due to the huge amount of image data, it is very difficult to store, transmit and process, so the compression of image data is very important.

4. Chaos image encryption

Chaos

At present, there is no more unified definition of chaos. Scholars have only given different description methods from different angles. Among them, the Li-Yorke definition is more widely accepted [7]. The definition of Li-Yorke is shown in formula (1).

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

among them, $\mu \in (0,4)$, $x \in [0,1]$, $n=1,2,\ldots$.

Chaos theory is an exciting new academic research field. The discovery of chaos is very compelling and controversial. Chaos connects people's daily life with the laws of nature by explaining the subtle relationship between simplicity and complexity, order and randomness. The famous American mathematician Ian Stur defined it as: the ability of a simple model without inherent randomness to produce highly irregular behavior. Shannon proposed two basic principles before, which are the main basis for supervising cryptographic design in the field of cryptography. These two basic principles are chaos and proliferation [8].

From the 90s but now, chaotic science can already be integrated with other sciences, whether in mathematics, physics, psychology, astronomy, meteorology, economics, even music, art and other fields Popular applications. Nowadays, the discovery of chaos and the theory of relativity and quantum mechanics are also called the three major achievements of physics in the century. The establishment of chaos has created the basic connection between the two scientific systems of determinism and probability theory. The development of the entire modern science has had a profound impact. Nowadays, it is considered to be one of the most important theoretical discoveries since the emergence of quantum theory in the 20th century [9].

Chaos model

Over the past few decades, scientists in different fields such as weather forecasting, fluid mechanics, chemistry, and population biology have established models that include nonlinear and feedback factors to study natural phenomena. The models exhibit two conflicting characteristics. First, they all have only a few simple equations. Second, the solutions to these equations are quite complex and unpredictable. Analysis of these models and similar behaviors found in experiments are what people now call "chaos theory."

Take this simple equation as an example, $x*x + c = result$ where x is a changing complex value, but a fixed complex value. If the operation results are continuously fed back to the position of the changing value x, that is, iterating this equation-a chaotic model will be generated.

Characteristics of chaos

The system studied by chaos theory has a distinctive feature: unstable non-periodic behavior can be expressed by simple mathematical formulas. These very simple but well-defined mathematical models can present extremely complex behaviors. Another distinguishing feature of chaotic systems is that they are sensitively dependent on initial conditions-very small differences at the beginning will cause huge changes afterwards. This behavior is called the characteristic of chaos.

Some scientists believe that these characteristics of chaotic systems are an important source of novelty and diversity in nature. Other scientists regard it as the boundary of human cognition, as if nature is ordering people to stop moving forward.

Chaos-based image encryption

Chaos is a very complex power with a special form, has system parameters, and has a strong sensitivity to initial values. Chaos has obvious characteristics such as trajectories without random rules, randomness and boundedness. Chaos and cryptography have similar properties. In recent years, chaos has been applied to cryptography research problems. The area detection balance and sequence etc. are carried out through statistics and other means, which can be used for image encryption in the sequence. With the help of chaos, some calculated the reversible characteristics of the expression, and substituted the pixel value into the chaos calculation formula to successfully complete the substitution and diffusion of pixels [10]. In 1998, Fridrich proposed a symmetric block encryption algorithm based on two-dimensional standard baker mapping [11]. In the same year, Scharinger developed an image encryption technology based on chaotic Kolmogorov flow [12]. In 2004, a symmetric image encryption algorithm was discussed and studied by Chen et al. [13]. Literature [14] proposed an image encryption algorithm based on chaotic system and DNA technology (deoxyribonucleic acid sequence). In [15], a chaotic map function is used instead of a hash function to construct a chaotic image encryption algorithm based on two-level key

inscription association. Literature [16] proposed an algorithm that changes the matrix transformation encryption of pixel values without changing the position of pixels, and can be cracked by choosing a plaintext attack to solve the congruent equations. Today, The chaotic systems often used for image encryption have the following points.

a. Logistic chaotic map

Logistic map is a very classic model mainly including dynamic system, chaos, fractal and other complex system behaviors. It is also called Logistic iteration. In short, it is a time-discrete dynamic system. Iterative iteration is performed according to equation (2).

$$x(t+1)=\mu x(t)(1-x(t)) \tag{2}$$

Where t represents the iteration time step, $x(t)\in[0,1]$, μ represents adjustable parameters, $\mu\in[0,4]$.

b. Piecewise linear chaotic map

It is a piecewise linear chaotic map based on the transformation of hash functions of chaotic dynamic parameters, spatiotemporal chaos, hyperchaos and variable parameters to form a one-way hash function. Many other chaotic systems have been widely used .

Deficiency of chaotic encryption

Literature [17] analyzed a chaotic system encrypted by an image and found that after processing the values generated by the chaotic system, many operands used for stream cipher encryption are 0; it points out that this method generates pseudo-random Encrypting images for several times is insecure, and a few examples of image encryption are cited. From these encrypted pictures, the characters in the plain text can be seen inconsistently. Literature [18] for most encryption algorithms, these methods only encrypt one image at a time, but in actual situations where a large number of images need to be transmitted through batch processing, an algorithm is proposed that combines vector quantization and index compression of batch images In fact, the encrypted index is quantized and the resulting index is streamed in the form of a password. At present, the analysis and attacks on chaotic encryption systems are aimed at low dimensions, and studying high-dimensional chaotic systems or hyperchaotic systems [19] may find chaotic encryption schemes with more complicated and random evolutionary rules.

5. Image encryption based on neural network

A. Neural network

Neural network can be roughly divided into two manifestations, one is called biological neural network, and the other is called artificial neural network. Biological neural

network generally refers to the network system of organisms' brain neurons, cells, and other organizational structures. It is a system in which organisms generate consciousness, helping organisms to think and start actions. An artificial neural network can also be called a neural network or a connection model. It is mainly an algorithm model that imitates the behavioral characteristics of animal neural networks and performs distributed parallel information processing. It mainly relies on extremely complicated systems, through the adjustment of the interconnection relationship between most internal nodes, to effectively process information. Its research content can be described as quite extensive, fully showing the characteristics of multidisciplinary interdisciplinary technology.

In the field of machine learning, the calculation model of artificial neural networks is mainly based on the animal's central nervous system, mainly the brain. And it has a great role in estimating or can rely on a large number of inputs and generally unknown approximate functions. Artificial neural networks are usually expressed in the form of interconnected "neurons", which can calculate values from input, and are capable of machine learning and pattern recognition due to their adaptive nature of the system.

B. Image encryption based on neural network

There are two main modes of chaotic god neural network introduced in literature [20]----Aihara neural network and Inoue neural network----both of which have nonlinear dynamic characteristics and are applicable for information encryption. The neural network is composed of highly interconnected neurons, which process the external dynamic input of internal information. The distributed processing mode is the most prominent feature of this method. Neural networks have the advantages of nonlinear associative memory and are suitable for information encryption. Reference [21] uses a recursive training process and uses a three-layer BP neural network to train the improved Henon chaotic sequence. Reference [22] uses the BP algorithm to propose a chaotic diagonal recurrent neural network learning algorithm.

6. Conclusion

This article mainly introduces the related knowledge of cryptography, related terms of cryptography, and related knowledge of chaos and neural networks. It briefly outlines the image encryption method based on chaos and the chaotic neural network based on the combination of chaos and neural network. The method of image encryption, the main purpose and focus of future work is to train the neural network and optimize the decryption algorithm, improve the encryption effect, increase the encryption efficiency, improve the system interference ability, and let the chaotic neural network system continue to develop.

Acknowledgements

This work is supported in part by the Liaoning Province Natural Science Foundation Project under Grant 20180551011.

References

[1] JONT B.ALLEN.Short Term Spectral Analysis,Synthesis,and Modification by Discrete Fourier Transform[J].IEEE Transactions onAcoustics Speech & Signal Processing, 1977,25 (3): 235-238.

[2] ZHANG Y Q,WANG X Y.A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice[J].Information sciences,2014,273（8）：329-351.

[3]Jiasheng Liu.Research on image encryption based on chaos [D]. Hefei: Anhui University, 2007.

[4]B Schneier. Applied Cryptography——Protocol, Algorithm and C Source Program [M]. Beijing: Mechanical Industry Press 2000.

[5] Changgang Li, Zhengzhi Han. Overview of image encryption technology [J]. Computer Research and Development, 2002, 39 (10): 1317-1324.

[6]Songxin Yi. Research on Data Protection and Encryption——Security of Computer Network [M]. Beijing: Science Press,1991.

[7]Bo Hai. Research on the construction of chaotic sequences and image encryption [D]. Anhui: Anhui University of Science and Technology, 2019.

[8]Shan C E.Communication theory of secrecy systems [J]. Bell System Technical Journal , 1949 , 28 (4):656-715.

[9]Shiyin Yan . Research and Implementation of Image Encryption Scheme Based on Chaos [D]. Shanghai: East China Normal University, 2007

[10]Han Zhang, Wang Xiufeng, Li Zhaohui, et al. A fast image encryption algorithm based on chaotic system and Henon mapping [J]. Computer Research and Development, 2005, 42 (12): 2137-2142.

[11]Fridrich Jiri.Symmetric ciphers based on two dimensional chao-tic maps[J].Int J Bifurcation and Chaos,1998,8(6):1259-1284.

[12] Scharinger J.Fast encryption of image data using chaotic Ko-lmogrov flow[J]. J Electronic Eng,1998,7(2):318-325.

[13]Chen Guanrong,Mao Yaobin , Charles K.A symmetric image encryption scheme based on 3D chaotic cat maps [J]. Chaos.Soli-tons and Fractals , 2004,21(3):749-761 .

[14]Chai X, Chen Y, Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations[J].Optics and Lasers in Engineering, 2017, 88(Complete):197-213.

[15]Zhang Y, Xia J, Cai P, et al. Plaintext Related Two-level Secret Key Image Encryption Scheme[J]. Telkomnika Indonesian Journal of Electrical Engineering, 2012, 10(6).

[16]Acharya B,Patra S K,Panda G.Image Encryption by NovelCryptosystem Using Matrix Transformation [C]//First Internation Conference on Emerging Trends in Engineering and Technology ,2008．Washington D C :IEEE Press,2008.

[17]Alvarez G,LiShu－jun．Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image

encryption[J].Communications in Nonlinear Science and Numerical Simulation, 2009, 14:3743-3749.

[18] Chen T-H,WyChang-Sian. Compression-unimpaired batch image encryption combining vector quantization and index compression[J].Information Sciences,2010,180:1690-1701.

[19] Gao Tie-gang,Chen Zeng-qiang.A new image encryption Algorithm based on hyper chaos[J].Physics letters A,2008(372):394-400.

[20]Kun Li, Jing Liu. Research on image encryption based on chaos and neural network [J]. Information and Computer. 1003-9767 (2019) 05-060-02.

[21]Jin Wang, Rong Qiu, Wang Xiang. Image encryption research based on chaos and neural network [J]. Intelligent Processing and Application 2095-1302 (2018) 04-0079-03.

[22]Yi Zhen, Boyuan Ma, Yi Zhang, Lina Liu.Image compression based on chaotic diagonal neural network [J] .Journal of Hebei Normal University.2015.5.

About the author: JiaMing Zhao(1997-), male, Han nationality, native of Anshan, Liaoning, undergraduate, postgraduate, current research direction: chaos, information security;

Ye Tao (1980-), male, Han nationality, native of Liaoyang, Liaoning, master student, lecturer, research direction: information security, chaos;

Wenyu Zhang (1973-), male, Han nationality, from Anshan, Liaoning, doctoral student, professor, research direction: machine learning, computer control.