Acta Scientific COMPUTER SCIENCES

Volume 5 Issue 1 January 2023

Review Article

A Review of Artificial Neural Network Based Block Cipher in China

Wanni Huang*

Department of Information Engineering, Guilin Institute of Information Technology, China

***Corresponding Author:** Wanni Huang, Department of Information Engineering, Guilin Institute of Information Technology, China.

Received: August 23, 2022

Published: December 13, 2022

Abstract

In the era of swift changes in technical information, the development of any technology should not be limited to the technology itself. In the age of rapid development of artificial intelligence technology, cryptography research should not be limited to traditional research based only on number theory. The combination of artificial neural networks and block cipher has essential value and significance for promoting the development of cryptography. The article takes the concept of chaos as the connection and entry point of cryptography and artificial neural network research and further elaborates on the research process of combining cryptography and artificial neural network. In addition, the article further discusses and summarizes the critical directions of the early research on chaotic block ciphers for academic circles in China. Finally, this paper analyzes and summarizes the new progress of neural networks and block cipher research in China. This paper aims to discuss the antecedents and current status of the research on neural network block ciphers and provide a reference for future research on neural network block ciphers.

Keywords: Chaos; Artificial neural network; Block cipher; Symmetric cipher; Encryption

Abbreviations

M-P Model: The M-P Model is a Model Named After the American scholars McCulloch and Pitts, Which is a Mathematical Model of Neurons Based on the Biological Nervous System; AES: Advanced Encryption Standard; DES: Data Encryption Standard; IDEA: International Data Encryption Algorithm; RC5: The RC5 Block Cipher Algorithm was Proposed by Professor Ronald L. Rivest of the Massachusetts Institute of Technology in 1994 and Named After Himself. The Full Name of RC5 is Rivest Cipher5; RC6: Rivest Cipher6; TEA: Tiny Encryption Algorithm; MLP: Multilayer Perceptron; CNN: Convolutional Neural Networks; ResNet: Residual Networks

Introduction

Data encryption technology is one of the essential technical means to ensure information security. The data encryption technology used in the work and life of human society today is mainly based on cryptography technology based on number theory. Cryptographic techniques based on number theory are divided into two broad categories of cryptographic systems. One is a symmetric encryption system, and the other is an asymmetric encryption system. The most significant difference between the two cryptosystems is that the symmetric encryption system uses the same encryption key and decryption key, which can also be called single-key encryption. The encryption key and decryption key used by the asymmetric encryption system are different, and the encryption key and the decryption key appear in pairs through mathematical derivation. In an asymmetric cryptosystem, either of the two keys can be used as a public or private key, but the private key must be kept secret and held by the recipient of the information. In studying the main differences between asymmetric and symmetric keys, it can be found that the computational time complexity of the two is different. According to previous research, under the premise of considering the same security requirements, the calculation time of asymmetric encryption will be longer than that of symmetric encryption under similar conditions.

Due to the relatively complex calculation of asymmetric encryption, these characteristics led to the dilemma of large computational power consumption and increased algorithm cost. Therefore, even if the symmetric encryption system has defects such as difficulty in critical distribution and management, from the perspective of low algorithm complexity and low promotion cost, the symmetric encryption system has research value and significance. Since the late 1980s, chaos has gradually been used in secure communications, among which the chaotic sequence password has attracted much attention [1]. On the other hand, because the thinking of the human brain is mainly within the boundary of chaos and order, it is difficult to simulate and evolve the neural network of the human brain through the classical artificial neural network, which gave birth to the development of the chaotic neural network [2]. With the deepening of research, the research of block cipher based on neural networks began to emerge, which enriched the vacancy in the research of block cipher based on artificial neural networks in China, and provided a reference for future in-depth research.

Artificial neural network is an important subject that has developed rapidly in recent years. Due to its advantages in structure and information processing characteristics, the application of artificial neural networks has been fruitful in recent years [3]. As one of the important technologies of traditional secure communication, cryptography can significantly promote the development of cryptography by using artificial neural network technology to solve problems in cryptography [3]. In the era of rapid changes in technical information, the development of technology should not be limited to the technology itself, and the powerful adaptation characteristics will directly affect the further replacement of any technology. In the era of rapid development of artificial intelligence technology, cryptography research should not be limited to research based on traditional number theory. The combination of artificial neural networks and cryptography has crucial practical value and significance.

Research background of artificial neural network and symmetric encryption

In this section, we first present the concept of the artificial neural network and then discuss the research significance of block cipher.

The concept of artificial neural network

In 1943, American scholars McCulloch and Pitts proposed the M-P model, establishing a mathematical model of neurons based on the biological nervous system. Since the advent of this model, artificial neural networks have gradually appeared in the academic field. The development of neural networks has gone through several important stages, namely single-layer neural network, discrete and continuous Hopfield Neural Network, Boltzmann Machine (BM), Chaotic Neural Network, deep belief network (DBN), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Generative Adversarial Network (GAN) model, etc. Although the development of neural networks is tortuous and diverse, one of the special networks mentioned above has chaotic commonalities with cryptography, that is, chaotic neural networks [4]. Chaos phenomenon can be understood as an inherent random performance of a nonlinear deterministic system, chaotic dynamics provide an opportunity for the study of artificial neural networks, and the fantastic and perfect characteristics of biological systems provide essential guidance for the study of chaotic neural networks [5]. With the development of the chaotic neural networks, there are mainly Global Coupled Mapping (GCM) models, Aihara chaotic neural network models, and neural network models in which the coupled chaotic oscillator is a single neuron structure [5], etc. The technology based on chaotic neural networks has been gradually applied to the research of information encryption, which provides an excellent reference value for the follow-up research of this paper.

Research significance of block cipher

At the beginning of the development of cryptography, it was developed based on the ideas of diffusion and confusion. The idea of diffusion and confusion is similar to that of chaos. Based on the idea of confusion and diffusion, the later symmetric cryptosystem came into being with the continuous development of cryptography. In the current Hyper Text Transfer Protocol over Secure Socket Layer environment, the information exchange and communication in the Internet environment uses a hybrid encryption method to ensure data security. This mode is a mixture of symmetric encryption and asymmetric encryption. In this hybrid encryption method, symmetric encryption is used to encrypt the message information in the channel, while asymmetric encryption is used to encrypt the symmetric encryption key. It can be seen that the symmetric encryption system plays an important role in the security of modern network information transmission. Symmetric encryption generally has two encryption classifications, one is sequence cipher, namely stream cipher. The other is the block cipher. The former is usually used for data confidentiality in secure network communications, especially in the application of data confidentiality

in national defense, state agencies, and other confidential departments [6]. The prominent feature of the sequence cipher is that it is encrypted bit by bit. Such characteristics make sequence ciphers have higher requirements on the correctness of each bit. In addition, a stream cipher is more suitable for hardware encryption, and the encryption speed is faster, but its advantages are not outstanding for software encryption. It can be seen that the development of block ciphers can effectively make up for the shortcomings of sequence ciphers [7]. A block cipher divides the plaintext into several data blocks and encrypts it using a round function and a key. One of the classic cipher structures of block ciphers is the Feistel cipher structure, which divides the plaintext into left and right parts and encrypts them using a round function and a key. The data encryption standard DES is a block cipher algorithm based entirely on the Feistel cipher structure. The advantage of the block cipher is that the key can be reused. In addition, when an error occurs in a certain block in the block cipher, it has less impact on the operation of subsequent blocks. More importantly, block ciphers are more suitable for software applications than stream ciphers [7]. Therefore, the research on block cipher has very important practical value and significance.

Development and research of block cipher based on artificial neural network

In this section, we first present the development of chaotic block ciphers and then discuss research on block ciphers based on artificial neural networks.

The development of chaotic block ciphers

Symmetric encryption is mainly divided into two types: stream cipher and block cipher. The well-known block ciphers' algorithms include the DES algorithm, Rijndael algorithm, in AES, IDEA, RC5/RC6, TEA Tiny Encryption Algorithm, etc. Since the 1980s, research based on chaos and block ciphers has gradually developed [8]. In 1989, Matthews, Pecora, Carroll, and others put forward the research on chaotic cryptography, respectively. Although chaotic ciphers face the risk of being broken, a small number of chaotic ciphers have withstood most of the external attacks [8]. In addition, systematic methods of chaotic ciphers are gradually formed. These systematic methods analyze the security of the system in more detail. Such systems include the aforementioned block ciphers. The structure of the S-box of such block ciphers is integrated into the chaotic system [8]. Since then, research on hybrid block ciphers has gradually increased. Quan Jingjing and others proposed using hyper-chaotic sequences to improve block cipher algorithms [9]. By introducing hyper-chaotic sequences, the effect of improving DES and AES algorithms was achieved, thereby realizing data encryption. Peng Fei and others introduced binary fractions to convert floating point operations into integer operations, thereby improving the efficiency of block cipher algorithms for chaotic systems. Gao Jie and others proposed a chaotic block cipher algorithm based on ciphertext and output mixed feedback [10,11]. Analyzing key space, key sensitivity, and differential attack (plaintext sensitivity test), proves that the algorithm can achieve high-security performance and high efficiency with only two rounds of iterations. Liu Jialing and others analyzed and improved the encryption algorithm based on an iterative chaotic map from the perspective of a plaintext attack [12]. The researchers proposed that the generation of the sub-key sequence requires the combination of the ciphertext and the data extracted from the chaotic mapping so that the subkey sequence satisfies the characteristics of uniform distribution and random statistics. Chen Shuai and others used an improved discrete map to generate subkeys, constructed a Feistel block encryption function for discrete chaotic operations, and proved through experiments that the single-byte discrete chaotic block cipher system is feasible to run on the nodes of wireless sensor networks [13]. Yan Lei and others proposed a block cipher based on chaotic state space search [14]. The cipher system hides the chaotic orbit information, which is quite different from the traditional Feistel block cipher. Han Rui and others proposed a chaotic block cipher algorithm based on the extended Feistel structure [15]. The S box in the algorithm is generated by the chaotic map, and the key algorithm is iteratively generated by the Cubic map. The experimental results show that this chaotic mapping algorithm has large key space, good diffusivity, and chaotic performance. Zheng Hao and others studied the effectiveness of chaotic block ciphers based on Feistel structure in resisting differential cipher attacks [16]. By comparing the fixed S-box and the dynamic S-box, it is analyzed that the Feistel-structured chaotic block cipher can resist the attack from the differential cipher more effectively. Aiming at the problem of dynamic S-box construction, Fan Minghui, *et al*. proposed a method to construct a dynamic S-box based on a Logistic chaotic map and Tent chaotic map and tested the bijectivity, nonlinearity, strict avalanche, and other aspects of the S-box [17]. With the analysis, the researchers prove the algorithm's security through the above analysis. According to the above analysis, we can

be seen that domestic research on chaotic block ciphers focuses on chaotic systems [8,10], chaotic sequences [9], key spaces [11,15], Feistel block ciphers and image encryption algorithms [7,13-16] and other topics. Chaos is one of the important contents of neural network research. The research of chaotic block cipher provides the premise and foundation for the research and development of neural network block cipher. In 2007, Cheng Xu and others proposed a block cipher system based on a feedforward network [18]. The researchers constructed a mathematical model of a block cipher and implemented the above block cipher system based on a two-layer feedforward network. Simulation proves that the block cipher system has better security, chaos, and scalability.

Research on block ciphers based on artificial neural networks

Since 1995, there has been relatively little research on neural network block ciphers in China. In 1995, Du Shenghui and others discussed the design principles of block ciphers, pointed out some weaknesses of DES and IDEA block ciphers, and provided a reference for subsequent research on artificial neural network block ciphers [19]. In addition, Du Shenghui, *et al*. also proposed a multilayer Hopfield neural network in 1995 [20]. The researchers pointed out that each network of the memory Hopfield neural network is reversible at runtime, and its inverse transformation is also the same type of transformation. The properties of multilayer Hopfield neural networks with memory are suitable for constructing block ciphers. In 2016, Qi Rui, *et al*. proposed introducing the nonlinear and random characteristics of the chaotic mechanism into the cryptographic system, which can effectively strengthen the confidentiality of information [21]. The researchers constructed a relatively complete artificial neural network block cipher system based on a discrete Hopfield neural network, which is simpler and more secure than DES. In 2020, Wang Kai, *et al*. proposed side channel analysis as one of the threats to the security of embedded cryptographic devices [22]. The researchers use the ability of the MLP neural network to extract features and use this feature to mine the profound relationship between energy leakage information and sensitive information and between energy leakage information and cryptographic data. In this study, the proposed MLP neural network is trained and tested by collecting the energy curve generated during the operation of the AES encryption algorithm. Through the above experiments, the training parameters and training time of the MLP neural network can be effectively reduced, and the number of energy curves required for key recovery can also be reduced. In 2022, Hou Zezhou, *et al*. proposed to focus on the differential analysis of block ciphers, using Convolutional Neural Network (CNN) and Residual Neural Network (ResNet) to train differential discriminators of two lightweight block cipher algorithms SIMON32 and SPECK32 [23]. In this study, it was found by comparison that ResNet performed better on the SIMON32 differential discriminator, while CNN performed better on the SPECK32 model. Secondly, the study also found that under the same conditions, increasing the number of convolutional layers of the CNN model and the number of residual blocks of the ResNet model will decrease the model's accuracy. Finally, the researchers pointed out that when selecting the construction model and parameters of the deep learning discriminator, the CNN model with low convolutional layers and the ResNet model with low residual blocks should be given priority.

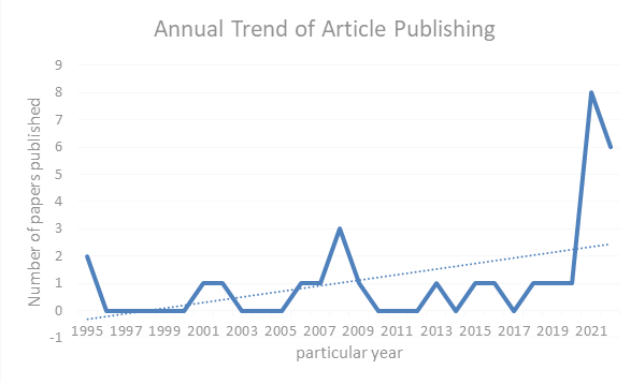

Figure 1: Overall trend analysis of block cipher research based on neural network.

The data in figure 1 above comes from the CNKI database in China. Through research, it is found that since 1995, the research on neural network block ciphers in the early stage mainly focuses on the characteristics of chaotic mechanisms and the theme of multi-layer memory Hopfield neural network. In the past ten years, domestic research on neural network block ciphers has begun to study from the perspective of side-channel analysis, convolutional neural network training models, and deep learning.

Conclusion

The above research shows that the origin of the development of block ciphers based on artificial neural networks in China is closely

related to the theory of chaos. Chaos theory has an impact on the early development of artificial neural networks and the early development of cryptography. Therefore, the two theories that do not seem to intersect, artificial neural networks and block ciphers, have gradually begun to blend and develop with the continuous advancement of research on block ciphers based on artificial neural networks. In China, it was first based on the combination of the characteristics of the chaotic mechanism and the cryptographic system, and then based on the multi-layer neural network to construct block ciphers for analysis, and finally developed to the perspective of side-channel analysis, convolutional neural network training and other perspectives as the starting point to carry out research.

It can be seen from the above analysis that there are relatively few domestic researches on the fusion of artificial neural networks and block ciphers. In the earlier studies, the themes were mainly based on the broader chaos theory. With the development of technology, research topics are becoming more and more concentrated, and research directions are becoming more and more detailed. Although there are few research results in the initial research stage, the research results on neural networks and block ciphers have increased in recent years. Since chaos is the common connection point of artificial neural network and block cipher research in the initial study, if the research in this direction wants to be further developed, it is recommended to start from this point and then intensely discuss the chaos aspects of artificial neural network and block cipher [1,2]. It is possible to increase the coupling point between the two and increase the mutual influence between the

Bibliography

1. Yang Xin. "Application Research of Information Security Encryption System Based on Chaos Theory". Ph.D. dissertation, Chongqing University (2008).

2. Qin Ke. "Eigen Analysis of Chaotic Neural Network and its Application in Pattern Recognition and Cryptography". Ph.D. dissertation, University of Electronic Science and Technology, (2010).

3. Lin Maoqiong, *et al*. "The Application of Neural Network in the Field of Cryptography". *Computer Application Research* 4 (2002): 8-10, 20.

4. Ge Zhaocheng and Hu Hanping. "Intersection of Neural Networks and Cryptography". *Chinese Journal of Cryptography* 8.2 (2021): 215-231.

5. Shi Yuanding and Wang Jianhua. "Research Progress of Chaotic Neural Network". *Microcomputer Development* 6 (2002): 33-35, 39.

6. Zhao Shilei, *et al*. "Research on Stream Cipher Algorithm, Architecture and Hardware Implementation". *Journal of Cryptography* 8.6 (2021): 1039-1057.

7. Lin Zhe. "Analysis, Design and Comparison of Block Cipher and Stream Cipher—Take AES and RC4 as Examples". *Commodities and Quality* S4 (2012): 313-314.

8. Tang Guoping. "Research on Chaotic Block Cipher and its Application". Ph.D. dissertation, Chongqing University (2005).

9. Quan Jingjing., *et al*. "Block Cipher Algorithm Based on Hyperchaotic Sequence and Its Application". *Journal of Nanjing University of Posts and Telecommunications* 4 (2005): 80-84.

10. Peng Fei and Qiu Shuisheng. "Research on a New Block Cipher Algorithm based on Chaotic Map". *Small and Microcomputer Systems* 12 (2007): 2162-2166.

11. Gao Jie, *et al*. "A Chaotic Image Encryption Algorithm based on Mixed Feedback". *Computer Applications* 2 (2008): 434-436.

12. Liu Jialing, *et al*. "Analysis and Improvement of a Class of Iterative Chaotic Block Ciphers". *Computer Science* 6 (2008): 141-144.

13. Chen Shuai, *et al*. "Research on Chaos Block Cipher for Wireless Sensor Networks". *Science in China (Series F: Information Science)* 39.3 (2009): 357-362.

14. Yan Lei and Wang Zhongxia. "A Chaotic Block Cipher Based on State Space Search". *Science and Technology Information* 20 (2010): 78-79.

15. Han Rui, *et al*. "Block Cipher Algorithm Based on Chaos Map". *Computer Engineering* 37.16 (2011): 120-122.

16. Zheng Hao, *et al*. "Anti-differential Cipher Attack Analysis of a Chaotic Block Cipher Based on Feistel Structure". *Journal of Beijing Institute of Electronic Science and Technology* 20.2 (2012): 60-66.

17. Fan Minghui and Yang Fengfan. "Dynamic S-box Construction based on Chaotic Mapping in Block Ciphers". *Radio Engineering* 46.3 (2016): 33-36, 40.

18. Cheng Xu and Zhao Xuemin. "A Block Cipher System based on Feedforward Network". *Computer Technology and Development* 1 (2007): 167-169.

19. Du Shenghui and Ruan Chuangai. "Block Cipher and Its Research". *Communication Technology and Development* 4 (1995): 45-49.

20. Du Shenghui and Ruan Chuangai. "Constructing Block Ciphers with Multilayer Hopfield Neural Networks". *Communication Secrecy* 1 (1995): 1-4.

21. Qi Rui, *et al*. "Symmetric Cryptosystem based on Neural NetWork". *Journal of Tsinghua University (Natural Science Edition)* 9 (2016): 89-93.

22. Wang Kai, *et al*. "Research on Energy Analysis of Block Cipher Algorithm Based on MLP Neural Network". *Computer Application Research* 4 (2020): 27-28.

23. Hou Zezhou, *et al*. "Research and Application of Deep Learning on Differential Discriminators of Block Ciphers". *Journal of Software* 33.5 (2022): 1893-1906.