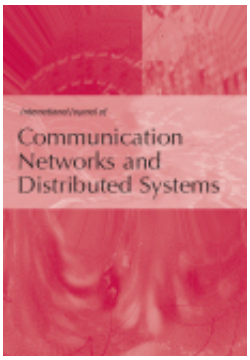


International Journal of Communication Networks and Distributed Systems

ISSN online: 1754-3924 - ISSN print: 1754-3916
https://www.inderscience.com/ijcnds

Research on an optimised encryption algorithm for network information security communication

Ju Li

DOI: 10.1504/IJCNDS.2022.10044390

Article History:
Received: 05 November 2021
Accepted: 14 December 2021
Published online: 06 December 2022

Research on an optimised encryption algorithm for network information security communication

Ju Li

Chongqing Technology and Business Institute,
Chongqing 401520, China
Email: juxian032562871@163.com

Abstract: At present, one of the commonly used encryption algorithms is the block cipher AES method, while in the design, we often only consider the bounded attack opponent, but in the face of the needs of the development of artificial intelligence, it is difficult to meet the secure communication of network information. This time, an optimised and improved GANs encryption algorithm based on neural network is proposed. The encryption algorithm can improve the objective function and learning model, so as to achieve better algorithm security performance. Through simulation analysis, it can also be seen that with the increase of training times, the neural network training effect of Bob, Alice and Eve is better. The proposed optimisation algorithm can realise face generation in the case of non-artificial knowledge, which has significant advantages compared with the traditional encryption algorithm.

Keywords: network information; safety; encryption algorithm; GANs model; neural network.

Reference to this paper should be made as follows: Li, J. (2023) 'Research on an optimised encryption algorithm for network information security communication', *Int. J. Communication Networks and Distributed Systems*, Vol. 29, No. 1, pp.31–46.

Biographical notes: Ju Li received his Master's degree from the Chongqing University of Posts and Telecommunications in 2015. He is an Associate Professor in the Chongqing Technology and Business Institute. He is interested in computer technology and network security.

1 Introduction

The development and popularisation of modern internet technology has brought the society into the era of network information explosion. People have realised a new industry development model through network information transmission, such as smart city, intelligent medical treatment, virtual reality technology and so on. These new technologies have higher and higher demand for wireless communication networks, of which the very important is the secure communication of network information (Yang et al., 2020). The security of data communication involves many contents, including security performance, cryptographic protocol, etc. among them, encryption technology is the key to realise information security (Shah et al., 2020). In order to realise the secure transmission of information between the sender and the receiver, people will allow the attacker to steal the communication information, but the plaintext information can not be

recovered from the stolen information (Tamilarasi and Jawahar, 2020). At present, the cost of common password systems such as 3DES and idea is high, and the running speed of the system is slow and the cost is high. The neural network can realise the construction of adaptive system through simple nonlinear calculation elements, and can simulate the human brain to calculate complex tasks. The neural network can show very good prediction performance (Wei et al., 2019). This time, neural network is introduced to optimise and improve the GANs encryption algorithm, and the security performance of the algorithm is improved through symmetric encryption technology.

With the rise of telemedicine technology, many medical images are transmitted with the internet. In order to protect the privacy of these data in the transmission process, Banik et al. proposed a confidential algorithm for medical images. This algorithm can effectively solve the problem of data expansion and can be applied to the encryption of multiple medical images (Banik et al., 2019). A security monitoring system of internet of things system based on video summarisation and image encryption proposed by Muhammad et al. can extract information frames by using a video security method by using the processing ability of visual sensors. Considering the requirements of system equipment storage and processing, a fast probability and lightweight key frame pre transmission encryption algorithm is designed and developed, the final experimental simulation results show that the method has robustness and security performance (Muhammad et al., 2018). At present, a large number of multimedia contents such as images, videos and texts are shared through the internet every day, and these contents may be invaded by hackers at any time. Raja proposes an encryption technology based on multi-scale transform and multi symmetric key. The algorithm makes comprehensive use of wavelet transform, band transform and curve transform, which can achieve good application results (Raja, 2019). Sundararajan et al. discussed the image security in the computer communication network. In order to realise the encryption of more multimedia content, partial encryption is adopted to achieve faster computing speed and improve the security level through lightweight fast algorithm (Sundararajan et al., 2019). Ji et al. proposed a multi-user cross layer security network. This is the first time to quantitatively analyse the security performance. In this method, eavesdroppers need to obtain the information they want, not only to obtain OCDMA optical code in the physical layer, but also to decipher the algorithm password in the data layer. This idea can effectively improve the information security (Ji et al., 2019).

Chen proposes a mobile intelligent data security model with homomorphic encryption algorithm. This technology is mainly to provide a unified edge computing solution for data users and provide reliable guarantee for users' data security (Chen, 2020). In the process of public channel transmission, image encryption technology is also very important. Many scholars have studied the plane graphics encryption technology of public network communication, and analysed its robustness, histogram and key sensitivity to verify the performance of the algorithm (Wang et al., 2019; Kumar and Raghava, 2021; Wang and Zhao, 2019). For wireless media and other information transmission with ultra dense broadcasting nature, it is easy to be attacked by malicious eavesdroppers (Chopra et al., 2019). Uchiteeva et al. proposed a pseudo-random secret key chain algorithm applied to radio transceivers. The algorithm has very good robustness against deceptive or violent attacks, and is suitable for large node networks in the industrial internet of things (Uchiteleva et al., 2020). Qian et al. proposed an extensive encrypted communication scheme, which adopts a more advanced encryption standard algorithm to achieve the high efficiency of the encryption algorithm, and avoids

the attacker's control or modified malicious instructions through the elliptic curve crypto digital signature algorithm (Qian et al., 2019). The communication of the medical industry has high requirements for the privacy protection of patients. The service of the medical service industry for patients not only stays in clinical treatment and consultation, but also needs to realise diversified and convenient comprehensive medical services (Fan et al., 2020). Dhanvijay and Patil designed an internet of things communication system applied to the medical industry. This method can effectively avoid the loss of signal information and ensure that patients' privacy will not be leaked (Dhanvijay and Patil, 2020). With the continuous development of quantum computer, optical confidentiality technology has become an encryption communication method that can be realised. In the optical communication system, Zhao et al. designed an encryption method using private chaotic phase scrambling. This scheme can reduce the communication delay and encrypt the whole network at the same time (Zhao et al., 2021). Vaseghi et al. proposed an encryption method for satellite imaging. In order to deal with the delay between transmitter and receiver in satellite communication, they designed a communication encryption method based on synchronous chaotic key (Vaseghi et al., 2021; Varma et al., 2021).

The key of cryptographic communication is to hide the information through key technology. Only the authorised person can decrypt and obtain the hidden information (Mathews, 2021). Patel et al. designed a cryptographic random number generator and used neural network technology to increase the randomness of the generator, which can improve the security of the key (Patel et al., 2021). The rise and application development of 5G technology is the inevitable trend of modern communication technology. In order to improve the security of 5G communication technology, Lu et al. (2019) designed a physical layer encryption algorithm based on chaotic sequence. In military applications, underwater network communication is an important application technology. Because the underwater acoustic channel has a strong spatial dependence on space, the attacker can simulate a small number of receivers to try to obtain the legitimate channel of the transmitter. Therefore, it is very important to encrypt the individual nodes in the network structure and increase the trusted nodes of the receiving nodes (Diamant et al., 2019). Amiruddin et al. designed a communication encryption algorithm based on improved scrambling factor and improved Fibonacci key generation algorithm to realise the communication encryption of data transmitted in communication network. This algorithm has increased randomness and belongs to lightweight computing algorithm (Amiruddin et al., 2019). Fu et al. proposed a network communication security technology based on quantum key distribution, which can be applied to more advanced 6G technology in the future to maximise the rate of security key through quantum device scheduling strategy (Fu et al., 2020; Yi et al., 2019). In order to meet the real-time and secure communication needs of multimedia, scholars have proposed many image confidentiality algorithms based on chaos, but these algorithms have many shortcomings in practical application (Nkandeu and Tiedeu, 2019). In the construction of modern secure communication mechanism, the internet of things plays an important role. The development of quantum technology has a good application prospect in communication security. As an excellent key generator, quantum walk has the characteristics of high sensitivity and can resist various attacks (El-Latif et al., 2020; Imran et al., 2020). Viswanathan and Kannan proposed an elliptic curve cryptosystem based on cyclic group. The model can effectively

reduce the effectiveness of the algorithm and improve the security of the algorithm (Viswanathan and Kannan, 2019).

Through the relevant research on network information security communication encryption algorithms at home and abroad, it can be seen that the current research status mainly focuses on the following two parts:

1 the encryption algorithm is aimed at the relatively complex image data in data transmission, more is the encryption transmission of images, while the data security transmission of the whole system network is relatively less.

2 at present, in the setting of network information security transmission, although various encryption algorithms are designed, their evaluation indexes are relatively simple and can not fully evaluate the performance of encryption algorithms.

Therefore, the generation countermeasure network structure is proposed this time, and the CAA algorithm is introduced based on neural network for optimisation and improvement (Han et al., 2018; Almalkawi et al., 2019; Liu et al., 2019; Fan et al., 2019; Chalee and Werasak, 2019). The main innovations of this time are as follows:

1 the algorithm model takes the attack behaviour as the corresponding defence scheme, which can ensure the security of the key used in network information communication

2 based on the countermeasure neural network, the data receiving, sending and the competitive confrontation of the attacker are realised, so as to improve its computing ability to resist decoding

3 build a security detection network structure to evaluate the security degree of data.

In terms of specific application, the intelligent algorithm proposed in this paper has significant self-learning ability, so it can achieve independent and automatic continuous evolution defence system, and has strong scalability. It can be predicted that it can have a certain application potential in artificial intelligence in the future.

2 GANs algorithm model structure

2.1 GANs algorithm model

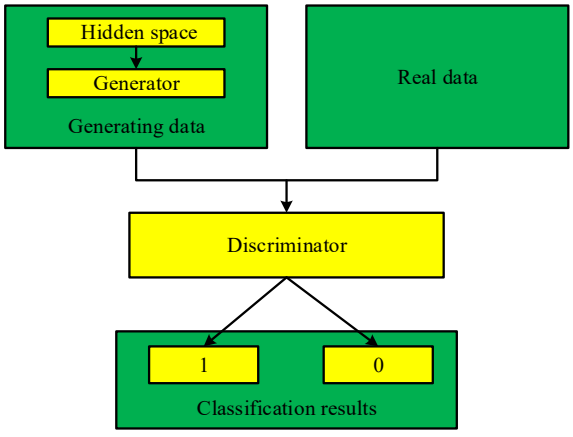
At present, there are many researches on counter neural networks. Most of the existing researches are on the message exchange in Alice and Bob neural networks. However, the decoding of Eve neural networks is greatly limited, and there is no special cryptographic algorithm or specific solution for these neural networks. Therefore, after analysing the operation mechanism of the algorithm, this research puts forward an improvement scheme for the existing shortcomings. Generative adversarial networks (GANs) is a data distribution generation algorithm in the form of confrontation. The algorithm model adopts the parallel data production mode, so it has a very fast production speed and has better advantages in the results. In the GANs algorithm model, the discriminator is represented by discrimination component D and the generator is represented by generation component G. Generator and discriminator compete with each other in order to achieve their own purposes, which is the origin of the antagonism of the algorithm (Tauhid et al., 2019). Generator G can generate false data according to the dependent

variable, and discriminator D will judge whether the data comes from the real data space or from generator G according to the input. If G determines that the input comes from the real data space, it will output a specific value. The implicit variable set in GANs is z, and in data space χ, the distribution of real data probability is expressed as $P_{data}(x)$; In the hidden space Z, the probability distribution of the hidden variable z is $p_z(z)$. Thus, GANs can be expressed by equation (1):

$$\min_G \max_D V(G, D) = \min_G \max_D E_{x\sim p_{data}}\left[\log D(x)\right] + E_{z\sim p_z}\left[\log\left(1 - D(z)\right)\right]. \tag{1}$$

In equation (1), $V(G, D)$ is a binary cross entropy function, and discriminator D classifies samples according to true and false, so this function is a special objective function. If the sample data comes from the real data, the analysis from the perspective of discriminator D is to maximise the real sample data; conversely, if the sample data comes from generator D, discriminator D will achieve a minimised output. If discriminator D receives a false sample, generator G will try to deceive it to maximise the D output. It can be seen from the comprehensive analysis that for function $V(G, D)$, discriminator D is to realise the maximisation function, and generator G is to realise the minimisation function. The principle structure diagram of GANs algorithm is shown in Figure 1.

Figure 1 The principle structure of GANs algorithm (see online version for colours)



If generator G and discriminator D have sufficient capacity space, the conditions for their balance are as follows:

$$p_{data}(x) = p_g(x). \tag{2}$$

In equation (2), $p_g(x)$ represents the data probability distribution provided by G. Let the optimal discriminator be D^*, so there are:

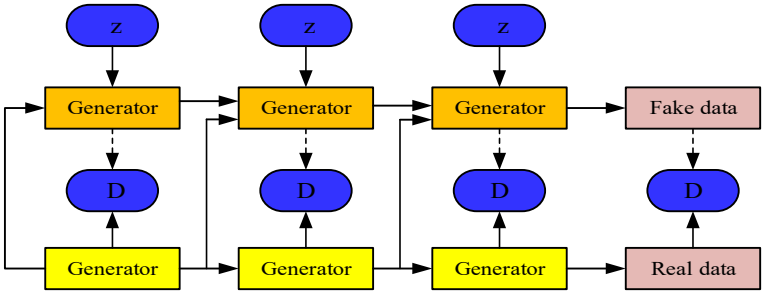
$$D^* = p_g(x) / \left(p_g(x) + p_{data}(x)\right). \tag{3}$$

By substituting equation (3) into equation (1), the Jensen Shannon divergence about $p_{data}(x)$ and $p_g(x)$ can be obtained.

GANs model has two typical structures: hierarchical structure and self-encoder structure. When dealing with the generation of high-resolution images, the hierarchical

structure can be used to generate images level by level and stage by stage, so as to improve the resolution. The common GANs model hierarchy is shown in Figure 2.

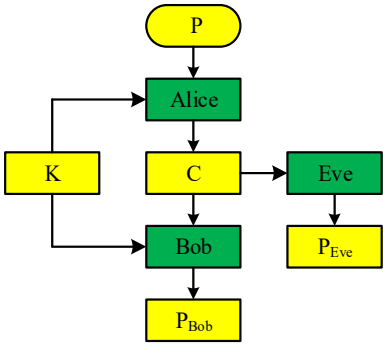
Figure 2 Typical hierarchical structure of GANs model (see online version for colours)



2.2 GANs encryption system architecture

In the scenic spot encryption scenario against neural network, Bob, Eve and Alice are included. Bob and Alice share the same key K and the transmission name is P. Eve is a passive attacker trying to eavesdrop on communication, that is, obtain the information of plaintext P through ciphertext C. These three agents are neural networks in the ANC system model. They are not bit sequences, but networks dealing with floating-point numbers. The symmetric encryption and decoding model composed of the three is shown in Figure 3.

Figure 3 ANC symmetric encryption and decoding model (see online version for colours)



Let Alice's parameter be θ_A, Bob's parameter be θ_B, Eve's parameter be θ_C, Alice's encryption input be $E_A(\theta_A, P, K)$, Bob's decryption output be $D_B(\theta_B, C, K)$, Eve's decryption output be $D_E(\theta_E, C)$. Let the length of plaintext be L, and define the distance L_1 between the real plaintext and the estimated value:

$$d(P, P)' = \frac{1}{N}\sum \left| Pi - p_i' \right|. \tag{4}$$

Eve is to accurately reconstruct plaintext P. the amount of error decoded by Eve is expressed by $L_E(\theta_A, \theta_E, P, K)$, and its loss function is defined as:

$$L_E(\theta_A, \theta_E, P, K) = d\left(P, D_E\left(\theta_E, E_A(\theta_A, P, K)\right)\right). \tag{5}$$

The loss function can be defined using an expected value:

$$L_E(\theta_A, \theta_E) = E_{P,K}\left[L_E(\theta_A, \theta_E, P, K)\right]. \tag{6}$$

The optimal Eve is achieved by minimising the loss, that is:

$$O_E(\theta_A) = \arg\min_{\theta_E}\left(L_E(\theta_A, \theta_E)\right). \tag{7}$$

Bob is optimally treated according to the idea of Eve optimality, so Bob's loss function can be defined:

$$L_B(\theta_A, \theta_B, P, K) = d\left(P, D_B\left(\theta_B, E_A(\theta_A, P, K), K\right)\right), \tag{8}$$

$$L_B(\theta_A, \theta_B) = E_{P,K}\left[L_B(\theta_A, \theta_B, P, K)\right]. \tag{9}$$

Determine the joint loss function of Bob and Alice in combination with the optimal value of L_B, L_E:

$$L_{AB}(\theta_A, \theta_B) = L_B(\theta_A, \theta_B) - L_E\left(\theta_A, O_E(\theta_A)\right). \tag{10}$$

By minimising $L_{AB}(\theta_A, \theta_B)$, Bob and Alice can be optimised:

$$(O_A, O_B) = \arg\min_{(\theta_A, \theta_B)} L_{AB}(\theta_A, \theta_B). \tag{11}$$

3 Improved algorithm of GANs encryption based on neural network

3.1 Network communication password security detection method

Common network communication password attacks mainly include the following: known ciphertext attack, known plaintext attack, selected ciphertext attack, selected plaintext attack, etc. they are sorted according to the attack intensity, which is shown as selected ciphertext attack > selected plaintext attack > known plaintext attack > known ciphertext attack. In cryptography, exclusive or (XOR) is a common binary non differentiable operation. It is necessary to use neural network to perform XOR operation internally to realise generalisation, so as to map bit 0 and bit 1 to angle 0 and angle π respectively. The mapping formula for defining bit b to angle is:

$$f(b) = \arccos(1 - 2b). \tag{12}$$

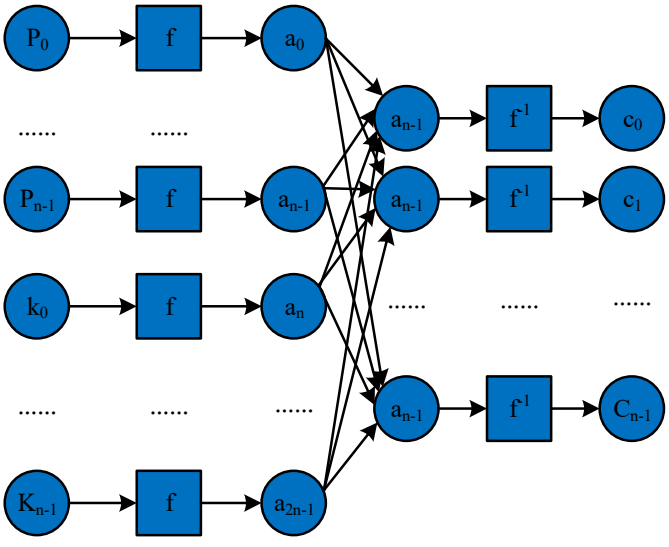
Further, a continuous bit mapping of the inverse angle a can be provided:

$$f^{-1}(a) = \frac{1 - \cos(a)}{2}. \tag{13}$$

By introducing it, an encryption detection network based on neural network can be obtained. In the communication network, the bit information can be transformed into angle information by equation (12) and used as the input of neural network. In the encryption detection network, the data processed are floating-point numbers between 0

and 1, not composed of bits. The typical structure of the encryption detection network is shown in Figure 4.

Figure 4 Typical structure diagram of encryption detection network (see online version for colours)



In the counter encryption network, the weight matrix of the hidden layer and convolution layer is redefined as W, the angle obtained by the plaintext and the key is a_0, a_1, …, a_{2n-1}, the output variable of the counter encryption network is h_0, h_1, …, h_{n-1}, and the n-bit vectors of the input plaintext, the input key and the output ciphertext are expressed as P, K, C respectively. Therefore, the cipher set can be expressed as:

$$C = \xi_n (W, P, K). \tag{14}$$

The cipher set can be input in combination, and the input bits are mapped to angle 0 or π. when all W elements are integers, it is equivalent to the XOR operation of the input bits.

3.2 Model design of improved encryption algorithm

In order to improve the security performance of anti neural network model, CCA classification algorithm (common communication adapter) is introduced again. This algorithm has the characteristics of adaptability and non adaptability. In order to enable Bob and Alice to build a more reliable and secure communication model, so to improve the ANC system, we must find a security system that can prevent ciphertext attacks (Gupta et al., 2020). Considering that the deep network has very strong learning ability and can be applied to high security scenarios, but the calculation is too complex, which may affect the real-time communication performance. Bob and Alice use the anti encryption network structure to realise the encryption and decryption process of network information.

The eve structure of this design receives two keys K_0, K_1 and ciphertext C, converts the angle through equation (12), and converts it into continuous bits through equation (13). In the network structure, the second fully connected layer combines the conversion results into the softmax layer logic, and finally outputs the ciphertext. If $k_0 > k_1$, the output is 1, and if $k_0 \leq k_1$, the output is 0.

In the model, in order to adapt to the new countermeasure network model, the original Eve loss function needs to be redefined. If the ciphertext generated by key $p_0^{(i)}$ a is $C^{(i)}$, then $t_1^{(i)} = 1$; If the ciphertext generated by key $p_0^{(i)}$ is $C^{(i)}$, then $t_0^{(i)} = 1$. Here, Eve's loss is redefined:

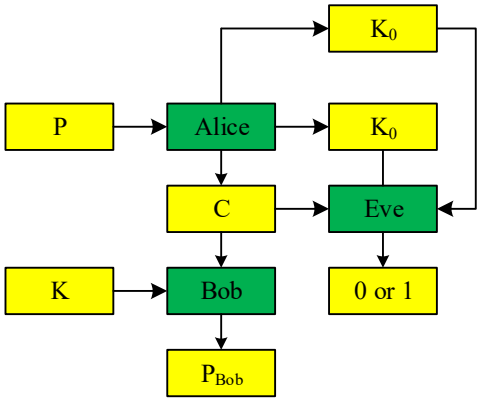
$$L_E = -\frac{1}{M}\sum_{i=0}^{M-1}\sum_{j=0}^{1} t_j^{(i)} \log\left(\pi_j^{(i)}\right). \tag{15}$$

Eve's learning process is realised by minimising L_E. Bob and Alice learn by minimising L. Let Eve's classification error be L and the learning process of Err be:

$$L = L_{AB} - \gamma \min(Err, 0.5). \tag{16}$$

In equation (16), γ is a super parameter. For the improved countermeasure network model, Eve sends the K_0, K_1 key to Alice, and one of the two keys is randomly selected and encrypted to form ciphertext C. Although Bob will decrypt the information through the ciphertext and key, he will not attack and decode C. Eve uses the neural network to determine the encryption mode of the ciphertext, so as to determine whether the output result is 0 or 1, so as to build the improved model in Figure 5.

Figure 5 Improved symmetric encryption countermeasure network model diagram (see online version for colours)



Under the algorithm model, Alice and Bob realise secure communication through the encryption system, which can effectively improve the quality of the encryption scheme.

4 Algorithm simulation analysis

4.1 Simulation environment settings

In order to verify the performance of the algorithm, the algorithm is simulated and analysed. The simulation system selects MATLAB for model construction and specific simulation analysis. When the selected mini-batch parameter is $M = 4{,}096$, $\gamma = 7$ and the regularised key length n of L_2 is 4, 8 and 16, the corresponding super parameter α is set to 0.1, 0.1 and 0.015 respectively. For eve network, the number of neurons in the hidden layer is set to $4n$, which ensures that Eve can analyse the number of linear combinations of functions at the same time. In order to cope with the increase of function formula caused by the increase of the number of keys, it is necessary to select parameters according to experience and set them according to the proportion of parameters and the number of key bits, so as to improve Eve's ability to crack Alice and Bob's passwords. The parameter settings of the algorithm simulation analysis are shown in Table 1.

Figure 6 Simulation flow chart of optimised encryption algorithm (see online version for colours)

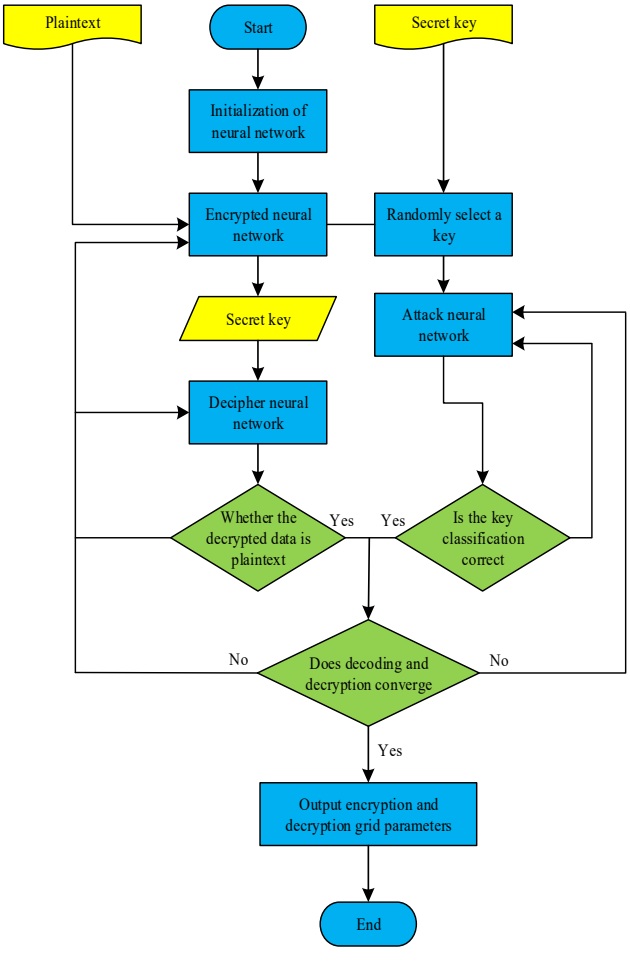


Table 1 Simulation parameter setting

Model setup	*Parameter*
Mini-batch	4,096
Key length	4, 8, 16
Hyperparameter	0.1, 0.1, 0.015
Learning rate	0.0008
Optimiser	Adam

The flow of the simulation algorithm is shown in Figure 6. After learning and training combined with the neural network, Eve can have greater computational advantages. Whenever Bob and Alice train three mini-batches, Eve trains 60.

4.2 Analysis of simulation results

The training and test results of Alice and Bob with key lengths of 4-bit, 8-bit and 16-bit are shown in Table 2.

Table 2 Learning and testing results of different length keys

Key length (bit)	*4*	*8*	*16*
Number of test networks	50	50	50
Number of successful encryption and decryption	50	50	50
Security number of encryption algorithm	0	0	0

After the data training, ANC algorithm is used to test the encrypted network. The test results are shown in Table 3. It can be seen from Table 3 that after the communication network is trained by Alice and Bob, the structure of the anti encryption network is relatively simple, so its security can be realised without the help of neural network.

Table 3 Test results of ANC algorithm for different key lengths

Key length (bit)	*4*	*8*	*16*
Number of test networks	50	50	50
Number of successful encryption and decryption	50	50	50
Security number of encryption algorithm	8	27	32

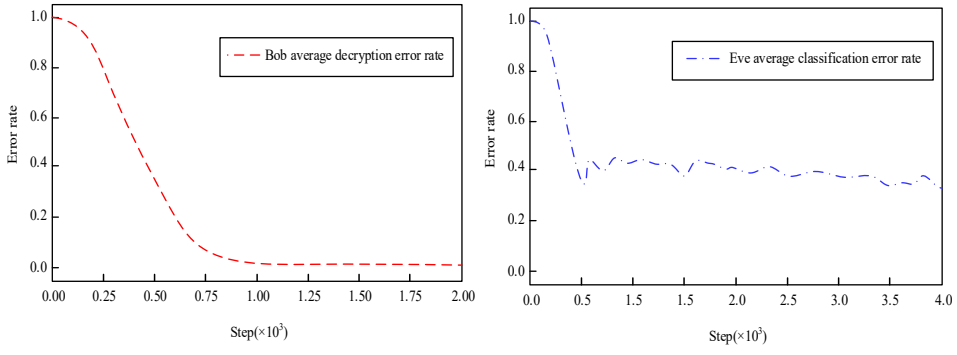
It can be seen from Table 3 that the design of the algorithm model is successful, but the security of the encryption algorithm needs to be further tested. The optimised and improved algorithm is used to test the use of different key sizes. The test results are shown in Table 4.

Table 4 Test results of the improved encryption algorithm for different key sizes

Key length (bit)	*4*	*8*	*16*
Number of test networks	50	50	50
Number of successful encryption and decryption	50	50	50
Security number of encryption algorithm	48	50	50

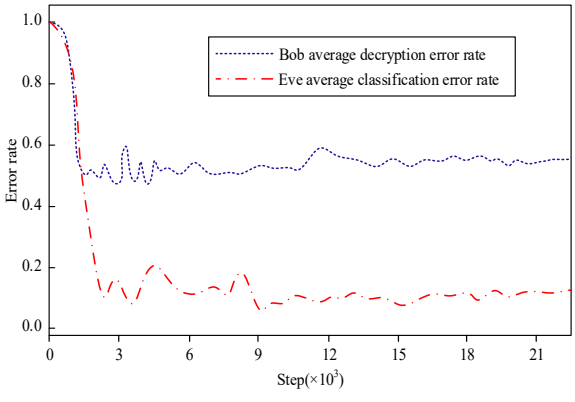
According to the research results in Tables 2–4, the improved algorithm can significantly improve the training results of the model. Finally, only two models failed in training and learning. Under the improved algorithm, most training models can train and learn the secure encryption network, and only a very small number do not learn the secure encryption network, which is caused by the short key length or the randomness of the neural network. Comparing Tables 3 and 4, the number of successful experiments has increased significantly. Through in-depth analysis, it can be seen that Eve is an attacker with weak decoding ability in the original encryption method of ANC, so Bob and Alice can have more corresponding encryption solutions and have a great degree of freedom to choose. The improved encryption algorithm model is used to train the 16-bit password. The training results of Bob and Alice are shown in Figures 7(a) and 7(b) respectively.

Figure 7 Training result graph of Bob and Eve based on improved encryption algorithm (see online version for colours)



(a) (b)

Figure 8 Training results of improved encryption algorithm with 4-bit key length (see online version for colours)

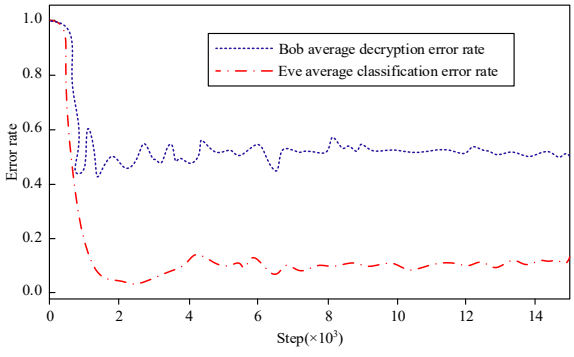


Alice and Bob want to minimise the eve classification accuracy and Bob decryption error rate, while Eve wants to maximise the classification accuracy. As can be seen from Figure 7(a), Bob's decryption error rate is gradually decreasing with the passage of time. As can be seen from Figure 7(b), the eve classification rate increases with the increase of

time. The convergence speed of the improved encryption algorithm has been improved, and the improved algorithm can obtain more information, which makes the communication process more secure and reliable.

Further, the training results of the improved encryption algorithm with 4-bit and 8-bit encryption length are simulated and analysed. The simulation results are shown in Figures 8 and 9. As can be seen from the figure, a key with a smaller length can have a better encryption effect than a key with a 16-bit length.

Figure 9 Training results of improved encryption algorithm with 8-bit key length (see online version for colours)



In order to test the encryption efficiency of the improved encryption algorithm, the trained model is input to 1,024 MB data for encryption speed test. The encryption time required by the improved algorithm (64-bit) is 13.5 s and the average speed is 75.85 MB/s compared with other similar encryption algorithms, this algorithm has faster operation speed and has certain advantages in encryption speed.

5 Conclusions

This research optimises and improves the traditional GANs algorithm, puts forward a new idea to build an encryption algorithm model against neural network, and realises a higher and better security secret generation algorithm through autonomous learning. After introducing CCA algorithm, the model can be more adaptive. Through the simulation analysis of the improved genetic algorithm, it can be seen that the system model has good security after Alice, Bob and Eve are trained. With the increase of the number of experiments, the better the model training effect of the improved algorithm. When the input value of the trained input model is 1,024 MB, 13.5 s can be obtained and the average speed of 75.85 MB/s can be realised. Comprehensive analysis shows that the proposed improved optimisation algorithm has better operation speed and reliable security performance. Although the proposed encryption optimisation algorithm has good performance, good security performance and transportation speed, it needs to be applied to specific network communication examples in subsequent applications to judge its application effect and further improve and optimise it.

Acknowledgements

This study was supported by the Science and Technology Research Program of Chongqing Municipal Education Commission C: (KJQN202104004).

References

Almalkawi, I.T., Halloush, R., Alsarhan, A., Al-Dubai, A. and Al-Karaki, J.N. (2019) 'A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications', *Information Security Technical Report*, December, Vol. 49, pp.102384.1–102384.13.

Amiruddin, A., Ratna, A. and Sari, R.F. (2019) 'Construction and analysis of key generation algorithms based on modified Fibonacci and scrambling factors for privacy preservation', *International Journal of Network Security*, Vol. 21, No. 2, pp.250–258.

Banik, A., Shamsi, Z. and Laiphrakpam, D.S. (2019) 'An encryption scheme for securing multiple medical images', *Journal of Information Security and Applications*, Vol. 49, p.102398.

Chalee, T. and Werasak, K. (2019) 'A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification', *International Journal of Communication Systems*, Vol. 32, No. 12, pp.e3991.1–e3991.21.

Chen, X. (2020) 'A security integration model for private data of intelligent mobile communication based on edge computing', *Computer Communications*, Vol. 162, No. 1, pp.204–211.

Chopra, G., Jha, R.K. and Jain, S. (2019) 'RBA: detection and protection analysis using region-based algorithm in ultra-dense networks', *IEEE Access*, Vol. 7, pp.52997–53011.

Dhanvijay, M.M. and Patil, S.C. (2020) 'Optimized mobility management protocol for the IoT based WBAN with an enhanced security', *Wireless Networks*, Vol. 27, pp.537–555.

Diamant, R., Casari, P. and Tomasin, S. (2019) 'Cooperative authentication in underwater acoustic sensor networks', *IEEE Transactions on Wireless Communications*, Vol. 18, No. 2, pp.954–968.

El-Latif, A., Abd-El-Atty, B., Venegas-Andraca, S.E. et al. (2020) 'Providing end-to-end security using quantum walks in IoT networks', *IEEE Access*, Vol. 8, pp.92687–92696.

Fan, A., Wang, Q. and Debnath, J. (2019) 'A high precision data encryption algorithm in wireless network mobile communication', *Discrete & Continuous Dynamical Systems*, Vol. 12, Nos. 4/5, pp.1327–1340.

Fan, S., Li, K., Zhang, Y. et al. (2020) 'A hybrid chaotic encryption scheme for wireless body area networks', *IEEE Access*, Vol. 8, pp.183411–183429.

Fu, Y., Hong, Y., Quek, T. et al. (2020) 'Scheduling policies for quantum key distribution enabled communication networks', *IEEE Wireless Communication Letters*, Vol. 9, No. 12, pp.2126–2129.

Gupta, A., Singh, D. and Kaur, M. (2020) 'An efficient image encryption using non-dominated sorting genetic algorithm-Ill based 4-D chaotic maps', *Journal of Ambient Intelligence and Humanized Computing*, Vol. 11, No. 3, pp.1309–1324.

Han, Z., Qin, G., Zhao, R., Liu, Y. and Liang, Y. (2018) 'Design and implementation of security protocol for in-vehicle FlexRay buses', *Hsi-An Chiao Tung Ta Hsueh/Journal of Xi'an Jiaotong University*, Vol. 52, No. 12, pp.63–69.

Imran, O.A., Yousif, S.F., Hameed, S. et al. (2020) 'Implementation of El-Gamal algorithm for speech signals encryption and decryption', *Procedia Computer Science*, Vol. 167, No. 1, pp.1028–1037.

Ji, J., Li, W., Wu, B., Wang, K., Xu, M. and Sun, L. (2019) 'Design and investigation on image transmission in multi-user cross-layer security network', *IEEE Access*, Vol. 7, pp.132066–132073.

Kumar, A. and Raghava, N.S. (2021) 'An efficient image encryption scheme using elementary cellular automata with novel permutation box', *Multimedia Tools and Applications*, Vol. 80, No. 1, pp.21727–21750.

Liu, J., Yang, Z., Wu, Z., Yin, Z., Jiang, X. and Fu, Y. (2019) 'Control code multiple encryption algorithm on satellite-to-ground communication', *Mobile Networks & Applications*, Vol. 24, No. 6, pp.1955–1974.

Lu, X., Lei, J., Li, W. et al. (2019) 'Physical layer encryption algorithm based on polar codes and chaotic sequences', *IEEE Access*, Vol. 7, pp.4380–4390.

Mathews, M. (2021) 'Using bit flips as a source of randomness in CubeSat communication encryption', *Acta Astronautica*, Vol. 179, No. 4, pp.546–549.

Muhammad, K., Hamza, R., Ahmad, J., Lloret, J., Wang, H. and Baik, S.W. (2018) 'Secure surveillance framework for IoT systems using probabilistic image encryption', *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 8, pp.3679–3689.

Nkandeu, Y. and Tiedeu, A. (2019) 'An image encryption algorithm based on substitution technique and chaos mixing', *Multimedia Tools and Applications*, Vol. 78, No. 8, pp.10013–10034.

Patel, S., Thanikaiselvan, V., Pelusi, D. et al. (2021) 'Colour image encryption based on customized neural network and DNA encoding', *Neural Computing and Applications*, Vol. 33, No. 14, pp.14533–14550.

Qian, J., Hua, C.X., Guan, X. et al. (2019) 'A trusted-ID referenced key scheme for securing SCADA communication in iron and steel plants', *IEEE Access*, Vol. 7, pp.46947–46958.

Raja, S.P. (2019) 'Multiscale transform based secured joint efficient medical image compression-encryption using symmetric key cryptogrphy and EBCOT encoding technique', *International Journal of Wavelets, Multiresolution and Information Processing*, Vol. 17, No. 5, pp.1907–1917.

Shah, D., Shah, T. and Jamal, S.S. (2020) 'Digital audio signals encryption by Mobi us transformation and Henon map', *Multimedia Systems*, Vol. 26, No. 2, pp.235–245.

Sundararajan, M., Veerappan, M. and Anbazhagan, S. (2019) 'Partial image encryption based on using discrete cosine transform coefficients and lightweight stream algorithm', *Journal of Computational and Theoretical Nanoscience*, Vol. 16, No. 4, pp.1573–1576.

Tamilarasi, K. and Jawahar, A. (2020) 'Medical data security for healthcare applications using hybrid lightweight encryption and swarm optimization algorithm', *Wireless Personal Communications*, Vol. 114, No. 3, pp.1865–1886.

Tauhid, A., Tasnim, M., Noor, S.A., Faruqui, N. and Yousuf, M.A. (2019) 'A secure image steganography using advanced encryption standard and discrete cosine transform', *Journal of Information Security*, Vol. 10, No. 3, pp.117–129.

Uchiteleva, E., Hussein, A.R. and Shami, A. (2020) 'Lightweight dynamic group rekeying for low-power wireless networks in IIoT', *IEEE Internet of Things Journal*, Vol. 7, No. 6, pp.4972–4986.

Varma, R., Melville, C., Pinello, C. et al. (2021) 'Post quantum secure command and control of mobile agents inserting quantum-resistant encryption schemes in the secure robot operating system', *International Journal of Semantic Computing*, Vol. 15, No. 3, pp.359–379.

Vaseghi, B., Hashemi, S.S., Mobayen, S. et al. (2021) 'Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems', *IEEE Access*, Vol. 9, No. 99, pp.2169–3536.

Viswanathan, S. and Kannan, A. (2019) 'Elliptic key cryptography with beta gamma functions for secure routing in wireless sensor networks', *Wireless Networks*, Vol. 25, No. 8, pp.4903–4914.

Wang, H., Xiang, S. and Gong, J. (2019) 'Multi-user image encryption algorithm based on synchronized random bits generator in semiconductor lasers network', *Multimedia Tools and Applications*, Vol. 78, No. 18, pp.1–21.

Wang, X. and Zhao, H. (2019) 'Cracking and improvement of an image encryption algorithm based on bit-level permutation and chaotic system', *IEEE Access*, Vol. 7, No. 99, pp.112836–112847.

Wei, H., Zhang, C., Wu, T., Huang, H. and Qiu, K. (2019) 'Chaotic multilevel separated encryption for security enhancement of OFDM-PON', *IEEE Access*, Vol. 7, pp.124452–124460.

Yang, F., Mou, J., Sun, K. and Chu, R. (2020) 'Lossless image compression-encryption algorithm based on BP neural network and chaotic system', *Multimedia Tools and Applications*, Vol. 79, Nos. 1–2, pp.19963–19992.

Yi, L., Tong, X., Wang, Z. et al. (2019) 'A novel block encryption algorithm based on chaotic S-box for wireless sensor network', *IEEE Access*, Vol. 7, pp.53079–53090.

Zhao, A., Jiang, N., Liu, S. et al. (2021) 'Physical layer encryption for WDM optical communication systems using private chaotic phase scrambling', *Journal of Lightwave Technology*, Vol. 39, No. 8, pp.2288–2295.