Application of GAN-Based Data Encryption Technology in Computer Communication System

Min Li
School of Computer and Artificial Intelligence, Henan Finance University, Zhengzhou, 451464, China
E-mail: limin980501@163.com

Keywords: generating adversarial network, computer communication, data encryption technology, CCA-ANC

Received: June 13, 2024

With the rapid development of information technology, how to ensure the secure transmission and storage of data has become an important issue in today's society. The experiment innovatively proposes an encryption method to improve the security of computer communication systems under various attack modes. This method is based on Chosen Cipher-text Attack (CCA) and improved adversarial neural network. In the process, the adversarial neural network is first used to encrypt the data. A new symmetric encryption system structure, namely Adversarial Neural Cryptography (ANC), is introduced to merge with Generative Adversarial Network (GAN). In addition, a Chosen Cipher-text Attack-Adversarial Neural Cryptography (CCA-ANC)-based encryption method is proposed to build a computer communication data encryption system. GAN is adjusted and optimized based on the CCA test results to jointly realize the encryption of data transmission. The experiment uses two public data sets: CAIDA and UNIBS. 1520 data in the CAIDA data set are finally selected as the validation set and named as data set A by removing redundant data. 380 data in the UNIBS data set are selected as the test set and named as data set B. The experiment selects the iteration, AUC value, classification accuracy, and other performance indicators. The results showed that the research model reached a stable state with a fitness value of 0.612 after 38 iterations. Compared with existing technologies such as Blockchain technology, X-IDEA, and HS-IQRG algorithms, the AUC of the proposed method was 0.978. On dataset A, the research method had a maximum classification accuracy of 98.24% when the system iterated 75 times. The encryption time of the research method on dataset A was only 0.0424s when the system iterated 44 times. The above results all show that the research method can encrypt data. Meanwhile, this method learns a safe password generation method in the automated system, which makes certain contributions to computer communications. This experiment provides a new theoretical perspective on achieving more secure computer communication systems by combining CCA and ANC technologies. From a technical point of view, the effectiveness of the proposed method is verified through performance testing, which provides an experimental basis for the application of the technology. Meanwhile, the application potential of this technology in different network environments is discussed, providing a valuable reference for future communication security practices.

Povzetek: Opisana je izvirna uporaba tehnologije GAN pri šifriranju podatkov v računalniških komunikacijskih sistemih. Prispevek združuje napad izbranega šifrirnega besedila (CCA) in napredno nevronsko kriptografijo (ANC) za povečanje varnosti prenosa podatkov.

1 Introduction

In 2017, vulnerabilities in the Struts open-source software were exploited by hackers to launch an attack on Equifax, the United States credit reporting giant. As a result, the company's core data were leaked, involving the theft of core information of nearly 145 million users. In 2022, network security and vulnerability incidents occurred frequently in the United States medical field, which had serious impact on hospital operations and patient information protection. As time goes by, the confidentiality, integrity and reliability of data play an important role [1]. Traditional Data Encryption Technology (DET) can usually only encrypt data, but cannot protect the integrity and authenticity of the data. Meanwhile, traditional encryption methods usually consume a lot of computing resources and time when running, seriously affecting data transmission efficiency. With the continuous development of computer technology, traditional encryption methods may face more attacks and cracking risks. Meanwhile, they also face multiple challenges such as the rapid growth of computing power, complex network threats, and new attack methods. Therefore, developing a new, efficient, and reliable encryption technology has become an urgent task [2]. In recent years, deep learning technology, especially the Generative Adversarial Network (GAN), has made breakthroughs in computer vision and natural language processing. The core idea of GAN is to generate data through adversarial training between two networks (generators and discriminators). GAN was originally designed to generate virtual data such as images, sounds, etc. However, researchers quickly realize that GAN can also be applied to data encryption [3]. GAN makes it impossible for unauthorized users to understand or access data, especially when considering the nature of encryption. The potential of GAN has received widespread attention. As an advanced deep learning technology, GAN can generate new data instances by learning large amounts of data patterns. In data encryption, this capability can be used to create complex and unpredictable encryption patterns, thereby improving the security of encrypted data. In addition, GAN learns the deep features of the data through the adversarial process. GAN can identify and strengthen the most important features in data encryption, thereby improving the effectiveness of the encryption algorithm. This makes it difficult for attackers to decrypt encrypted data without appropriate decryption methods or keys, thereby increasing the security of the data [4]. Compared with traditional encryption technology, GAN-based encryption technology can adapt to new threats and attack modes through continuous adversarial training, which means that the encryption system can self-adjust according to changes in the network environment. Compared with traditional static encryption methods, this method provides greater flexibility and adaptability. At the same time, GAN can generate highly complex and unpredictable encryption patterns, which are extremely challenging for traditional decryption algorithms. This complexity increases the difficulty of cracking and increases the security of data. In addition, GAN-based data encryption has other advantages. Firstly, it can quickly encrypt large amounts of data to meet the needs of modern big data environments. Secondly, GAN is an adaptive model, which can be adjusted according to different data sources or attack modes, making encryption technology more adaptive and robust. However, applying GAN to DET also brings new challenges. First of all, the GAN training process itself has high computational complexity and requires a lot of computing resources and time [5]. To solve this problem, the experiment plans to simplify the network structure, use more efficient training methods, or use advanced parallel computing technology to reduce GAN's dependence on computing resources. Secondly, the encrypted data generated by GAN need to ensure sufficient randomness and unpredictability to resist various cryptographic attacks [6]. The experiment focuses on improving the GAN model to ensure that the encrypted data generated by GAN can resist cryptographic attacks to improve the security of the generated data. This includes the use of more complex randomness algorithms and unpredictability detection mechanisms to ensure the randomness and security of data. Furthermore, the application of GAN in computer communication systems also needs to consider the real-time nature and transmission efficiency of data [7]. The experiment will explore lightweight GAN models and data compression technology to reduce the impact of the encryption process on system performance and ensure high efficiency of data transmission. In addition, the reliability and stability of the GAN model are also important considerations. The experimental plan continues to test and optimize the GAN model. More stable training datasets and improved model evaluation methods can be used to ensure stability and reliability under various conditions.

Based on this background, this paper analyzes the application prospects and research status of GAN in data security, designs an innovative Chosen Cipher-text Attack-Adversarial Neural Cryptography (CCA-ANC) DET, and applies it to data encryption systems. The experiment mainly carries out the following two aspects by in-depth studying the potential of GAN in data encryption. First, a comprehensive analysis of the existing GAN architecture and encryption technology is conducted to understand its advantages and disadvantages in data protection. limitation. Secondly, an encryption method based on CCA-GAN is designed. This method generates encrypted data that are difficult to crack through adversarial learning. As a result, the security of data encryption can be enhanced to obtain cross-cutting results in computer science, artificial intelligence, and data security. The great potential of combining these fields is demonstrated.

With the widespread application of computer communication systems in modern society, data security and privacy protection have become important issues in the field. To better cope with the above challenges, optimizing and training GAN or adopting more efficient hardware support can reduce its resource consumption. Continuous research and improvement of GAN models are required to improve the security of generated data. Combining with traditional encryption technology, the overall security protection can be enhanced. In addition, light-weight GAN models and compression technologies can be explored to reduce the impact of the encryption process on system performance.

The innovation of this article can be divided into two points. First, the research uses the generation ability of GAN to creatively implement a data encryption method that does not require traditional keys. This method can reduce the system's dependence on key management and simplify the encryption process while ensuring data security. Second, the experiment successfully improves the complexity and randomness of encrypted data. Meanwhile, the experiment enhances the security of the encryption algorithm when facing various attacks by adjusting the structure and training strategy of GAN. This is unprecedented in the data encryption and provides a new perspective for the application of GAN.

The main contributions of this research are: (1) The encryption framework constructed in the experiment solves data security and low encryption efficiency in current research. (2) Compared with traditional encryption technology, the CCA-ANC-based data encryption method proposed in the experiment can significantly improve the processing speed and efficiency of encrypted data while ensuring data security. For ease of reading, a table of abbreviations for experimental preparations is shown in Table 1.

Table 1: Introduction to abbreviations

Full name	Abbreviation	Full name	Abbreviation
Area Under Curve	AUC	Encryption Detection Network	EDN
Receiver Operating Characteristic	ROC	Adversarial Neural Cryptography	ANC
X-IDEA algorithm	X-IDEA	Data Encryption Technology	DET
Hyper-chaotic Systems and Improved Quantum Rotating Gate	HS-IQRG	Generative Adversarial Network	GAN
Chosen Ciphertext Attack	CCA	Chosen Cipher-text Attack-Adversarial Neural Cryptography	CCA-ANC

This article mainly includes four parts. Firstly, it is mainly a summary of domestic and foreign GAN applications and computer communication systems. Secondly, the improved adversarial neural network encryption algorithm is introduced, and simulation experiments are conducted on the structure and mathematical basis of the algorithm model, and the security of the model is analyzed in detail. In view of the shortcomings of the ANC algorithm, an improved encryption algorithm (CCA-ANC) based on Chosen Cipher-text Attack (CCA) is proposed, and a secure encryption algorithm is obtained through detailed analysis and comparison of the security capabilities of the algorithm. The third part analyzes the performance and application effectiveness of the computer communication system constructed by the research institute. Finally, the whole research is summarized.

2 Related works

The secure transmission and encryption of networks and insecure channels' data have become many urgent problems to fit industry demand and technology progress. Numerous scholars have conducted relevant research on DET. Hong and Sun proposed a new attribute-based sensor cloud data access system to improve the flexibility of data sharing in sensors. Throughout the experiment, attribute-based cryptography and hash cryptography techniques were used to prove the excellent performance of the original data encryption to achieve access control of the data. Performance evaluation showed that the proposed solution had high security and efficiency [8]. Kumar and Bhatt believed that elliptic curve encryption was chosen for identity verification, data encryption, and data decryption due to its key size. However, this method had certain shortcomings and could not effectively protect data security. In response to this issue, the research team proposed a method that combined natural inspired optimization with elliptic curve encryption. This method combined DNA encoding and elliptic curve encryption. These experiments confirmed that the proposed method was more secure and occupies less space than elliptic curve encryption [9]. Hong et al. proposed an online or offline signature method based on key policy attributes to improve the efficiency of data authentication security of mobile sensing network. The proposed method combined the advantages of attribute-based cryptography with the chameleon hash function and allowed the data owner to set access rules. The final results showed that the proposed scheme was highly safe and efficient [10]. Yan et al. found that there were a large number of nodes and some useless nodes on the hospital internet. The presence of these nodes made it difficult to transmit data packets. In response to this issue, the research team proposed a routing and path oriented data encryption system based on network statistics. This system could encrypt data in cloud servers. These experiments confirmed that the proposed system could encrypt data based on its type and conditions, thereby ensuring data security [11]. Chen found that with the development of computer network technology, the informatization of accounting was an inevitable trend. However, the complexity of industry accounting reports, the randomness and diversity of users needed to obtain information using reports. The security of data limited the development of this industry. In response to this problem, the research team proposed a data encryption method that could encrypt through 64-bit packet data. Experimental results showed that the proposed method had better encryption effect and encryption efficiency than traditional encryption methods and realized one encryption process at a time to a certain extent, which could effectively resist exhaustive search attacks [12].

GAN, as a neural network model, is widely used in the safe operation of systems. Scholars have also conducted numerous discussions on it. Meanwhile, Andrius et al. found that GAN, as a large-scale simulation algorithm, had certain limitations, such as unstable training process, inherent randomness of output results, and difficulty in training algorithms on multiple datasets. In response to these issues, the research group adopted some commonly used methods to generate weak lens convergence maps and red shifts by training adversarial networks. These experiments confirmed that there was good consistency between simulated images generated by adversarial networks and real images under the proposed improved method in most data [13]. Luo et al. found that the movement of the arm was completed through a series of complex operations, which appeared more complex in robots. Therefore, the research team proposed a model to establish basic unit motion through GAN. These experiments confirmed that the proposed model could provide certain assistance for the motion of robot arms [14]. Wang et al. believed that the operating data of power plants were irregular, which could lead to data imbalance and affect the model for monitoring power plants. In response to this issue, this study proposed a conditional variational automatic encoder and a method for generating adversarial networks. This method could predict the operational status of power plants through imbalanced datasets. These experiments confirmed that using the dataset generated by the proposed method to train the model improved the accuracy of predicting polluted air emissions [15]. Jiang et al. found that renewable energy sources such as wind and solar energy accounted for an increasing proportion of energy in daily life. However, natural resources had randomness. The operation and planning of power systems faced enormous uncertainty. In response to this issue, the research team proposed an unsupervised distribution learning method for renewable scenario prediction based on GAN. This method could predict wind and solar energy for energy planning. These experiments confirmed that this method could make the prediction generation model's iteration time reduced by at least half, which had a high model accuracy [16]. Ghosheh et al. proposed an improved GAN and applied it to the electronic medical health data recording. During the experiment, the system's data fidelity and privacy protection performance were verified. The results showed that the model had superior performance in healthcare and electronic health data protection [17]. Scholars such as Shim proposed a crack detection method based on GAN and self-training to reduce the difficulty of regularly checking the aging degree of infrastructure. The crack images synthesized from the predicted images were merged with the data through self-training. Then results with higher credibility were produced. Data showed that the F1 value of this method was 76.31%, and its performance was superior [18].

In summary, DET and GAN are widely used in many fields to enhance the security performance of computer systems. However, there is little research on the integration and application of GAN and DET in computer communication systems. In view of this, the study analyzes GAN and introduces attackers who choose cipher-text attack to form an improved adversarial encryption neural network algorithm, hoping to provide new technical support for communication data security. A summary of related works is shown in Table 2.

Table 2: Summary of related works

Author(s)	Year	Method/Algorithm	Performance metrics	Observations
Hong and Sun [8]	2021	A new attribute-based sensor cloud data access system is proposed.	Security level and efficiency	Higher security level and efficiency
Kumar and Bhatt [9]	2020	A method combining nature-inspired optimization with elliptic curve cryptography is proposed.	Security and space occupied	Higher security and smaller footprint
Hong et al [10]	2021	Online or offline signature method based on key policy attributes	Security performance	Higher security and efficiency
Yan et al [11]	2021	A routing and path-oriented data encryption system based on network statistics is proposed.	Security performance	Encrypt data according to data type and conditions to ensure data security
Chen [12]	2021	A method for data encryption is proposed.	Encryption effect and efficiency	Better encryption effect and encryption efficiency, effectively resisting

				exhaustive search attacks
Andrius et al [13]	2021	Generate weak lens convergence map and redshift by training a GAN	Image consistency	Good consistency between the generated simulated image and the real image
Luo et al [14]	2019	A model for building basic unit motion by GAN is proposed.	Robot movement efficiency	Can provide certain assistance for the movement of the robot arm
Wang et al [15]	2021	A conditional variational autoencoder and GAN is proposed.	Prediction accuracy	Improve the accuracy of polluted air emission prediction
Jiang et al [16]	2021	An unsupervised distribution learning method for reproducible scenario prediction based on GAN is proposed.	Prediction time and accuracy	Reduce the prediction time and show higher model accuracy
Ghosheh et al [17]	2024	A method for electronic medical health data recording based on improved GAN is proposed.	Data fidelity and privacy protection performance	Excellent performance in healthcare and electronic health data protection
Shim [18]	2024	A crack detection method based on GAN and self-training is proposed.	F1 value	F1 value up to 76.31%

3 Research on gan and det in computer communication

Computer communication penetrates into every corner of modern life. From people's daily life, business communication to national security, its importance is self-evident. However, with it comes increasingly serious data security issues. Traditional DET gradually reveals its weaknesses in the face of new network attacks and complex threat environments. Therefore, how to explore new and more powerful encryption methods has become a research hotspot. In this chapter, the research proposes an improved ANC adversarial encryption method, which changes the attacker in ANC from a pure ciphertext attack to a selected ciphertext attack. The experiment calls this adversarial encryption algorithm CCA-ANC. CCA is a method with better attack effect in cryptography. The existing encryption algorithm of neural network can be improved by introducing attackers with CCA. This encryption method prevents selected ciphertext attacks, which are more common in deciphering. CCA can effectively protect data security.

3.1 Data encryption technology based on gan

GAN has the ability to learn high-dimensional and complex real data distributions and has received widespread attention in machine learning. Particularly, GAN does not rely on any assumptions and produces real examples simply. Based on this background, this experiment will explore how GAN combines with traditional and the latest DET. This experiment provides a new perspective and exploring new possibilities for data encryption and transmission security in computer communication [19]. GAN contains two components, namely generation component G and discrimination component D. G and D are constantly in competition to achieve their respective goals, resulting in a characteristic of confrontation. This learning is achieved through parameterized networks G and D, as defined in equation (1).

$$\min_{G}\max_{D} V(G,D)=\min_{G}\max_{D} E_{x-p_{data}(x)}\left[\log D\left(x\right)\right]+E_{z-p_{z}(z)}\left[\log\left(1-D\left(G\left(z\right)\right)\right)\right] \tag{1}$$

In equation (1), $p_{data}(x), p_z(z)$ refer to the true data probability distributing defined in the data space $\mathcal{X}$ and the Z probability distributing defined in the hidden space Z, respectively. V(G,D) represents a binary crossing entropy function and is often applied in binary classification issues. Figure 1 shows the relevant structure of GAN.

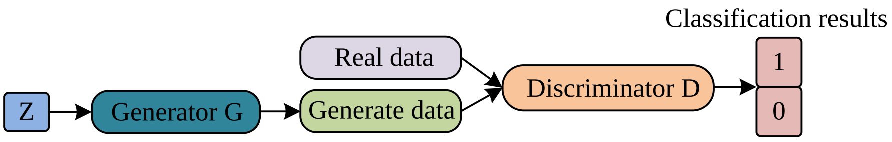


Figure 1: Relevant structure of GAN

In Figure 1, it is assumed that both G, D models contain sufficient capacity space. When $p_{data}(x) = p_g(x)$, G, D will reach a stable state, and the classification accuracy of D is 50%. $p_g(x)$ represents the distributing of relevant data from generator. Formally, the optimal discriminator $D*$ can be obtained for a certain generator G. The commonly used structure of GAN is a hierarchical structure. By using a hierarchical structure, encrypted images can be generated hierarchically and in stages, gradually improving resolution. Taking StackGAN as an example, Figure 2 shows its corresponding hierarchical structure.

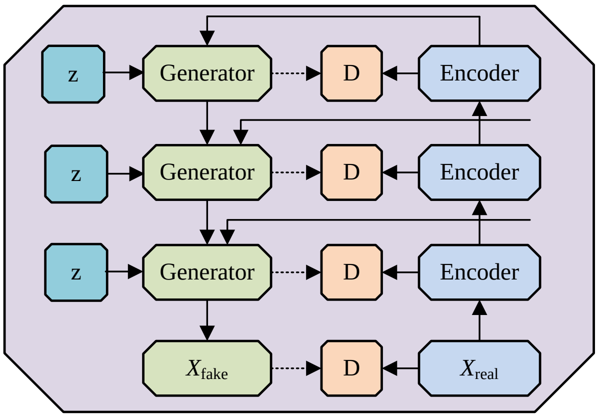


Figure 2: Hierarchy-StackGAN

GAN has a faster generation speed compared to traditional encryption models. GAN replaces the sampling process with a generator and does not introduce a lower bound to approximate likelihood. GAN also has certain shortcomings. First, the quality of data generated by GAN fluctuates, and the diversity may be limited, which may affect the effectiveness of using GAN-generated data for encryption algorithm testing. Secondly, the training of GAN may be unstable, making it difficult for the model to converge, which may seriously affect the performance evaluation of the model. Therefore, a new symmetric encryption system structure, namely Adversarial Neural Cryptography (ANC), is introduced, which integrates and interacts with GAN. For CCA attacks, ANC can analyze the security of encryption systems. ANC mainly tries to crack the encryption algorithm by exploring the statistical correlation between plaintext and ciphertext. In the ANC system, Alice and Bob communicate securely through a shared key K. Eve, as a passive attacker, tries to obtain information about the plaintext P by analyzing the ciphertext C. In the design of the ANC system designed in the experiment, special consideration is given to the need to resist CCA attacks [20]. Specifically, the ANC system uses a multi-layer encryption strategy and a complex key exchange mechanism to reduce the identifiable correlation between plaintext and ciphertext. In addition, the experiment uses the generator of GAN to increase the randomness and unpredictability of the ciphertext, further reducing the feasibility of CCA attacks. The experiment results section specifically analyzes the performance of CCA when it is attacked to verify the resistance of the ANC system to CCA attacks. Figure 3 shows the symmetric encryption and decryption model.

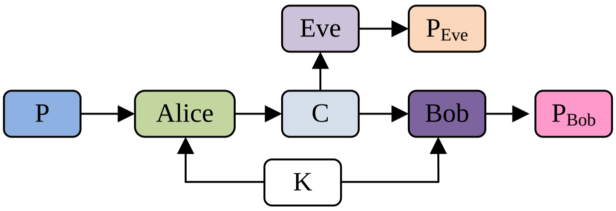


Figure 3: Symmetric encryption and decryption model

In ANC, these three structures are all networks that handle floating-point numbers, not sequences. In the block cipher designed in the experiment, the data types of K, P, PBob, PEve, and C refer to floating-point numbers. Because their parameters are represented as $\theta_A, \theta_B, \theta_E$, $E_A(\theta_A, P, K)$ is defined in this experiment as the encrypted output of Alice's input plaintext P and key K. $D_B(\theta_B, C, K)$ serves as the decryption output when Bob inputs C and K. $D_E(\theta_E, C)$ represents the deciphered output when Eve inputs C [21]. To evaluate the real plaintext and the estimating value's mutual distance, L_1 is selected for the calculation in equation (2).

$$d(P, P') = {}^{1}\!/_{N} \sum |P_i - P_i'| \qquad (2)$$

In equation (2), N represents the plaintext length. To achieve Eve's goal of reconstructing plaintext P_e, the loss function of Eve is defined in equation (3).

$$L_E(\theta_A, \theta_E, P, K) = d(P, D_E(\theta_E, E_A(\theta_A, P, K))) \; (3)$$

In equation (3), $L_E(\theta_A, \theta_E, P, K)$ represents the calculated amount of decoding error for Eve with P and K. When the plaintext and key distribution are unknown, an expecting value can be taken to define Eve's loss function in equation (4).

$$\begin{cases} L_E(\theta_A, \theta_E) = E_{P,K}\left[L_E(\theta_A, \theta_E, P, K)\right] \\ O_E(A) = \arg\min_{\theta E}(L_E(\theta_A, \theta_E))) \end{cases} \qquad (4)$$

In equation (4), $L_E(\theta_A, \theta_E)$ represents the expected value of Eve. $O_E(A)$ represents the optimal Eve obtained through minimum loss. Similarly, Bob's loss function can be obtained and extended to the corresponding plaintext and key in equation (5).

$$\begin{cases} L_B(\theta_A, \theta_B, P, K) = d(P, D_B(\theta_B, E_A(\theta_A, P, K), K)) \\ L_B(\theta_A, \theta_B) = E_{P,K}\left[L_B(\theta_A, \theta_B, P, K)\right] \end{cases} \qquad (5)$$

In equation (5), L_B represents Bob loss function. When Alice and Bob want to exchange accurate data, these two functions require Eve to keep their communication data confidential. Therefore, the joint loss function of Alice and Bob can be defined by combining the optimal values of L_B, L_E in equation (6).

$$L_{AB}(\theta_A, \theta_B) = L_B(\theta_A, \theta_B) - L_E(\theta_A, O_E(\theta_A)) \quad (6)$$

Based on the above formula, the optimal Alice and Bob can be obtained by making $L_{AB}(\theta_A, \theta_B)$ minimized in equation (7).

$$O_A, O_B = \arg\min_{(\theta A, \theta B)}(L_{AB}(\theta_A, \theta_B)) \quad (7)$$

3.2 Construction of an encrypted computer communication system based on improved cca

This experiment conducts a detailed analysis of the encryption structure, algorithm functions, and security of ANC in the previous section. However, some scholars have found that when applying ANC technology to computer communication systems, combining it with multi-layer neural networks cannot generate a secure encryption system. Meanwhile, it is highly likely to be cracked by other neural networks through training. Therefore, an improved ANC adversarial encryption algorithm is proposed in this experiment. By giving attackers greater cracking power, the sender and legitimate receiver are forced to take a superior password system, thereby obtaining a invulnerable encrypting method. This method is called CCA-ANC. This technique allows an attacker to select a sequence of cipher-text and analyze the corresponding plaintext or key information. The strength and security of the ANC encryption algorithm can be effectively tested and evaluated by analyzing CCA. This attack is particularly useful for evaluating the ANC algorithm's ability to withstand sophisticated password analysis and cracking attempts. By simulating CCA, potential weaknesses in the ANC encryption mechanism can be revealed, thereby providing guidance for algorithm improvement. Furthermore, the application of this attack method helps to strengthen the resistance of the ANC and improve its security and reliability in practical applications. In summary, CCA is an important tool for optimizing the ANC encryption algorithm. CCA enhances the overall password security by revealing and repairing weaknesses in the encryption algorithm. This experiment first adds a numerical conversing operator to the adverse-encrypting network in the previous section. Then the adversarial neural network can learn some cipher methods, which has relatively simplicity [22]. Cryptography always involves XOR. To better improve its application in computer communication, the study provides a continuous extension of XOR. The experiment maps bit 0 to angle 0 and position 1 to angle π. XOR can be generalized using the unit circle. The resulting XOR is equivalent to two angles' sum. The operations in this process are continuous. Therefore, angles different from 0 or π can be utilized and extended to a continuous space. Then the mapping from position b to angle can be obtained in equation (8).

$$f(b) = \arccos(1-2b) \tag{8}$$

In equation (8), $f(b)$ represents the mapping from position b to angle. In equation (9), the mapping from diagonal a to continuous bits is inversely derived.

$$f^{-1}(a) = \frac{1-\cos(a)}{2} \tag{9}$$

After obtaining the numerical conversion operator, the experiment can introduce a smaller neural network into the encryption detecting network to verify the encrypting learning security, which is called Encryption Detection Network (EDN). Figure 4 shows its specific structure.

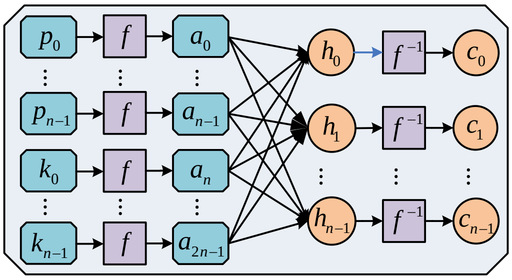


Figure 4: The specific architecture of the encryption detection network

In Figure 4, an EDN is used to receive plaintext and keys for inputting, which are converted through $f(b)$ to transform the bit into angle as input to neural network firstly. Next, the weight matrix multiplication reaching an adverse-encrypting network is calculated to get the initial cipher-text. The final one can be get through $f^{-1}(a)$ transformation inversely. Overall, it should be noted that all data processed by EDN are floating-point numbers. Therefore, EDN's cipher-text owns the numbers in [0, 1]. From a mathematical perspective, cipher set's fully connecting layer should perform the operations in equation (10).

$$\begin{pmatrix} h_0 \\ h_1 \\ \vdots \\ h_{n-1} \end{pmatrix}^T = \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \\ a_n \\ \vdots \\ a_{2n-1} \end{pmatrix}^T W \tag{10}$$

In equation (10), W represents all hiding and convolutional layers' unified weight matrix in this adverse-encrypting network. $(a_0, \cdots, a_{2n-1})$ refers to plaintext and key's angle. $h_0, \cdots, h_{n-1}$ represent this adverse-encrypting network's output variables. In other parts of this experiment, the cipher set will be represented as a function using mathematical concepts in equation (11).

$$C = \xi_n(W, P, K) \tag{11}$$

P, K, C refer to the inputting plaintext, key, and output key's n bit vectors in equation (10), respectively. CCN is an attack model that can be used for password analysis. Password analysts usually choose cipher-text and obtain the specific attack behavior of decryption information without knowing the key. The classification of CCN can be adaptive or non-adaptive. An improved ANC algorithm is introduced to establish a more reliable secure communication model between Alice and Bob. That is, Eve can choose to use cipher-text attacks to attack and decipher the key. After successful decryption, it can obtain the cipher-text that has been deciphered. Therefore, data encryption in the computer communication system needs to prevent Eve's attacks. Therefore, Alice and Bob need to find a security system that can prevent the selection of cipher-text attack methods to improve system security. Throughout the entire experimental process, Alice and Bob jointly perform encryption and decryption operations through an adversarial encryption network structure [23]. The network structure corresponding to Eve needs to be adjusted to a large extent to obtain an improved Eve classifier. This classifier receives K_0 and K_1, C as system inputs. If the system believes that C comes from K_0, attacker Eve will classify C as 0. If the system believes that the input C comes from K_1, C is classified as 1. Figure 5 shows the setting of Eve.

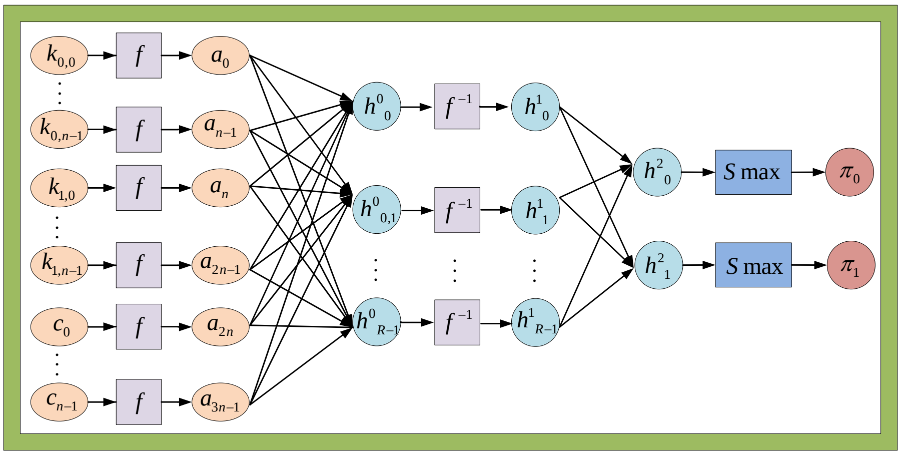


Figure 5: Setting of eve

The change in the model requires a redefinition of Eve's loss function to adapt to the new adversarial network model. Equation (12) is Eve's new loss definition.

$$LE = -{}^{1}\!/_{M}\sum_{i=0}^{M-1}\sum_{j=0}^{1} t_j^{(i)}\log(\pi_j^{(i)}) \qquad (12)$$

In equation (12), if $C^{(i)}$ is a cipher-text generated through the key $P_o^{(i)}$, $t_l^{(i)}=1$. If $C^{(i)}$ is a cipher-text generated through key $P_o^{(i)}$, $t_o^{(i)}=0$. In Eve's learning by minimizing the parameter L_E, Alice and Bob can learn by minimizing the given parameter L in equation (13).

$$L = L_{AB} - \gamma\min(Err, 0.5) \qquad (13)$$

In equation (13), Err represents the classification error of Eve. γ represents a hyperparameter. In the new adversarial network model obtained, Eve will choose to send the keys K_0, K_1 to Alice. Alice randomly selects a key, encrypts it through a neural network to obtain the corresponding C, and then transmits C to Eve and Bob. The obtained model is CCA-ANC in Figure 6.

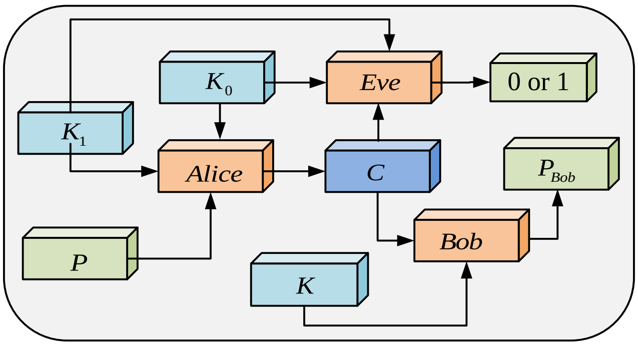


Figure 6: The specific architecture of CCA-ANC

This paper defines the hiding layer neurons number R as $4n$ for Eve to train the experimental network. Neurons number defines that Eve can analyze functions' linear combinations simultaneously. Keys increasing requires more function calculations for Eve's prevention. Therefore, this experiment selects parameters on the foundation of experience and further obtains computer communication system process based on CCA-ANC in Figure 7.

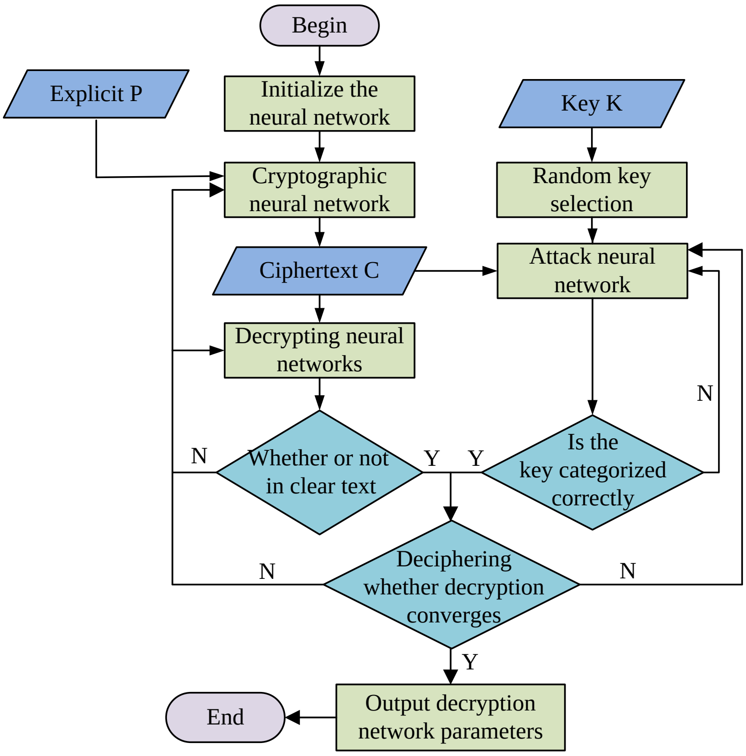

Begin
Explicit P
Initialize the neural network
Key K
Cryptographic neural network
Random key selection
Ciphertext C
Attack neural network
Decrypting neural networks
N
Whether or not in clear text
Y
Y
Is the key categorized correctly
N
Deciphering whether decryption converges
N
N
Y
End
Output decryption network parameters

Figure 7: Operation of computer communication data encryption system based on CCA-ANC

In Figure 7, the training alternates between Alice, Bob, and Eve. To give Eve a great computational advantage, Alice and Bob train 60 mini-batches for every 3 mini-batches. Overall, the experiment designs an encryption model based on GAN. The model mainly contains two parts, namely the generator (used for data encryption) and the discriminator (used to verify the effectiveness of encryption). The original communication data are input into GAN. The generator in the model receives the data and encrypts them. The discriminator evaluates how to distinguish the encrypted data from the original data. CCA attacks are performed on encrypted data to test data security. Based on the CCA test results, the GAN model is adjusted and optimized to achieve encryption of data transmission and facilitate use in computer communication systems.

4 Performance testing and application effectiveness of computercommunitation data encryption system

4.1 Performance test comparison

The experiment verified the effectiveness of GAN and DET in computer communication system to comprehensively understand the specific performance of the constructed model. Firstly, the simulation environment and related parameters for the experiment were set in Table 3.

Table 3: The experimental basic environmental parameters

Parameter variables	Parameter selection
The overall implementation platform of the system	Simulink
Operating system	Windows10
Operating environment	MATLAB
System PC side memory	36 G
CPU dominant frequency	2.62 Hz
GPU	RTX-2070
Central Processing Unit	i7-8700
Data storage	MySQL
Data regression analysis platform	SPSS 26.0

This study first selected computer communication encryption system based on Blockchain technology, mobile communication image and text encrypting technology based on the X-IDEA algorithm (X-IDEA), and image encryption algorithm based on Hyper-chaotic Systems and Improved Quantum Rotating Gates (HS-IQRG) to compare their performance with the research method [24]. To ensure the rationality and fairness of the system performance testing experiment, all methods are conducted under unified experimental conditions. The experiment selected two public datasets, CAIDA and UNIBS, for testing. The source of the CAIDA dataset is http://www.caida.org/data. The source of the UNIBS dataset is http://www.ing.unibs.it/ntw/tools/traces/index.php. 1520 pieces of data were randomly selected from the CAIDA dataset as the verification set, named dataset A. 380 pieces of data were selected from the UNIBS dataset as the test set, named dataset B. Meanwhile, to ensure the reproducibility and fairness of the experiment, the selection and partitioning of the dataset followed standard data science practice principles. The fitness value is a key indicator for evaluating the performance of GAN during the training. The fitness value usually reflects the quality of the data generated by the model and the stability of the model. Firstly, the convergence rates of different algorithms were compared in Figure 8.

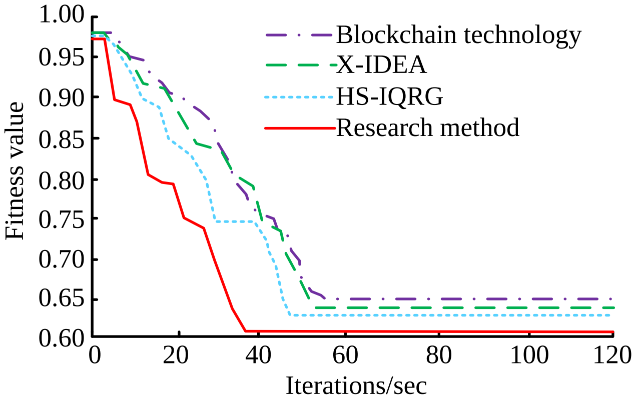


Figure 8: Convergence iteration of different models

In Figure 8, as the iteration increases, the optimal fitness values of Blockchain technology, X-IDEA, HS-IQRG, and the research method all begin to decrease. The fitness value is used to measure the performance of the generator and discriminator in GAN. A higher fitness value indicates that the generator can produce high-quality and indistinguishable encrypted data. Moreover, the discriminator can effectively distinguish between real data and generated data. The research model reaches a stable state with a corresponding fitness value of 0.612 after 38 iterations. This result indicates the model's fast convergence and efficient learning ability. When the iteration is 38 times, the research model first iterates to a stable state, corresponding to a fitness value of 0.612. When the iteration is 49 times, HS-IQRG starts to stabilize, with the optimal fitness value of 0.644. Compared to the first two, the iterative states of X-IDEA and Blockchain technology are more unstable, requiring the system to iterate 53 and 58 times, respectively, to enter a smooth and stable state. When reaching a stable state, the optimal fitness values for X-IDEA and Blockchain technology are 0.652 and 0.661, respectively. From the comparison, the research method reaches the stable fitness value first and can reach the convergence speed faster in the same time, which means more efficient learning ability and better algorithm design. This comparison is critical for selecting or designing the best model for a specific task, especially in application scenarios where fast and accurate responses are required. Figure 9 shows the Area Under Curve (AUC) obtained by training four algorithms on the test set.

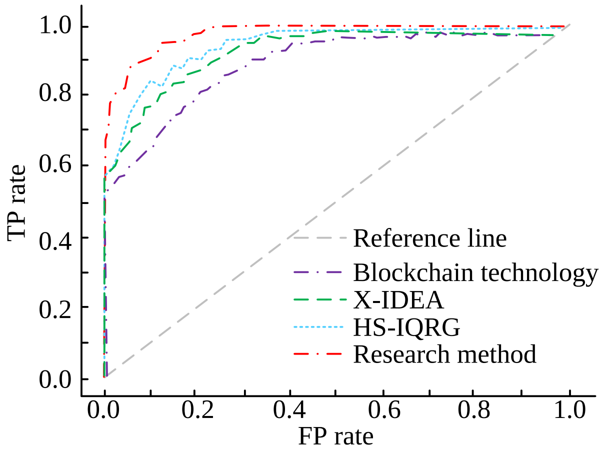
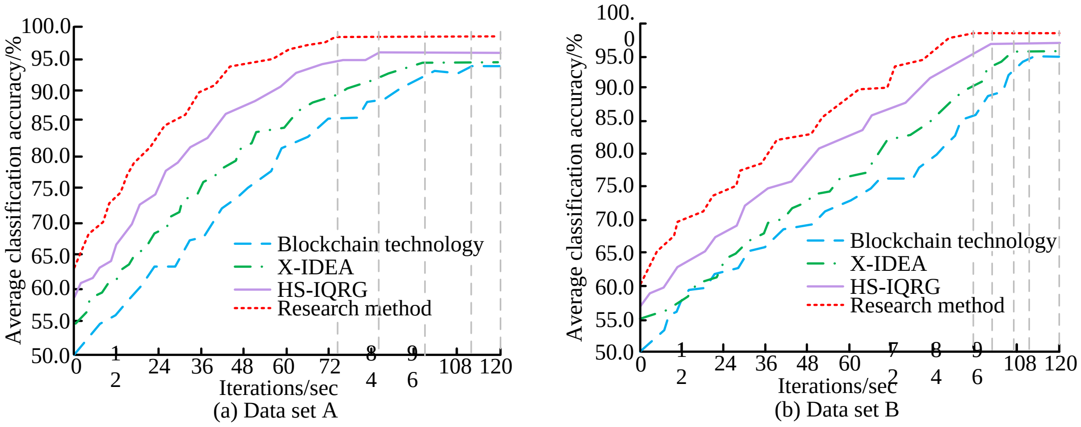


Figure 9: Comparison of ROC changes

In Figure 9, TP rate reflects the model's ability to correctly identify attacks (positive class). FP rate represents the probability that the model incorrectly identifies legitimate communications as attacks (negative class). The higher the area under the Receiver Operating Characteristic (ROC) curve, the more effective the encryption technology is at distinguishing attacks from legitimate communications. After being calculated, the ROC of the research method, Blockchain technology, X-IDEA, and HS-IQRG algorithms is 0.978, 0.967, 0.951, and 0.914, respectively. By comparison, the AUC of the research method is much greater than that of the other three methods. The AUC value of the research method is closer to 1, which shows that the model has better classification ability and higher diagnostic accuracy. This is mainly because GAN detects data faster and can generate new data according to the characteristics of real data. It also shows that the proposed GAN-based encryption technology is significantly better than other technologies in terms of AUC value. This technology has high accuracy and diagnostic capabilities in identifying attacks and legitimate communications. The research method has better detection performance in the process of encrypting computer communication system data, which helps computer engineers better protect data. Classification accuracy is a measure of the consistency between the model's predictions and the actual results. In the context of data encryption, classification accuracy reflects the model's ability to encrypt and decrypt data in practical applications. On this basis, the average classification accuracy of the four methods for ciphertext detection on the two datasets was then compared. The results are shown in Figure 10.

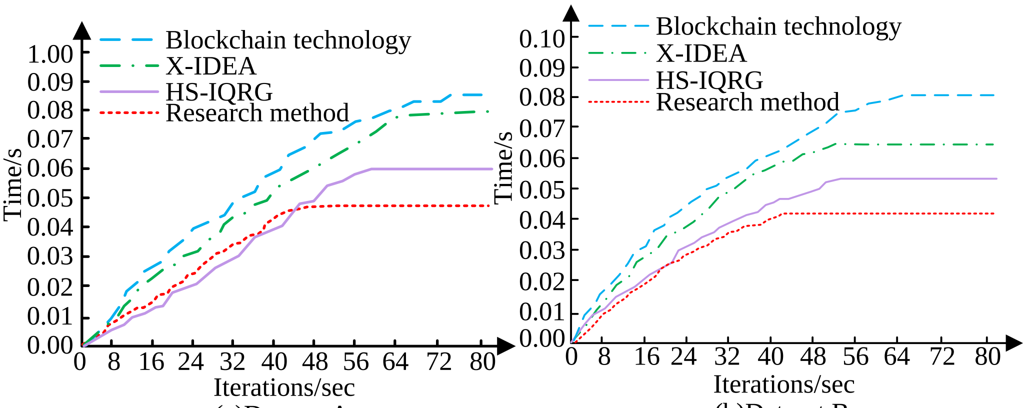


(a) Data set A

(b) Data set B

Figure 10: Comparison of average classification accuracy

Figure 10 (a) shows the average classification accuracy changes of these four models on dataset A. When the iteration changes, the average classification accuracy of all four models shows a rapid increasing trend. When the system iterates to 75 times, the research method has the maximum classification accuracy, with a value of 98.24%. At this point, the average classification accuracy of Blockchain technology, X-IDEA, and HS-IQRG is constantly changing. When the system iterates 111, 98, and 86 times, the classification accuracy of Blockchain technology, X-IDEA, and HS-IQRG is 93.21%, 94.57%, and 96.23%, respectively. The classification accuracy of the research method on dataset A is significantly higher than other algorithms. Figure 10 (b) shows the average classification accuracy changes obtained by different algorithms running on dataset B. When the classification accuracy of the research method continuously approaches 99.99%, the corresponding system iteration is 96 times. At this point, the average classification accuracy of other three methods does not reach a stable state. When the system iterates 112, 107, and 100 times, the classification accuracy of Blockchain technology, X-IDEA, and HS-IQRG is 93.54%, 94.68%, and 98.79%, respectively. According to the significance comparison, there is a significant difference in classification accuracy between the research method and the other three methods. This indicates that the research method has a relatively small error between the actual detection and measurement data in computer communication data encryption, resulting in a higher accuracy of data encryption. Then, in Figure 11, a comparison was made on the time required for these four methods to train and run until reaching a stable state on two datasets.



(a)Dataset A

(b)Dataset B

Figure 11: Time taken for reaching stable state

Figure 11 (a) shows the stability time comparison of four methods on dataset A. When the iteration runs 44 times, the running time of Blockchain technology, X-IDEA, HS-IQRG, and the research method is 0.0654, 0.0537, 0.0432, and 0.0424, respectively, with the research method approaching a stationary state. In Figure 11 (b), when the iteration runs to 43 times, the research method begins to approach stationarity, while other models are still fluctuating. At this time, the running time of Blockchain technology, X-IDEA, HS-IQRG, and the research method is 0.0655, 0.0589, 0.0437, and 0.0388, respectively. By comparison, the research method is applied to the computer communication system. Meanwhile, the time it takes for the system to reach a stable state is significantly lower than other three methods, which can improve the efficiency of data encryption to a certain extent. At the same time, the research method also shows that the startup and stabilization of the system are more efficient under the research method, making the system more suitable for environments that require rapid response. Comparisons between different methods can also help identify possible performance bottlenecks or optimization opportunities. For example, if one system takes significantly longer to initialize than another system, its configuration or structure may require further analysis to determine the cause of the delay. Table 4 shows the data encryption accuracy obtained under the specific SU Signal-to-noise Ratio (SNR) and PU power ratio.

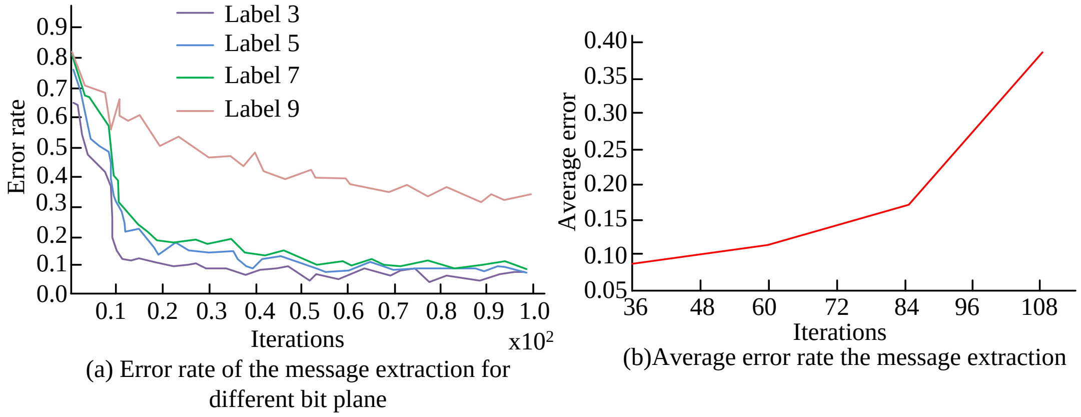
Table 4: Accuracy of four models under different SU SNR and PU power ratios

Model	SU SNR				PU power ratio				
	-10	-5	0	5	0.5:1	1.0:1	1.5:1	2.0:1	2.5:1
Blockchain technology	0.379	0.632	0.767	0.810	0.823	0.851	0.858	0.873	0.832
X-IDEA	0.455	0.702	0.817	0.831	0.841	0.872	0.884	0.881	0.865
HS-IQRG	0.621	0.874	0.908	0.902	0.944	0.961	0.927	0.962	0.943
Research method	0.787	0.968	0.981	0.947	0.963	0.977	0.968	0.979	0.958
Model	Data size/MB			Encryption time/s			Average speed/MB/s		
Blockchain technology	1024			4.2			25.28		
X-IDEA				4.8			21.68		
HS-IQRG				2.0			57.12		
Research method				1.4			69.89		

According to Table 4, when the SU SNR increases from -10 to 5, the encryption accuracy of all four models increases to varying degrees. When the SU SNR is -10, -5, 0, and 5, the encryption accuracy of the research method is 0.787, 0.968, 0.981, and 0.947, respectively. When the PU power ratio increases from 0.5:1 to 2.5:1, the encryption accuracy of all four models shows a trend of first increasing and then decreasing. When the PU power ratios are 0.5:1, 1.0:1, 1.5:1, 2.0:1, and 2.5:1, the encryption accuracy of the research method is 0.963, 0.977, 0.968, 0.979, and 0.958, respectively. When the data size is 1024MB, the encryption time of the research method is 1.4s and the average speed is 69.89MB/s. From the comparison, the research method is always more accurate than other algorithms in encrypting data when SNR and power ratio of the system environment are constantly changing. The research method also has superior performance of low time consumption and high calculation.

4.2 Application effect analysis

To further verify the feasibility of the scheme, based on the above experiments, the amount of embedded information in dataset B is increased, which means increasing labels in the encrypted image. Figure 12 shows the error rate of extracting information.



(a) Error rate of the message extraction for different bit plane

(b)Average error rate the message extraction

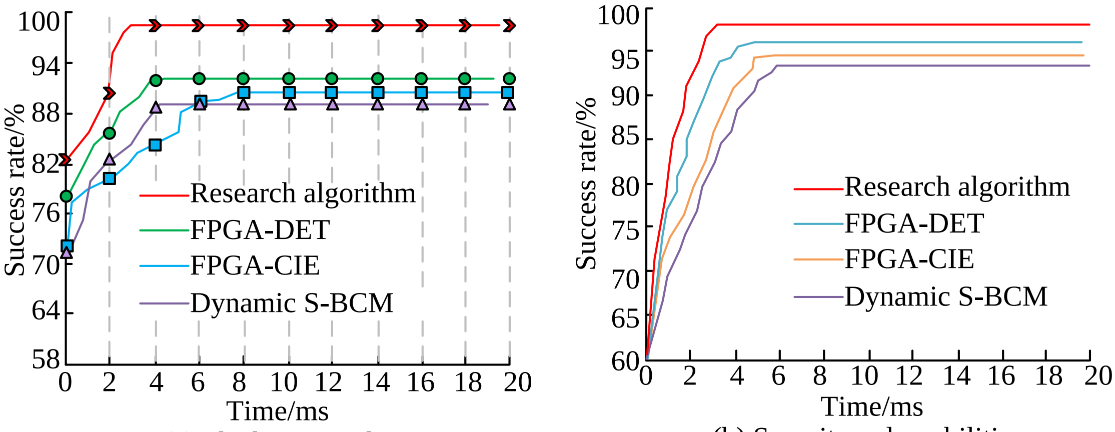
Figure 12: Error rate of extracting information

In Figure 12 (a), the number of dataset labels is 3, 5, 7, and 9, respectively. As labels in the dataset increase, the extracting information's error rate will also increase after the same training times. Figure 12 (b) is the extracting information's average error rate under different label numbers after 96 training times, which decreases as the number of labels decreases. When tags is ≤ 7, after 96 training times, the extracting information's error rate is less than 0.09. This error rate enables the computer communication system to meet the needs of real communication with the addition of error correction codes. Table 5 shows the packet loss rates of different methods.

Table 5: Comparison of packet loss rates among different methods

SNR	Research method	Blockchain technology	X-IDEA	HS-IQRG
1	0.010	0.041	0.038	0.031
2	0.009	0.040	0.037	0.030
4	0.008	0.039	0.036	0.029
6	0.007	0.037	0.035	0.028
8	0.006	0.035	0.034	0.027
10	0.005	0.034	0.033	0.026

According to Table 5, the computer communication system data encryption method designed in this study has a lower communication data packet loss rate under different SNRs, all of which are less than 0.010%. Blockchain technology and X-IDEA have higher communication data packet loss rates under different SNR, both exceeding 0.030%. Meanwhile, the packet loss rates of the three methods decrease with increasing SNR. These above results prove that the constructed method has a low packet loss rate, good overall encryption effect, high reliability, and certain application value. Finally, Field-Programmable Gate Array (FPGA)-DET based on parallel computing for data encryption and decryption, FPGA-Chaotic Image Encryption Algorithm (FPGA-CIE), and Dynamic S-box Chaotic Mapping (Dynamic S-BCM), and the research method against network intrusion is conducted [25-27]. The specific defense success rate results are shown in Figure 13.



(a) Phishing attack (b) Security vulnerabilities

Figure 13: Comparison of the defense capabilities of four algorithms against network intrusions

Figure 13 (a) shows the defense success rate against phishing attack network intrusion. When the time is 4.02ms, the maximum defense success rate of the research method is significantly higher, reaching 98.77%. At this time, the defense success rates of the other three models are significantly less than 95%. Figure 13 (b) is a comparison of the defense success rates of four algorithms against vulnerability scanning network attacks. When the system training time reaches 3.89ms, the research method's defense success rate against vulnerability attacks in webcasts can quickly reach a stable state and remain at the highest value. Comparison shows that the research method can effectively defend against different types of network attacks and successfully prevent the system from being damaged. CCA-ANC uses the generative adversarial properties of GAN to generate highly random and unpredictable encrypted ciphertext. This property makes it difficult for attackers to find patterns in encrypted data when facing powerful cryptanalysis attacks, thereby enhancing the robustness of encryption technologies. Through simulated attack tests, the CCA-ANC technology can effectively resist a variety of known cryptanalysis attacks, including different attack methods, emphasizing the significant advantages of the proposed method in terms of security.

5 Discussion

With the rapid development of computer communication systems, data security and privacy protection have become an important issue. In order to optimize the data encryption method, a data encryption method integrating CCA-ANC is proposed in this experiment. The application potential of data encryption technology based on improved GAN in computer communication systems is verified. For the chaotic compressed sensing encryption algorithm proposed by Wu T and other scholars, this algorithm combined encryption technology with OFDM-PON system in the experiment. This algorithm effectively saved network bandwidth and improved the security of data transmission. However, this algorithm had not achieved a comprehensive evaluation [28]. The CCA-ANC encryption method proposed in the experiment is analyzed through different performance indicators and shows higher data security. The data encryption method proposed by Chen et al. had good encryption effect and efficiency, which effectively resisted network search attacks. However, the performance and security of this method were significantly reduced when faced with large-scale or dynamically changing data [12]. The CCA-ANC encryption method breaks through this limitation. The key generated by GAN increases the complexity of the encryption algorithm and significantly enhances the accuracy of data encryption. When the SU signal-to-noise ratio was -10, -5, and 0, respectively, the encryption accuracy of the research method was 0.787, 0.968, 0.981, and 0.947, respectively. In the research of Tiwari D et al., they developed a lightweight secure encryption algorithm. Although this method was secure enough, it did not explain what kind of security attacks it could resist [29]. In addition, although the electronic medical health record method proposed by Ghosheh et al. effectively protected data privacy, it could not accurately predict the attacks on the system [17]. The proposed CCA-ANC encryption method can successfully resist external phishing attacks and vulnerability attacks. The proposed CCA-ANC encryption method can also be extended to various other computer communication systems. The method proposed in the experiment is also compared with the improved quantum key distribution method proposed by Nirmal Kumar et al. Although the methods of these scholars showed higher security in some aspects, under different signal-to-noise ratio changes, the packet loss rate of this method was large [30]. The packet loss rate of the CCA-ANC encryption method proposed in the experiment was always less than 0.010%, which had significantly superior network performance.

The experiment develops a new GAN-based DET by constructing an innovative encryption framework compared with the existing results. This technology shows significant advantages in resisting various known attack methods, and encryption speed is improved. It is also competitive in terms of resource consumption. While improving the security of data encryption, it is also superior to many existing methods in terms of adaptability and flexibility. This provides a new perspective on data protection in computer communication systems and points out the direction for future research.

6 Conclusion

After in-depth research and practical exploration, this article proposed and verified an improved adversarial neural network encryption algorithm for data encryption in computer communication systems. Firstly, the architecture and encryption algorithm of GAN were analyzed, followed by relevant research on neural cryptography and GAN. Subsequently, based on ANC encryption algorithm and combined with GAN, a new improved adversarial encryption algorithm model was proposed. Meanwhile, the security of this constructed algorithm was verified by introducing an EDN. These data showed that in the convergence comparison of different algorithms, when the iteration was 38 times, the research model first iterated to a stable state, corresponding to a fitness value of 0.612. The AUC of the four computer communication encryption algorithms, including the research method, Blockchain technology, X-IDEA, and HS-IQRG algorithms, was 0.978, 0.967, 0.951, and 0.914, respectively. On dataset A, when the research method iterated 75 times, it had a maximum classification accuracy of 98.24%. When the iteration ran 44 times, the running time of the research method was 0.0424 seconds. On dataset B, when iterating 96 times, the classification accuracy of the research method continuously approached 99.99%. When the iteration reached 43 times, the research method began to approach stationarity, taking only 0.0388 seconds. When the SU SNR was -10, -5, 0, and 5, the encryption accuracy of the research method was 0.787, 0.968, 0.981, and 0.947, respectively. When the labels were ≤ 7, after 96 training times, the research method's error rate in extracting information was lower than 0.09, indicating its high accuracy. The designed computer communication system data encryption method had a low packet loss rate for communication data under different SNRs, all of which were less than 0.010%. These above data all demonstrate the superior feasibility and effectiveness of the research method in encrypting data in the computer communication system, which can effectively enhance the security of data encryption. This provides a more accurate data encryption tool for computer engineers.

7 Limitations and future work

Overall, based on the proposed CCA-ANC, all models are secure when using long keys. However, the main problem currently is that the attackers will be more powerful to force the solution into a strong encryption system. That is, the CCA-ANC method alone is not enough to ensure security. Designing an adversarial attacker with a strong ability to attack cryptographic systems is the key to data security. From the minimalist models constructed in the study, it is possible to achieve data security. However, overall, it is an open problem that is very difficult to solve.

In future, more experiments can be conducted to evaluate more parameters. It is necessary to implement a parallel approach to improve performance and longer keys and more powerful attacks. The applicability of CCA-ANC technology can be investigated in real-time communication systems, such as online gaming and telemedicine.

Potential future application of CCA-ANC is in intelligent transportation systems, where communication between vehicles and vehicles and infrastructure requires highly secure DET. Meanwhile, CCA-ANC can be optimized to achieve efficient operation for resource-constrained environments such as Internet of Things devices.

References

[1] X. Chai, Y. Tian, Z. Gan, Y. Lu, X. J. Wu, and G. Long, "A robust compressed sensing image encryption algorithm based on GAN and CNN," Journal of Modern Optics, vol. 69, no. 2, pp. 103-120, 2022. https://doi.org/10.1080/09500340.2021.2002450.

[2] J. Zong, A. Hajomer, L. Zhang, and W. Hu, "Real-time secure optical OFDM transmission with chaotic data encryption," Optics Communications, vol. 473, no. 15, pp. 542-561, 2020. https://doi.org/10.1016/j.optcom.2020.126005.

[3] H. Ren, J. Deng, and X. Xie, "GRNN: Generative regression neural network-A data leakage attack for federated learning," ACM Transactions on Intelligent Systems and Technology (TIST), vol. 13, no. 4, pp. 1-24, 2022. https://doi.org/10.1145/3510032.

[4] Z. Cai, Z. Xiong, H. Xu, P. Wang, W. Li, and Y. Pan, "Generative adversarial networks: A survey toward private and secure applications," ACM Computing Surveys (CSUR), vol. 54, no. 6, pp. 1-38, 2021. https://doi.org/10.1145/3459992

[5] Z. Yi, "Research on trade data encryption of tobacco enterprises based on adversarial neural network," Soft Computing, vol. 26, no. 16, pp. 7501-7508, 2022. https://doi.org/10.1007/s00500-021-06479-6.

[6] A. A. Shah, S. A. Parah, M. Rashid, and M. Elhoseny, "Efficient image encryption scheme based on generalized logistic map for real time image processing," Journal of Real-Time Image Processing, vol. 17, no. 6, pp. 2139-2151, 2020. https://doi.org/10.1007/s11554-020-01008-4.

[7] M. Garipcan, and E. Erdem, "DESSB-TRNG: A novel true random number generator using data encryption standard substitution box as post-processing," Digital Signal Processing, vol. 123, no. 130, pp. 185-191, 2022. https://doi.org/10.1016/j.dsp.2022.103455.

[8] H. Hong, and Z. Sun, "A flexible attribute based data access management scheme for sensor-cloud system," Journal of Systems Architecture, vol. 119, pp. 102234, 2021. https://doi.org/10.1016/j.sysarc.2021.102234.

[9] P. Kumar, and A. K. Bhatt, "Enhancing multi-tenancy security in the cloud computing using hybrid ECC-based data encryption approach," IET Communications, vol. 14, no. 18, pp. 3212-3222, 2020. https://doi.org/10.1049/iet-com.2020.0255.

[10] H. Hong, B. Hu, and Z. Sun, "An efficient and secure attribute-based online/offline signature scheme for mobile crowdsensing," Hum. Cent. Comput. Inf. Sci., vol. 11, pp. 26, 2021. https://doi.org/10.22967/HCIS.2021.11.026.

[11] Q. Yan, W. Li, J. Li, H. Sheng, and J. Zhang, "Real-time air-to-ground data communication technology of aeroengine health management system with adaptive rate in the whole airspace," Mathematical Problems in Engineering, vol. 21, no. 7, pp. 1-13, 2021. https://doi.org/10.1155/2021/9912574.

[12] M. Chen, "Accounting data encryption processing based on data encryption standard algorithm," Complexity, vol. 2021, no. 5, pp. 1-12, 2021. https://doi.org/10.1155/2021/7212688.

[13] T. Andrius, H. A. Winther, K. Kazuya, D. Bacon, R. Nichol, and B. Mawdsley, "Investigating cosmological GAN emulators using latent space interpolation," Monthly Notices of the Royal Astronomical Society, vol. 506, no. 2, pp. 3049-3067, 2021. https://doi.org/10.1093/mnras/stab1879.

[14] D. Luo, M. Nie, and X. Wu, "Generating basic unit movements with conditional generative adversarial networks," Chinese Journal of Electronics, vol. 28, no. 6, pp. 1099-1107, 2019. https://doi.org/10.1049/cje.2019.07.013.

[15] P. Wang, F. Si, W. Fan, and S. Ren, "Data enhancement for data-driven modeling in power plants based on a conditional variational-adversarial generative network," Industrial & Engineering Chemistry Research, vol. 60, no. 24, pp. 8829-8843, 2021. https://doi.org/10.1021/acs.iecr.1c00141.

[16] C. Jiang, Y. Mao, Y. Chai, and M. Yu, "Day-ahead renewable scenario forecasts based on generative adversarial networks," International Journal of Energy Research, vol. 45, no. 5, pp. 7572-7587, 2021. https://doi.org/10.36227/techrxiv.11839122.v2.

[17] G. O. Ghosheh, J. Li, and T. Zhu, "A survey of generative adversarial networks for synthesizing structured electronic health records," ACM Computing Surveys, vol. 56, no. 6, pp. 1-34, 2024. https://doi.org/10.1145/3636424.

[18] S. Shim, "Self-training approach for crack detection using synthesized crack images based on conditional generative adversarial network," Computer-Aided Civil and Infrastructure Engineering, vol. 39, no. 7, pp. https://doi.org/1019-1041, 2024. https://doi.org/10.1111/mice.13119.

[19] A. Sarkar, "Generative adversarial networks based neural session key exchange protocol for secured transmission of information," Wireless Personal Communications, vol. 126, no. 3, pp. 2207-2229, 2022. https://doi.org/10.1007/s11277-021-08997-w.

[20] W. Zheng, K. Wang, and F. Y. Wang, "GAN-based key secret-sharing scheme in blockchain," IEEE Transactions on Cybernetics, vol. 51, no. 1, pp.

393-404, 2021. https://doi.org/10.1109/TCYB.2019.2963138.

[21] L. Raja, and S. P, Periasamy, "A Trusted distributed routing scheme for wireless sensor networks using block chain and jelly fish search optimizer based deep generative adversarial neural network (Deep-GANN) technique," Wireless Personal Communications, vol. 126, no. 2, pp. 1101-1128, 2021. https://doi.org/10.1007/s11277-022-09784-x.

[22] Z. Chen, A. Fu, Y. Zhang, Z. Liu, F. Zeng, and R. H. Deng, "Secure collaborative deep learning against GAN attacks in the internet of things," IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5839-5849, 2021. https://doi.org/10.1109/JIOT.2020.3033171.

[23] Z. S. Zhao, P. L. Li, and W. M. Gan, "Traceless encryption approach for physical layer security in coherent optical communications system," Opt. Express, vol. 31, no. 8, pp. 12585-12596, 2023. https://doi.org/10.1364/OE.482135.

[24] X. Wang, Y. Su, C. Luo, F. Nian, and L. Teng, "Color image encryption algorithm based on hyperchaotic system and improved quantum revolving gate," Multimedia Tools and Applications, vol. 81, no. 10, pp. 13845-13865, 2022. https://doi.org/10.1007/s11042-022-12220-8.

[25] A. A, Yazdeen, M. R, S, Zeebaree, M. M, Sadeeq, F. S, Kak, M. O, Ahmed, and R. R, Zebari, "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review," Qubahan Academic Journal, vol. 1, no. 2, pp. 8-16, 2021. https://doi.org/10.48161/qaj.v1n2a38.

[26] M. Maazouz, A. Toubal, B. Bengherbia, O. Houhou, and N. Batel, "FPGA implementation of a chaos-based image encryption algorithm," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 10, pp. 9926-9941, 2022. https://doi.org/10.1016/j.jksuci.2021.12.022.

[27] J. Zheng, and Q. Zeng, "An image encryption algorithm using a dynamic S-box and chaotic maps," Applied Intelligence, vol. 52, no. 13, pp. 15703-15717, 2022. https://doi.org/10.1007/s10489-022-03174-3.

[28] T. Wu, C. Zhang, Y. Chen, M. Cui, H. Huang, Z. Zhang, and K. Qiu, "Compressive sensing chaotic encryption algorithms for OFDM-PON data transmission," Optics Express, vol. 29, no. 3, pp. 3669-3684, 2021. https://doi.org/10.1364/OE.416154.

[29] D. Tiwari, B. Mondal, S. K. Singh, and D. Koundal, "Lightweight encryption for privacy protection of data transmission in cyber physical systems," Cluster Computing, vol. 26, no. 4, pp. 2351-2365, 2023. https://doi.org/10.1007/s10586-022-03790-1.

[30] S. J. Nirmal Kumar, S. Ravimaran, and M. M. Alam, "An effective non-commutative encryption approach with optimized genetic algorithm for ensuring data protection in cloud computing," Computer Modeling in Engineering & Sciences, vol. 125, no. 2, pp. 671-697, 2020. https://doi.org/10.32604/cmes.2020.09361.