ISSN: 2414-1895 DOI: 10.6919/ICJE.202110_7(10).0031

Overview of Image Encryption Technology based on Chaos and Neural Network

Mindan Zhang[1,a], Ye Tao[1,*] and Wenyu Zhang[1,b]

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

[a]1677254661@qq.com, *taibeijack@163.com, [b]zhangwenyu8518@126.com

Abstract

Artificial neural network is a very important operation model in the field of artificial intelligence. Ann deals with complex problems by simulating the structure and logic of human brain. Chaotic system is a dynamic system of deterministic, disordered and nonlinear motion. Whether random factors are added or not, it can show a random phenomenon, that is, it shows internal randomness, the motion trajectory is not periodic or divergent, and it depends on the initial value, and the sensitivity is also stronger. This paper introduces the types of ciphers in cryptography, encryption algorithms in cryptography and the characteristics of chaos, and introduces in detail the feedforward neural network, feedback neural network and self-organizing neural network in neural network, as well as the current encryption algorithms based on chaos and neural network.

Keywords

Chaos; Image Encryption; Encryption Algorithm; Neural Network.

1. Introduction

In the Internet age, the importance of information is particularly prominent. As the carrier of information, images appear in people's vision all the time, and images are vulnerable to attack in the process of transmission, resulting in the leakage of image information. Therefore, image information security has attracted extensive attention. Encryption of digital image is an effective way to prevent image information leakage. The traditional encryption method can not be satisfied with image encryption. In recent years, many scholars have combined chaos and neural network technology with image encryption, and achieved good encryption results.

2. Cryptography

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 types: substitution passwords and substitution passwords. Substitution password uses different bits, characters and strings to replace the original bits, characters and strings. Replacement password is to rearrange the original bits, characters and strings to hide their meaning.

Only using simple substitution and replacement can not make the encryption system achieve the desired effect. Therefore, in recent years, many scholars have developed new algorithms to encrypt information. According to the classification of encryption methods, cryptographic encryption algorithms can be divided into symmetric encryption algorithms and asymmetric encryption algorithms. In the symmetric encryption algorithm, the encryption key is consistent with the

ISSN: 2414-1895 DOI: 10.6919/ICJE.202110_7(10).0031

decryption key. Therefore, the key of symmetric encryption algorithm must be absolutely confidential. Such as DES, AES, etc. The encryption and decryption keys of asymmetric encryption algorithm are inconsistent, which are divided into public key and private key. The public key can be disclosed, and the private key needs to be kept absolutely confidential. Such as D-H, RSA, etc. [1].

3. Artificial neural network

Artificial neural network (ANN) is an abstract expression of human brain neurons by researchers. A neural network needs a large number of neurons. The function of each neuron is very simple, but the collection of a large number of neurons can solve very complex problems.

Warren McCulloch and Walter pits founded the M-P neuron model in 1943 [2], as shown in figure 1. In the M-P neuron model, a neuron has multiple inputs, which are represented by *x1*, *x2*... x_n respectively. *Wij* is the weight, *f (·)* is the activation function, which maps the input to the output and reduces its linear relationship. M-P model is the first artificial neuron model proposed. Although there are many forms of artificial neurons, they are all based on M-P neurons. A complete neural network includes three layers: input layer, hidden layer and output layer. When nonlinear separation of data is required, hidden layer is required.

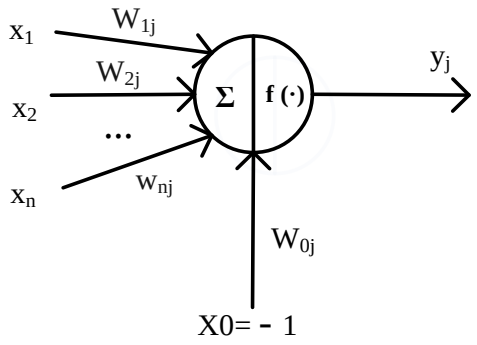

Figure 1 M-P neuron model

3.1 Fully Connected Neural Network (FCNN)

In the feedforward neural network, because the relationship between the two layers of neurons in the necklace is a fully connected relationship, it is called fully connected neural network (FCNN). In the fully connected network structure, nodes need to meet the following requirements: (1)All upper nodes and lower nodes are connected. (2) There is no node connection on the same layer. (3)There is no interlayer node for connection. There is no feedback signal in feedforward neural network. Feedforward neural network includes perceptron, BP neural network and so on.

The feedforward neural network is divided into two parts. One part is responsible for the linear summation of the input vectors, and the other part uses the excitation function to linearize the results obtained by the first summation. Common excitation functions include S*igmoid* function, T*anh* function and R*eLu* function

(1) Single layer perceptron and multi-layer perceptron. It is mainly used in model classification.

(2) BP neural network: back propagation learning algorithm is characterized by information forward propagation and error back propagation. That is, the information is transmitted from the input layer to the output layer. When the output value obtained by the output layer does not reach the expected value, the obtained error is transmitted back to all units of the input layer. In theory, BP neural network can realize any nonlinear mapping function and has self-learning ability. However, it takes a long time to learn, and the model training is more likely to fail.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202110_7(10).0031

3.2 Feedback neural networks (FNN)

Compared with feedforward neural network, feedback neural network increases the feedback of signal in feedback neural network. Each neuron was modeled by M-P model [3]. The most representative feedback neural network is Hopfield neural network. Because the connection of Hopfield network is fully connected, when the number of nodes is relatively large, the structure of the network is too complex, and there is no hidden layer in the network structure, which makes the nonlinear performance of the network poor, especially for complex nonlinear dynamic process systems, so its application is limited to a certain extent.

Hopfield neural network: Hopfield neural network is a single-layer fully connected feedback neural network. Each node is both input and output. That is, the input of each node at this time is the output of the previous time. The weight of the network is calculated, and once the weight is calculated, it will not change.

3.3 Self organizing neural networks (SOM)

Self organizing neural networks find the rules and relationships in the samples by themselves [4,5], and compete with each other for external stimuli among neurons. There is no fixed weight and output expectation in self-organizing neural network. Therefore, the network has the ability of self-learning, and the network learning is realized by competitive learning. The disadvantage of competitive learning is that when a neuron wins in the response to external stimuli, it will be more favorable in the subsequent competition. Therefore, some neurons may not be able to respond to external stimuli, resulting in the neuron becoming a god of death.

4. Chaos digital image encryption chaos

In the 1970s, as a new science, mixed purity theory entered a rapid development era.Chaos is a form of motion and exists in various fields such as nature, technical science and social science. It is a unique phenomenon in nonlinear dynamic systems. Mathematically speaking, if the initial value has been selected, the past state and long-term behavior in the dynamical system can be deduced. The images presented by hybrid purity seem chaotic, but in fact they are very regular. Chaos is a deterministic system, but it is difficult to predict, because its dynamic state is sensitive to the initial conditions. Chaos exists in complex systems and cannot be decomposed because of the topological characteristics of its copper dense orbits.

Chaos is a seemingly irregular process in nonlinear dynamic system. It is very sensitive to the initial value and has the characteristics of unpredictability, quasi randomness and good robustness. Shannon put forward two basic principles guiding password design as early as 1949, namely diffusion and chaos [6]. Chaotic image encryption matches the sensitivity of chaotic signal to initial value and quasi randomness with the requirements of digital image encryption. Therefore, many cryptographic researchers apply it to the process of digital image encryption, so as to improve the ability of anti statistical analysis and improve the security of ciphertext.

Logistic map and piecewise linear chaotic map are two common functions to generate chaotic sequences. Reference [7] proposed a chaotic image encryption algorithm based on improved logistic map. Through the improvement of modular operation of logistic map and bit reset of generated sequence, the newly generated sequence has better chaotic characteristics. Document [8] uses scrambling encryption, gray-scale transformation encryption and chaotic encryption to encrypt the picture at the same time. By comparing the correlation of adjacent pixels encrypted by different algorithms, it is found that the image security after chaotic encryption is stronger.

5. Image encryption based on chaotic neural network

As an intelligent information processing system, chaotic neural network is considered to realize real-world computing and is widely used in the study of high-dimensional nonlinear system dynamics. Chaotic neural network is based on the premise that there is chaos in human brain. Therefore, it has

ISSN: 2414-1895 DOI: 10.6919/ICJE.202110_7(10).0031

physiological basis and vitality. It has better performance than other existing models in associative memory and combinatorial optimization, and has great development potential.

Therefore, many scholars have applied chaos and neural network to digital image encryption in different ways and achieved good results. In the existing encryption algorithms, many scholars choose to train chaotic sequences with neural networks to eliminate the periodicity of chaotic sequences. This encryption method plays an important role in image scrambling in image encryption. The encryption process (as shown in Figure 2) can be summarized into three steps:

(1) Random array formation based on chaotic system;

(2) Random array learning and image scrambling based on artificial neural network;

(3) Image encryption based on piecewise differential diffusion.

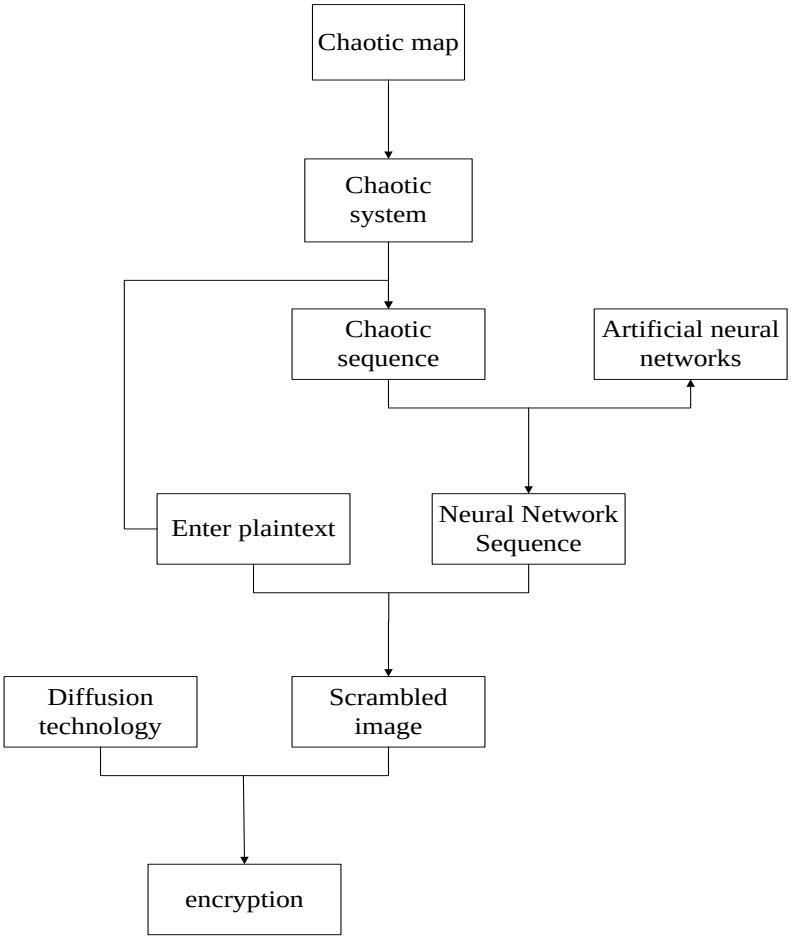

Figure 2. Encryption process

Many encryption algorithms use this encryption idea. For example, in reference [9], the chaotic sequence generated by Lorenz chaotic system is used as the input layer of neural network, and the neural network is trained to obtain two encrypted sequences, so as to complete the scrambling of image matrix. The image matrix is segmented, and the chaotic sequence with the same length and the number of sub matrices is generated by the chaotic system. The neural network is introduced to enhance the randomness of the chaotic sequence, and then the scrambled image is diffused. Complete the encryption of the image. In the encryption process, the initial value of chaotic system is independent of plaintext, so it is difficult to resist plaintext attack [10].

In the literature [11], the chaos system which is composed of sine, logistic and ten chaotic maps is improved to generate random array, in which the initial value of logistic map is related to the pixel point of image. Neural network is introduced to eliminate the periodicity of the pseudo-random array.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202110_7(10).0031

The output neural network sequence is used to scramble the plaintext. The segmented heterodiffusion technology is designed to change the pixel value and then complete the encryption. Because the key parameters are related to the pixel value of plaintext, it has good anti-differential attack. In addition, in order to prevent violent solution attacks, the key length in the encryption algorithm should be greater than that in 100 bit secret algorithm [12]. The encryption algorithm based on neural network and composite discrete chaos system proposed in document [13] is closely related to plaintext and the key length is more than 100 bits. In the literature [14], the chaos sequence is trained by using three-layer BP neural network, and the trained sequence is encrypted.

In document [15], a replacement image encryption algorithm based on BP neural network is proposed. The encrypted scrambling graph and the original image are different greatly, and the encryption effect is good, and the decrypted image is not significantly different from the original image. A hyperchaotic image encryption algorithm combining four-dimensional Hopfield neural network and AES encryption algorithm is proposed in document [16]. The shortcomings of the target key space caused by the encryption of images only by AES encryption algorithm are too small and fixed. The value of chaos sequence depends on the parameters of plaintext, so it can effectively resist the attack of clear text (ciphertext) image. The artificial neural network is introduced to eliminate its chaos periodicity, output the neural network sequence and chaos the plaintext. The image is classified, and the segmented heterodiffusion technology is designed to complete encryption.

In literature [17], the explicit mapping of Henon chaos is transformed into implicit mapping of neural network. Under the excitation of the same initial value and control rate, the chaotic neural network of both receiver and receiver can generate more hidden and unpredictable secret key stream of chaotic sequence asynchronously. It can realize the effective convergence of chaotic neural network, and avoid many inconveniences such as strict synchronization between the receiving and receiving ends in the chaotic synchronous communication.

In the literature [18], a dynamic self feedback chaos system is constructed as the key generating source; Different from the common scrambling methods, neural network is introduced to generate the scrambling matrix; And two rounds of pixel substitution are carried out to improve the ciphertext security. But there are two disadvantages in the implementation process: first, it can not achieve ergodicity when input layer I, diffusion matrix *G*, weight *W*, threshold b and initial control parameter matrix Q are randomly selected from sequence x (I); Second, the neural network has a long time to produce a complete scrambling matrix.

In recent years, although in Chaos Cryptography, the image encryption of chaotic neural network has achieved some relatively mature results, but there are still many shortcomings(1)The security performance of the algorithm has been improved in practical application, but it is difficult to design an algorithm with low encryption time, high security and easy to implement(2) Because the current chaotic image encryption algorithm is based on software simulation, according to the new information security technology, it is necessary to implement the image encryption through hardware in the practical application. This is still a problem we need to study. Whether it is based on the traditional cryptography method or the method based on chaotic neural network image encryption, the purpose of image encryption is to effectively encrypt the image, and thus ensure the security of image application and transmission. Therefore, in the future, neural network, cryptography theory and chaos theory can be closely linked.

6. Conclusion

This paper summarizes the methods of digital image encryption, digital image encryption based on chaos and digital image encryption based on neural network. This paper introduces two types of passwords. The structure of neural network and the development of neural network are introduced. With our continuous research on digital image encryption combined with chaos and neural network, digital image encryption technology will continue to improve.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202110_7(10).0031

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.

References

[1] Wang Yiting, Yin Xudong. Symmetric and asymmetric cryptosystems [J]. Office automation, 2021, 26(06): 16-17+42.

[2] Warren S. McCulloch and Walter Pitts. A logical calculus of the ideas immanent in nervous activity[J]. The Bulletin of Mathematical Biophysics, 1943, 5(4): 115-133.

[3] Xu Junbo, Xu Qingguo, Zhou Chuanguang, Zhao Wen. Progress of feedback neural network [J]. Chemical automation and instrumentation, 2003(01):6-10.

[4] Feng Xiangdong, Zhang Yuqin, Han Hongwei, Zhang Jianliang. Research on oil and gas stratification based on self-organizing neural network [J]. Computer technology and development, 2021,31(02):44-48.

[5] Adelaïde Nicole Kengnou Telem, Colince Meli Segning, Godpromesse Kenne, Hilaire Bertrand Fotsin, Martin Reisslein. A Simple and Robust Gray Image Encryption Scheme Using Chaotic Logistic Map and Artificial Neural Network [J]. Advances in Multimedia,2014,2014.

[6] C. E. Shannon. A Mathematical Theory of Communication[J]. 1948, 27(4) : 623-656.

[7] Zeng Xiangqiu, ye Ruisong. Chaotic image encryption algorithm based on improved logistic map [J/OL]. Computer engineering: 1-18 [2021-03-21]. http:// 221. 203. 21. 203: 8001/ rwt/ CNKI/ https/ MSYXTLUQPJUB/ 10.19678/j.issn.1000-3428.0059928.

[8] Liang Dongyun, Wu Xiaoyun, Liu Meng. Research on digital image encryption based on MATLAB [J]. System simulation technology, 2020, 16(04):248-251.

[9] Chen Sen, Xue Wei. Image encryption algorithm based on chaotic system and artificial neural network [J]. Computer system application, 2020,29(8): 236-241. DOI:10.15888/j.cnki.csa.007578.

[10] Junxin Chen, Zhi-liang Zhu, Li-bo Zhang, Yushu Zhang, Ben-qiang Yang. Exploiting self-adaptive permutation –diffusion and DNA random encoding for secure and efficient image encryption [J]. Signal Processing, 2018,142.

[11] ZHANG J, HOU D Z, REN H G.Image encryption algorithm based on dynamic dna coding and chen's hyperchaotic system [J]. Mathematical Problems in Engineering, 2016, 45 (20) :1011-1022.

[12] GONZALO ALVAREZ, SHUJUN LI. SOME BASIC CRYPTOGRAPHIC REQUIREMENTS FOR CHAOS-BASED CRYPTOSYSTEMS[J]. International Journal of Bifurcation and Chaos, 2006,16(8).

[13] Zhang Lijia, Liu Bo, Xin Xiangjun. Secure optical generalized filter bank multi-carrier system based on cubic constellation masked method.[J]. Optics letters, 2015,40(12).

[14] 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.

[15] Wang Lili, Gao Xincheng, Li Ruifang. Gray image scrambling and encryption method based on BP neural network [J]. Journal of Jiamusi University (NATURAL SCIENCE EDITION), 2014, 32(04):583-585.

[16] Chen S H,Liu H F,Hu Z H,et al.Simultaneous reconstruction and segmentation of dynamic PET via low-rank and sparse matrix decomposition [J]. IEEE Transactions on Biomedical Engineering, 2015, 62(7): 1784-1795.

[17] Luo Haibo, Ge bin, Wang Jie, Wu Bo. Image encryption of dynamic self feedback chaotic system integrating neural network scrambling image [J]. Chinese Journal of image graphics, 2018, 23(03): 346-361.

[18] Huang Li. Asynchronous encryption and decryption algorithm based on chaotic neural network [J]. Journal of Mianyang Normal University, 2019, 38(08):91-94+100.