Liang et al. EURASIP Journal on Wireless Communications and Networking (2019) 2019:151
https://doi.org/10.1186/s13638-019-1476-3

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Research on neural network chaotic encryption algorithm in wireless network security communication

Chen Liang[1,2], Qun Zhang[1*], Jianfeng Ma[2,3] and Kaiming Li[1]

Abstract

The rapid development of wireless network brings a lot of convenience to people's lives, but there are still many problems to be solved in wireless networks. Among them, communication security is the most critical, especially secure transactions on digital currency transactions are even more important. In traditional network communication encryption algorithms such as RSA and ECC, in order to further enhance the reliability of network communication security, the main means is to increase the length of the key, but this brings the complexity and workload of the calculation, and the speed of encryption cannot be realized. Compatible with security, the neural network chaotic encryption algorithm mainly uses the parallelity characteristics of the neural network and the chaotic dynamic characteristics to randomly generate a sequence, which has non-periodic characteristics. Therefore, the wireless network chaotic encryption algorithm is a good wireless communication security encryption algorithm. However, the traditional neural network chaotic encryption algorithm still has some shortcomings in its algorithm's security performance, encryption speed, encryption efficiency, and anti-deciphering performance. At the same time, the research on neural network chaotic encryption algorithm in wireless communication security is relatively less.
In this paper, the performance defect of the original neural network chaotic encryption algorithm is optimized. A dynamic key encryption and decryption neural network chaos algorithm for wireless communication security is proposed. The algorithm is mainly based on the Aihara neural network model and introduces chaos, mapping, and hybrid coding. At the end of the paper, the algorithms before and after optimization are compared. The experimental results show that the algorithm proposed in this paper has a significant improvement in the encryption and decryption speed and anti-deciphering ability of the key.

Keywords: Neural network, Chaotic encryption algorithm, Wireless communication, Communication security

1 Introduction

With the rapid development of communication technology, wireless communication technology has spread widely, but people must bear the risks brought by wireless networks while enjoying the convenience brought by wireless network communication. The main problems are mainly reflected in mobile terminal problems, communication link problems, and authentication system problems. The authentication system problem is communication security problem [1–3]. Wireless communication security issues are not only related to people's privacy and security, but also related to people's property security when conducting currency transactions on the network and even related to national defense security. The key to solving the security problem of wireless network communication lies in the application of encryption and decryption algorithms.

The traditional cryptographic technique is to protect the information by encrypting the readable file into unreadable garbled characters. The main features are four points: authenticity, integrity, confidentiality, and usability [4–6]. There are two main types of traditional cryptographic algorithms, symmetric and asymmetric. The symmetric algorithm is represented by the US data standard encryption algorithm [7]. This algorithm is exposed in the late stage, such as the key issue and

* Correspondence: zhangqunnus@gmail.com
[1]Institute of Information and Navigation, Air Force Engineering University, Xi'an 710051, China
Full list of author information is available at the end of the article

management is imperfect. The shortcomings of digital signature and authentication are provided, and the representative algorithm of the corresponding asymmetric algorithm is RSA algorithm [8]. The disadvantage of the algorithm is that the length of the key has reached 56 bits, which cannot meet the current wireless communication, password encryption, and decryption efficiency requirements. Compared with the improved algorithm of DES and RSA, IDEA [9] has further extended the length of the key, but the complexity brought by the excessively long key has become a drawback of its further development. The neural network chaotic encryption algorithm [10–12] mainly utilizes the basic features of mixing, strong sensitivity to parameters and initial values in chaos theory. In chaotic encryption algorithm, the early communication encryption chaos algorithm mainly has four types which are as follows: chaotic keying [13], chaotic expansion [14], chaotic parameter modulation [15], and chaotic masking [16]. The corresponding traditional chaotic encryption algorithm mainly includes the parameters and initial conditions of the logistic mapping proposed by Bianoo et al., and the partial key is used to encrypt each character in the information signal by the number of iterations of the mapping, but the number of iterations. The speed of its encryption is affected, and the encryption efficiency is not high [17]. Gotz proposed a discrete-time continuous numerical cryptosystem, which has better output distribution characteristics, but it has the disadvantage of poor password deciphering ability [18]. Therefore, it is very necessary and meaningful to study an excellent neural network chaotic encryption algorithm for communication security, especially wireless network communication security.

1.1 Related work

Aiming at the shortcomings of traditional neural network chaotic encryption algorithm, this paper proposes an optimization algorithm based on Aihara network model and chaotic mapping and hybrid coding. Finally, the traditional neural network chaotic encryption algorithm is compared with the optimization algorithm proposed in this paper. The main parameters include ciphertext independence, balance test, and encryption speed. Experimental results show that the proposed algorithm is superior to traditional algorithms.

The structure of this paper is organized as follows: In the second section of this paper, the wireless network security communication is analyzed. The basic principle and application method of neural network chaotic encryption algorithm are analyzed and discussed. The third section of this paper focuses on the optimization algorithm proposed in this paper. The fourth section carries out algorithm verification experiments and comparative analysis and draws conclusions.

2 Methods

2.1 Wireless network security communication

The rapid development of wireless networks has brought convenience to people, but the security problems in wireless communication are also plaguing people. The main problems are mainly reflected in three points:

1. There is a problem with the mobile terminal

There are many kinds of mobile terminals for wireless networks. The corresponding wireless network can also provide services according to the personalized needs of users, so as to ensure better access to the wireless network, but the access of a large number of users will inevitably require the broadband and speed of the terminal. With the increasing number of users of wireless networks, the relationship between their terminals and users is getting closer and closer, and the problems of the terminals are exposed.

2. Problems with network links

The transmission link of the current wireless network is poor in fault tolerance [19], which makes it easy to cause data transmission errors, which may result in leakage of personal privacy of the user and may even pose a security risk to the property.

3. There is a problem with the authentication system

There are still loopholes in the authentication system for wireless communication, and there are many types of network technologies for wireless communication, and the network mode is not uniform. Therefore, it is difficult to unify the real-name authentication, which also poses a danger to the user's information security.

Based on the above problems, the corresponding solution strategies mainly have the following three points:

1. Optimize the wireless encryption security technology to build a wireless network security system

A complete wireless network security system is a necessary condition for ensuring the security of wireless communication. The most important one is to establish an optimized wireless communication security encryption algorithm and other measures, such as the security protection of the wireless terminal through the construction of a configurable system. It is also possible to ensure the security and reliability of wireless communication through the construction of the negotiation system.

2. Strengthen network security measures

When the user accesses the wireless network, certain targeted security protection measures are taken, and the auxiliary network security device is set to effectively prevent the security factors existing in the wireless terminal access process.

3. Improve the protection of wireless terminals

Make full use of the performance of the wireless terminal to ensure secure communication, pay attention to the update of the wireless terminal, and effectively improve and optimize its operating system. Strict circuit detection of wireless network terminals is needed to ensure that they accept the integrity of the information.

2.2 Neural network chaotic encryption algorithm in communication

There are two kinds of chaotic models of neural networks [20]. One is a neural network chaotic model based on artificial neurons. The corresponding equations are shown in Eq. 1, Eq. 2, and Eq. 3. The other is a cell-based neural network model based on unit cells. The essence is a hybrid nonlinear circuit composed of a linear circuit and a nonlinear circuit, and the corresponding equations are shown in Eqs. 4 and 5:

$$x_i(t) = \frac{1}{1 + e^{-y_i(t)/\varepsilon}} \tag{1}$$

$$y_i(t+1) = ky_i(t) + \alpha\left(\sum_{j=1, j\neq i}^{n} w_{ij}x_j(t) + I_i\right) \tag{2}$$

$$z_i(t+1) = (1-\beta)z_i(t)(i = 1, 2, 3...n) \tag{3}$$

$$x_{ij} = -x_{ij} + \sum_{C(k,i)\in s_t(i,j)} A(i, j; k, l) * y_{kl} + \sum_{C(k,i)\in s_t(i,j)} B(i, j; k, l) * U_M + z_j \tag{4}$$

$$y_{ij} = f(x_i) = \frac{1}{2}|x_{ij} + 1| - \frac{1}{2}|x_{ij} - 1| \tag{5}$$

Compared with the traditional discrete neural network, the chaotic neural network has more nonlinear dynamic characteristics and complexity, and its main features are reflected in chaotic dynamics. The chaotic dynamics are added to the neural network, which makes the whole neural network have strong sensitivity and dependence on the initial conditions, which makes the whole system appear random, and this randomness comes from the inside of the system. Chaotic neural networks also have synchronization characteristics, which are a basic characteristic of chaotic phenomena. When two neural networks are coupled, the two networks will be excitation sources, and both use the self-feedback method to gradually reduce the two synchronization errors between the two neural networks. Chaotic neural networks also have chaotic attracting factors, which describe a certain state of network operation, which is the stability factor of the network. It is the main internal driving force for the chaotic phenomenon of neural networks. The application of chaotic neural network encryption algorithm in communication mainly has the following three points:

1. The application of chaotic synchronization based on the characteristics of encryption communication is mainly represented by the fourth generation chaotic pulse synchronous encryption communication. The theoretical basis is the Chua's oscillator, and its equation can be expressed as shown in Eq. 6:

$$\begin{cases} x = a[y - x - f(x)] \\ y = x - y + z \\ z = -by - cz \end{cases} \tag{6}$$

where a, b, and c are constants and $f(x)$ is a piecewise function of the Chua diode, and its correspondence can be expressed as in Eq. 7:

$$f(x) = dx + \frac{1}{2}(g - d)(|x + 1| - |x - 1|) \tag{7}$$

The corresponding encryption flowchart is shown in the Fig. 1.

2. The application of chaotic sequences in encrypted communication is mainly based on the non-periodicity of sequence traces output by chaotic networks. The characteristics of nonlinearity and randomness, which cannot be accurately predicted, make it have the characteristics of being the main key, so that the approximate "one time, one secret" full confidentiality requirement can be guaranteed.
3. The application of chaotic factor-based neural network encryption in communication is mainly based on chaotic attractors. There are two main types: one is probability-type symmetric encryption, and its corresponding encryption process is shown in Fig. 2. One is for unstable periodic orbital encryption. Such an encryption algorithm has certain security if it is based on a large number of neurons, but it is easily deciphered under the attack of an exhaustive method.

3 Optimized neural network chaotic encryption algorithm

3.1 Basic principle analysis and optimization algorithm

The traditional neural network chaotic encryption algorithm derives its algebraic structure from chaotic dynamics,

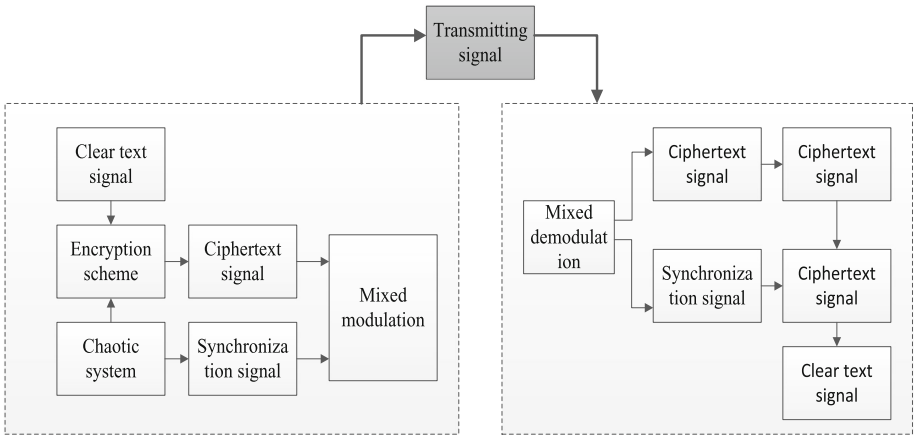

Fig. 1 The corresponding encryption flowchart. The figure shows the neural network encryption algorithm flowchart

chaotic attractors, and structural features of the attracting domain. The traditional neural network chaotic encryption algorithm is based on the chaotic attractor in the saturated Hopfield neural network as the relationship between the key and the ciphertext. The final result is a chaotic neural network-based security compared with the traditional encryption algorithm. The public key encryption algorithm, whose corresponding neural network energy function, is shown in Eq. 8:

$$E(t) = -\frac{1}{2}\sum_{ij} T_{ij} S_i(t) S_j(t) \tag{8}$$

A monotonic decrease in the energy function will cause the steady state of the entire algorithm to occur, and this steady state is also called an attractor. The corresponding algorithm flow chart is shown in Fig. 3.

The first step in the encryption process is to determine the key, which is obtained by transforming the large matrix. It requires each group of communication users to select a joint synapse matrix to form a singular matrix with a coefficient m. A transformation matrix is randomly selected in the m matrix, so that the user can combine the private key of the user with the public key of the information exchange to obtain a public key between each other. Then, after determining the key, the code of the readable plaintext is processed, and the plaintext content is mapped into the coded plaintext set according to the provided coding matrix M and the corresponding attractor. The third step is to iteratively calculate and derive a steady state. The corresponding decryption proceeds in reverse order of the encryption step, which is illustrated below by an example consisting of 8 neurons, where T_0 is the synapse matrix.

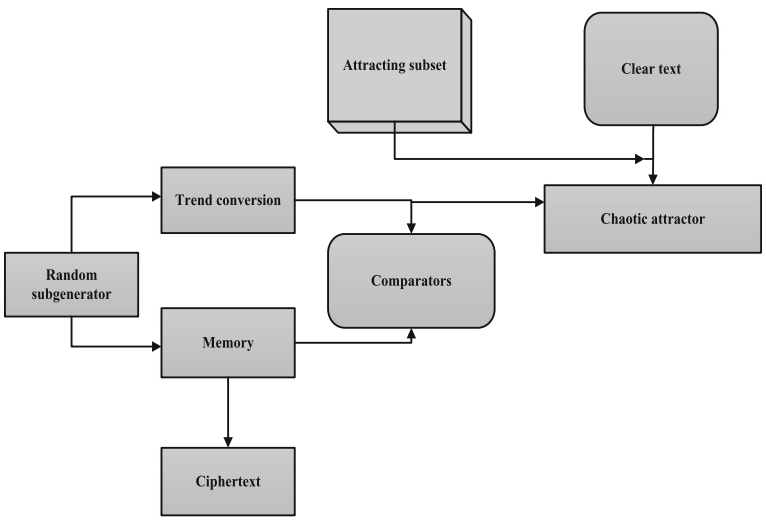

Fig. 2 Encryption process. The figure shows the neural network encryption algorithm process

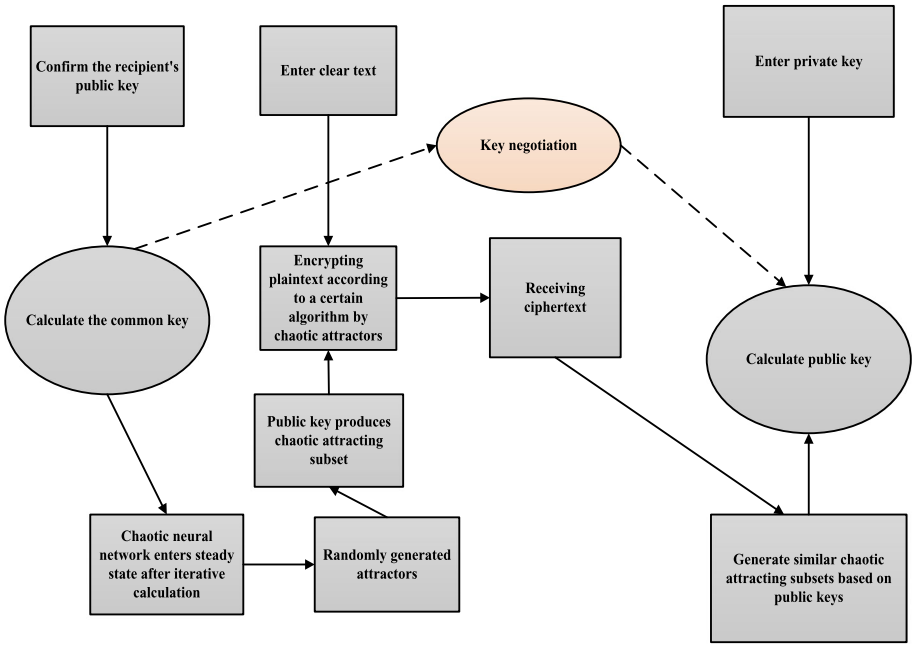

Fig. 3 Algorithm flowchart. The figure shows the traditional neural network chaotic encryption algorithm

$$T_0 = \begin{vmatrix} 1 & -1 & 0 & 1 \\ -1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{vmatrix} \quad (9)$$

$$P_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad P_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (10)$$

Then, the corresponding user and the sender's private key are respectively the following matrices P_1 and P_2, and the corresponding matrix is as shown in Eq.10:

To do the public key transformation, the final available Formula 11 is the common key for communication between the two parties.

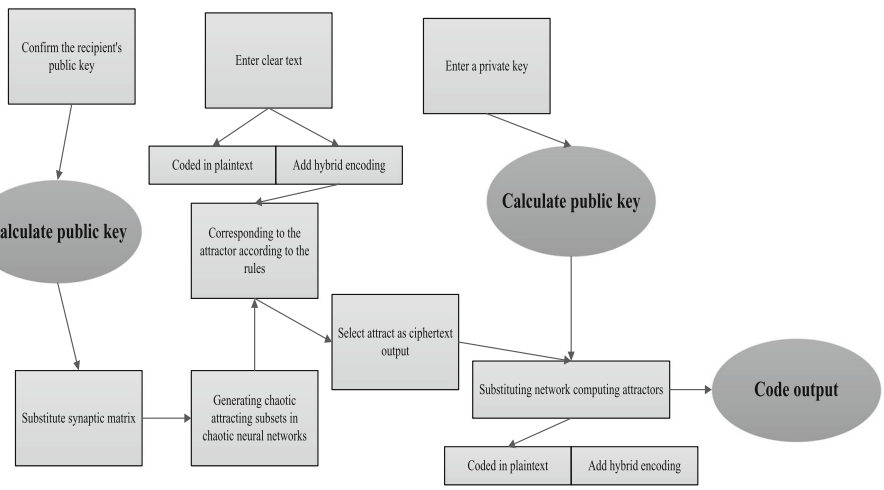

Fig. 4 The improved algorithm flow chart. The figure shows the improved algorithm encryption algorithm, which is mainly based on Aihara neural network and introduces chaotic mapping

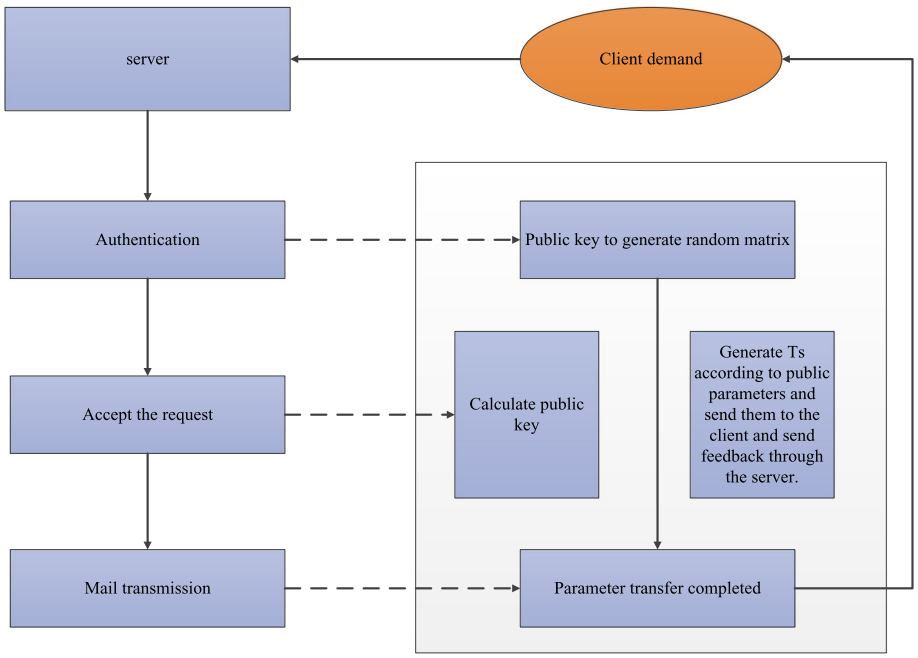

Fig. 5 Application flow chart on the wireless communication server side. The figure shows the application flow chart on the wireless communication server side

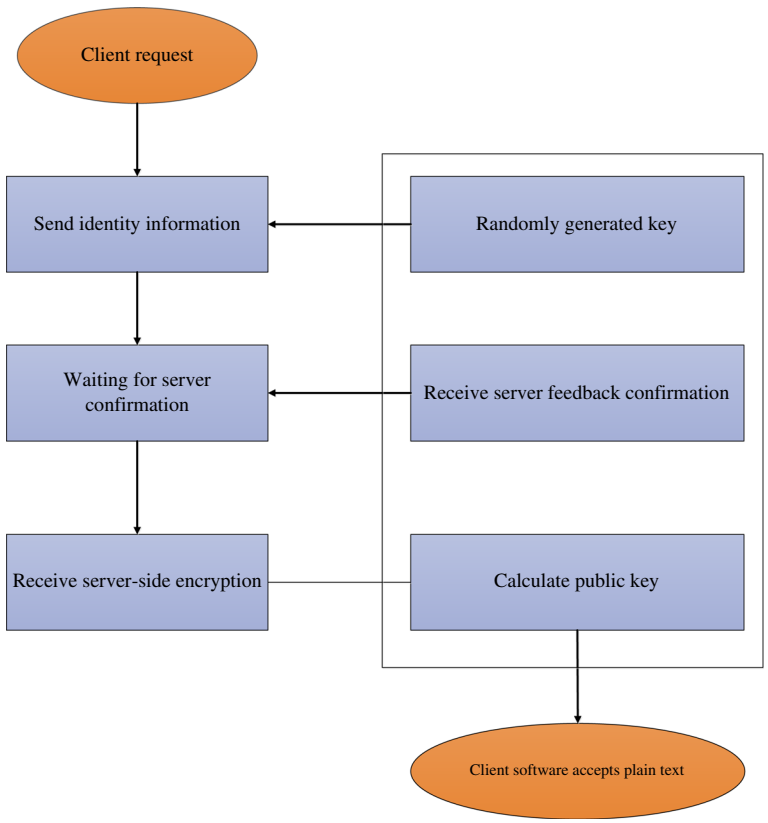

Fig. 6 The corresponding application algorithm flow chart of the client. The figure shows how to calculate the attractor and attract the domain and finally output the ciphertext to the client

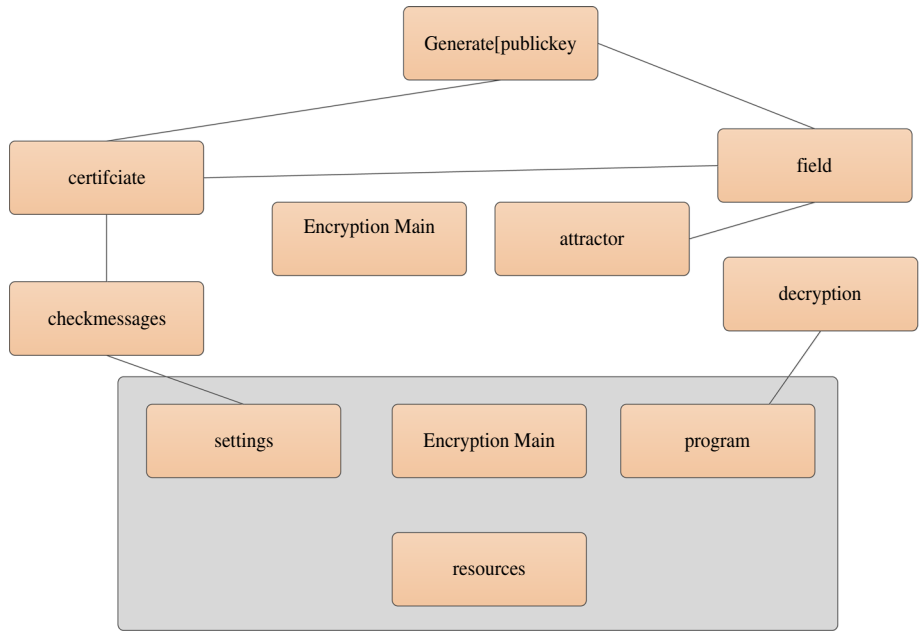

Fig. 7 The corresponding program class diagram. The figure shows the algorithm implementation process based on the VS software platform

$$T\hat{T} = H_r H_s T_0 H' H_\tau' = \begin{pmatrix} 1 & -1 & 0 & -1 \\ -1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ -1 & 1 & 0 & 1 \end{pmatrix} \quad (11)$$

Although the above algorithm can provide a secure key, it still has no good security for matrix decomposition attacks and statistics-based brute force attacks. Analysis of its root causes can be summarized as the following three points:

1. Avalanche effect is not ideal

When an output is randomly selected from the traditional chaotic encryption algorithm, the ciphertext will have at most eight direct changes, and the remaining ciphertexts will undergo an indirect random form change, which is probabilistically distributed and does not change with the plaintext. However, the diffusion characteristics are not high, so the avalanche effect is not ideal.

2. The encryption speed is slow

When the number of bits is extended to more than 8 bits, the chaotic encryption algorithm will increase the complexity and calculation amount of the entire encryption key, which is not conducive to the improvement of the encryption speed of the whole algorithm and affects the encryption efficiency.

3. Weak anti-deciphering ability

When subjected to attacks such as matrix decomposition, the corresponding password will be destroyed or even cracked. The main reason is that there is a problem in the selection of its neural network and the selection on the corresponding domain.

Table 1 The corresponding comparison table of encryption efficiency in PDF file mode

PDF file size (1.8 MB)		
Testing frequency	Optimization algorithm proposed in this paper (seconds)	Traditional algorithm (seconds)
1	17	15
2	14	14
3	16	17
4	17	17
Average	16	15.75

Table 2 TXT file data test

TXT file size (0.8 MB)		
Testing frequency	Optimization algorithm proposed in this paper (seconds)	Traditional algorithm (seconds)
1	7.9	6.1
2	6.4	6.5
3	6.3	6.4
4	6.9	6.2
Average	6.875	6.3

Table 3 The avalanche corresponding to the improved algorithm

Testing frequency	Optimization algorithm proposed in this paper	Traditional algorithm
1	37.11	26.12
2	38.15	27.93
3	37.59	28.32
4	37.06	26.11
5	36.79	25.11
Average	37.34	26.718

Based on the above problems, this paper proposes an optimization algorithm based on this algorithm, which is mainly based on Aihara neural network, and introduces chaotic mapping and hybrid coding technology. The improved algorithm flow chart is shown in Fig. 4:

The first step of the algorithm is unchanged from the original algorithm. The key receiver is still determined for the large matrix exchange, using the formula Ta = HaToHa′, and then Ha is treated confidentially. The corresponding second step is readable plaintext processing, where the optimization of the binary stream encoding method is mainly carried out here. The third step is mainly the generation of ciphertext. This paper mainly uses the magnified chaotic map to select the attracting domain and use it as the output of ciphertext. In this paper, the logistic map is used to select the attracting domain. The initial value of the logistic equation is set to the current microsecond time, and then iteratively magnified to obtain the modulo value, so that chaotic mapping can be realized by logistic, thus improving the random selection. The reliability increases the difficulty of external deciphering. In the improvement of the effect of the avalanche effect, the optimization scheme proposed in this paper adopts hybrid coding when encoding the plaintext. The essence is that the coding of each bit is directly generated by the directly affected code, and the corresponding formula is generated. For Eq. 12:

$$\mathrm{code}[i] = (\mathrm{code}[i] + \mathrm{code}[i-j]\%\mathrm{range}) \tag{12}$$

For the above-mentioned network composed of 8 neurons, the probability of the corresponding ciphertext change will be increased as shown in Eq. 13 when the optimization algorithm proposed in this paper is used for encryption processing:

$$\begin{aligned}\mathrm{prob}(\mathrm{cipher}) = {} & \mathrm{prob}(\mathrm{domain}) \\ & \times \left(\frac{\dim + (1/8) * \ \dim * n}{n}\right) \\ & + \mathrm{prob}(\mathrm{domain})\mathrm{prob}(\mathrm{code})\end{aligned} \tag{13}$$

The probability of the corresponding impact on the ciphertext after adding the hybrid coding is as shown in Eq. 14:

$$\begin{aligned}\mathrm{prob}(\mathrm{code}) = {} & \min(\mathrm{prob}(X_0) + \mathrm{prob}(X_1) + \ldots \mathrm{prob}(X_i)) \\ & * \frac{\dim - 1}{\dim}\end{aligned} \tag{14}$$

The internal state of the neural network Aihara based on this paper will gradually become stable after several rounds of iteration. Therefore, in the process of encrypting the plaintext, if the external input coding prototype of the neuron is set to plaintext, the neural network jumps out. Local attractors will be of great help, further enhancing their ability to resist matrix cracking attacks and statistical probability attacks.

3.2 Application of algorithm in wireless communication security

In the field of wireless communication security, the services provided by cryptography are required to be mainly confidential, authenticated, and plaintext integrity. Based on the algorithm of this paper, its application flow chart on the wireless communication server side is shown in Fig. 5.

In Fig. 5, the wireless network server first responds to the user's request with the corresponding module, performs user authentication, and then obtains the public key password of the user identity information after the verification succeeds, and then, the server encodes according to the algorithm, through the synapse matrix, to calculate the attractor and attract the domain and finally outputs the ciphertext to the client.

The corresponding application algorithm flow chart of the client is shown in Fig. 6.

4 Experimental

4.1 Implementation of the algorithm

Based on the above theoretical analysis of the algorithm, based on the VS software platform, the program is implemented in this paper. The corresponding program is composed of three modules, which are as follows: key calculation module, encryption and decryption module, and interface. The corresponding program class diagram is shown in Fig. 7.

4.2 Efficiency analysis

In this paper, we select a data below 5M in the efficiency test direction to compare the encryption test of the algorithm before and after the improvement. The corresponding comparison table of encryption efficiency in PDF file mode is shown in Table 1.

The corresponding encryption efficiency corresponding to the TXT file mode is shown in Table 2.

It can be clearly seen from Tables 1 and 2 that the improved algorithm is superior to the conventional algorithm.

4.3 Avalanche effect test

In the avalanche effect test, the detection algorithm is mainly responsible for the effectiveness of the key replacement. The excellent cryptographic algorithm should have an avalanche effect on the key transformation and keep its plaintext unchanged. Table 3 is the avalanche corresponding to the improved algorithm. Test comparison of effects:

It can be clearly seen from the table that the avalanche effect of the improved algorithm is significantly better than the avalanche effect before the improvement.

5 Results and discussion

Wireless communication network security is an important issue that affects people's daily privacy information and even property security. Neural network chaotic encryption algorithm has great advantages in improving the security of wireless communication, but the traditional chaotic encryption algorithm has low encryption efficiency. Based on the poor decoding ability and the avalanche effect, this paper proposes an improved optimization algorithm based on Aihara neural network and introduces chaotic mapping and hybrid coding technology. Based on this, the improved algorithm is compared with the traditional one. The performance of the algorithm has improved a lot. Experiments show that the optimization algorithm proposed in this paper has obvious advantages.

Abbreviations

DES: Data Encrytion Standard; ECC: Elliptic Curves Cryptography; NSFC: Natural Science Foundation of China; RSA: Rivest-Shamir-Adleman; US: United States

Acknowledgements

The Key Program of NSFC Grant (U1405255)
Shaanxi Science & Technology Coordination & Innovation Project (2016TZC-G-6-3)
The Fundamental Research Funds for the Central Universities (SA-ZD161504)
The National Natural Science Foundation of China: 61701530

About the authors

Chen Liang was born in Shiyan, Hubei, China, in 1992. He received the M.S. degree in Computer Application Technology from the College of Air and Missile Defense, Air Force Engineering University (AFEU), Xi'an, China, in 2017. He is currently pursuing the Ph.D. degree in Cyberspace Security. His research interest is wireless network security.

Qun Zhang (M'02–SM'07) received the M.S. degree in Mathematics from Shaanxi Normal University, Xi'an, China, in 1988, and the Ph.D. degree in Electrical Engineering from Xidian University, Xi'an, in 2001. He was a Research Engineer from 2001 to 2003 and a Research Fellow from 2005 to 2006 with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. He has published two books and over 200 papers in journals and conferences. His main research interests include signal processing, clutter suppression, and its application in SAR and ISAR.

Jianfeng-Ma received the B.S. degree in Computer Science from Shaanxi Normal University in 1982 and the M.S. and Ph.D. degrees in Computer Science from Xidian University in 1992 and 1995, respectively. He is currently a Professor with the School of Cyber Engineering, Xidian University. He has authored over 150 journal and conference papers. His research interests include information security, cryptography, and network security.

Kai-Ming Li received the M.S. degree in Electrical Engineering from the Institute of Telecommunication Engineering, Air Force Engineering University (AFEU), Xi'an, China, in 2009, and the Ph.D. degree in Electrical Engineering from the Institute of Information and Navigation, AFEU, Xi'an, in 2016. He is currently with the Institute of Information and Navigation, AFEU, as a Lecturer, and is also a Post-Doctoral Fellow with AFEU. He has published over 20 papers in journals and conferences. His research interests include signal processing and autotarget recognition in SAR and ISAR.

Authors' contributions

All authors read and approved the final manuscript.

Funding

The Key Program of NSFC Grant (U1405255)
Shaanxi Science & Technology Coordination & Innovation Project (2016TZC-G-6-3)
the Fundamental Research Funds for the Central Universities (SA-ZD161504)
The National Natural Science Foundation of China: 61701530

Availability of data and materials

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Ethics approval and consent to participate

This study does not involve any ethical research.

Consent for publication

All authors agree to publish this paper.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Institute of Information and Navigation, Air Force Engineering University, Xi'an 710051, China. [2]School of Cyber Engineering, Xidian University, Xi'an 710026, China. [3]Shaanxi Key Laboratory of Network and System Security, Xi'an 710071, China.

Received: 28 December 2018 Accepted: 22 May 2019
Published online: 06 June 2019

References

1. G. Maddodi, A. Awad, D. Awad, et al., A new image encryption algorithm based on heterogeneous chaotic neural network generator and dna encoding. Multimed. Tools Appl. **77**(19), 24701–24725 (2018)
2. M. Dridi, M.A. Hajjaji, B. Bouallegue, et al., Cryptography of medical images based on a combination between chaotic and neural network. IET Image Process. **10**(11), 830–839 (2017)
3. D.J. Li, Y.Y. Li, J.X. Li, et al., Gesture recognition based on BP neural network improved by chaotic genetic algorithm. Int. J. Autom. Comput. **15**(3), 1–10 (2018)
4. Y. Cui, Z. Zhao, Y. Ma, et al., Resource allocation algorithm design of high quality of service based on chaotic neural network in wireless communication technology. Clust. Comput. **20**(3), 1–13 (2017)
5. S. Li, Z. Yu, Z. Ming, et al., Hot oil pipeline simulation based on chaotic particle swarm optimized RBF neural network. Nanotechnol. Precis. Eng. **15**(3), 181–186 (2017)
6. Y. He, Y.Q. Zhang, X.Y. Wang, A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system. Neural Comput. & Applic. **30**(3), 1–14 (2018)
7. F. Han, X. Liao, B. Yang, et al., A hybrid scheme for self-adaptive double color-image encryption. Multimed. Tools Appl. **77**(11), 14285-14304 (2018)
8. D. Wei, Network traffic prediction based on RBF neural network optimized by improved gravitation search algorithm. Neural Comput. & Applic. **28**, 1–10 (2016)
9. B. R. Gangadari, S. R. Ahamed, Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications. Healthcare Technology Letters. **3**(3), 177–183 (2016)
10. C. Chen, L. Liu, T. Qiu, et al., Zhiyuan Ren, Driver's Intention Identification and Risk Evaluation at Intersections in the Internet of Vehicles. IEEE Trans. IoT., **5** (3), 1575–1587 (2018)
11. B. Islam, Z. Baharudin, P. Nallagownden, Development of chaotically improved meta-heuristics and modified BP neural network-based model for electrical energy demand prediction in smart grid. Neural Comput. & Applic. **28**(Suppl 1), 877-891 (2017)

12. J.C. Ban, C.H. Chang, S.S. Lin, On the structure of multi-layer cellular neural networks. J. Differ. Equ. **252**(8), 4563–4597 (2012)
13. S. Lakshmanan, M. Prakash, C.P. Lim, et al., Synchronization of an inertial neural network with time-varying delays and its application to secure communication. IEEE Trans. Neural Netw. Learn. Syst. **29**(1), 195–207 (2016)
14. J. Chen, P.C. Wei, W. Zhang, et al., Construct hash function based on RBF neural network and chaotic map. Comput. Sci. **33**(8), 198–201 (2006)
15. J.S.A.E. Fouda, J.Y. Effa, S.L. Sabat, et al., A fast chaotic block cipher for image encryption. Commun. Nonlinear Sci. Numer. Simul. **19**(3), 578–588 (2014)
16. P. Zhen, G. Zhao, L. Min, et al., Chaos-based image encryption scheme combining DNA coding and entropy. Multimed. Tools Appl. **75**(11), 6303–6319 (2016)
17. M. Boussif, N. Aloui, A. Cherif, Smartphone application for medical images secured exchange based on encryption using the matrix product and the exclusive addition. IET Image Process. **11**(11), 1020-1026 (2017)
18. J. Peng, Z.M. Yang, S.Z. Jin, et al., Image encryption algorithm using spatio-temporal chaotic sequences based on CNN and CML. Appl. Res. Comput. **24**(8), 159–161 (2007)
19. F.H. Hsiao, Applying elliptic curve cryptography to a chaotic synchronisation system: neural-network-based approach. Int. J. Syst. Sci. **48**(1), 1–16 (2017)
20. L. Tang, Y. Gao, Y.J. Liu, Adaptive near optimal neural control for a class of discrete-time chaotic system. Neural Comput. & Applic. **25**(5), 1111–1117 (2014)

6 Publisher's Note