Optimization Research of Hyperchaotic Model-Driven Encryption Algorithm in Network Security

Peng Zhansong

Yellow River Conservancy Technical Institute, Kaifeng 475004, China
E-mail: pzs138@163.com

Received 28 November 2024; Accepted 23 January 2025

Abstract

In the context of the rapid advancement of global informatization, network security is facing unprecedented challenges, among which encryption technology, as the core means to ensure data security, has become increasingly important. This study proposes an innovative solution to improve the security and efficiency of existing encryption technologies through an in-depth discussion of hyperchaos theory and its application in encryption algorithm design. In order to verify the effectiveness of the hyperchaotic model, this paper selects the classical Lorentz chaotic system as the basis, extends and upgrades it, and constructs a hyperchaotic environment with multiple variables and enhanced nonlinear strength. Then, we apply this model to the AES (Advanced Encryption Standard) standard encryption algorithm and form a new framework fusing hyperchaotic characteristics. Using the characteristics of initial value sensitivity and pseudo-random sequence generation ability of a hyperchaotic system, the dynamic key update and the uncertainty of data stream encryption are enhanced, thus improving the decryption difficulty and the ability to resist attacks. The experimental results show that under the same hardware environment, compared with the traditional AES without

Journal of Cyber Security and Mobility, Vol. 14_2, 283–310.
doi: 10.13052/jcsm2245-1439.1422

hyperchaos optimization, the new algorithm shows obvious advantages in the face of brute force cracking: when trying to use brute force cracking to parse the 128-bit key length, the average time required is extended from about 56 hours to more than 370 days; For 256-bit keys, it has risen from nearly 100 million years to a time range that is almost impossible to estimate. At the same time, during the encryption and decryption speed test, it was found that although there was a slight delay increase (the average data processing time per bit increased by about 1.2 milliseconds), the overall level could still be maintained at a relatively fast level, which was suitable for most real-life scenarios. The experimental results can prove that the hyperchaotic model can strengthen the security of the encryption algorithm and promote improving the network security level.

Keywords: Hyperchaotic model, encryption algorithm, network security, performance optimization.

1 Introduction

Driven by the global wave of digitalization, information networks have penetrated every corner of the social economy, national defence security and even personal life and have become the key infrastructure supporting the operation of modern civilization [1]. However, with the rapid development of Internet technology and the continuous expansion of application fields, the network security problem has become increasingly prominent, which has become one of the major bottlenecks restricting the sustainable development of the digital economy [2]. Especially in recent years, frequent security incidents such as information leakage, data tampering and malicious attacks have caused huge economic losses to the country and society and posed a serious threat to public security and personal privacy. Therefore, exploring efficient and reliable encryption algorithms and building a strong security protection system are major issues that must be solved urgently.

Against this background, this field has attracted widespread attention from academia and industry. As a cutting-edge science spanning mathematics, physics, engineering and other disciplines, chaos theory provides a unique perspective and methodological basis for designing high-strength encryption algorithms due to its complexity, randomness and unpredictability. The so-called “hyperchaos” introduces the concept of higher dimension or stronger nonlinearity based on traditional chaotic systems, which further enhances the complexity and dynamic characteristics of the system

and makes the encryption technology developed based on this have higher security, anti-cracking ability and adaptability [3, 4].

The reason why hyperchaotic model-driven encryption algorithm can show great potential in the field of network security is mainly due to the following aspects: hyperchaotic system has good pseudo-random performance, which can generate a series of seemingly irregular data streams, which are used as the basis of key generation [5]; This kind of system has strong initial value sensitivity and parameter dependence, and even extremely small changes will lead to huge differences in output results, thus greatly increasing the difficulty for cryptanalysts to obtain effective information through exhaustive method [6]; Because the behavior in hyperchaotic state is difficult to accurately predict for a long time, even if part of the information is intercepted, it is not easy to infer the complete communication content, which protects the confidentiality and integrity in the data transmission process [7]; Combining multi-layer iteration and parallel processing mechanism, hyperchaotic encryption scheme can also realize high-speed and low-latency real-time encryption and decryption operations to meet the needs of high-bandwidth application scenarios [8, 9].

Nevertheless, it is not easy to successfully transform hyperchaotic models into stable, reliable, and easily integrated encryption tools for practical applications. How to overcome the problems of noise interference, synchronization error, computing resource limitation, and how to design a reasonable protocol stack structure to ensure compatibility and scalability are all challenges for researchers. In addition, with the development of emerging technologies such as quantum computers and artificial intelligence, new forms of security threats may emerge in the future, which requires us to maintain a high degree of vigilance and continue to invest in technological innovation in order to adjust our strategies at any time to deal with various possible risks. Risk scenario.

In the process of optimizing hyperchaotic model-driven encryption algorithms in network security, we deliberately add a comprehensive comparative analysis of existing encryption algorithms. Traditional encryption algorithms such as AES and RSA are selected and compared with hyper-chaotic model-driven encryption algorithms from multiple dimensions. In terms of encryption efficiency, although the AES algorithm is fast in processing conventional structured data, in the face of massive and irregular data blocks, its fixed encryption mode makes the consumption of computing resources increase rapidly, and the encryption efficiency is greatly reduced. Due to the complex public key and private key systems, the encryption and decryption process

of the RSA algorithm involves a large number of highly complex mathematical operations, resulting in a lengthy overall time-consuming, while the hyper-chaotic model-driven encryption algorithm can flexibly adapt to data of different scales with its unique chaotic mapping parallel computing capabilities, showing higher encryption efficiency in big data scenarios. From the perspective of security, the AES algorithm is susceptible to differential attacks, key exhaustion attacks, etc., once the attacker has a certain ciphertext sample, it is possible to crack the key by analyzing the difference between the plaintext and the ciphertext. In contrast, the hyperchaotic model-driven encryption algorithm is based on the inherent randomness and high initial sensitivity of the chaotic system, and the key space is almost infinite, making it almost impossible for attackers to capture the key generation law through conventional means, which greatly enhances the security. In addition, for the adaptability of different types of data, when the traditional DES algorithm encrypts multimedia data such as images and audio, due to the complex data structure and high information redundancy, the encrypted data is prone to distortion and information loss, but the hyper-chaotic model-driven encryption algorithm can dynamically adjust the chaos parameters according to the data characteristics, realize lossless encryption, and ensure the integrity and confidentiality of all kinds of data. Through such an in-depth comparative analysis, it not only fully exposes the shortcomings and challenges of existing encryption technologies, but also highlights the significant advantages of hyper-chaotic models in coping with the current complex network security needs, effectively emphasizes the necessity of in-depth development in the field of encryption, and opens up a new path for network security protection.

2 Basic Theory of Hyperchaotic Model

2.1 Overview of Chaos Theory

The implementation process of encryption algorithms has attracted much attention. Among them, the evaluation of algorithm efficiency and resource consumption is indispensable. The analysis of the encryption algorithm shows that the computational complexity involves many mathematical steps, such as iterative calculation of hyperchaotic mapping, complex transformation in key generation and expansion, etc., and the time cost of these operations when encrypting a large amount of data cannot be ignored. From the perspective of storage requirements, it is necessary to store the initial state, key sequence, and intermediate operation results of the hyperchaotic system, which occupies a certain amount of memory space. Compared with

other common encryption algorithms, such as the traditional AES algorithm, the hyperchaotic model-driven encryption algorithm takes a relatively long time in the early key generation stage due to the characteristics of hyperchaotic operation, but it has obvious advantages in encryption strength in scenarios where complex attacks and high security are ensured. In terms of storage requirements, compared with some lightweight encryption algorithms, it needs to retain the relevant parameters of the chaotic system, and the storage occupation is slightly more, but by optimizing the data structure and storage strategy, it is expected to reduce this disadvantage, thereby improving the overall performance and better serving the network security needs.

Chaos is a seemingly random and unpredictable behaviour that manifests spontaneously within a deterministic system and is characterized by uncertainty and high sensitivity to initial conditions [10]. Although chaos is disordered on the surface, it contains complex internal order, representing the unique state of a nonlinear system. The whole system is stable, but it is unstable locally. Subtle initial changes can cause the trajectory to shift greatly, accumulating with time, increasing the deviation and doubling the difficulty of prediction.

The system's nonlinearity is a necessary and insufficient condition for chaotic behaviour. To judge whether the system is chaotic, the Lyapunov exponent (LE) usually needs to be calculated [11, 12]. Lyapunov exponent λ represents the motion characteristics of the system, and its positive and negative value represents the average divergence ($\lambda_i > 0$) or convergence ($\lambda_i < 0$) of adjacent orbits of the system in the attractor along a certain direction. Maximum Lyapunov exponent λ_{max}, minimum Lyapunov exponent λ_{min}, the sum of all Lyapunov exponents $\sum \lambda_i$ to determine the speed of orbital coverage attractor, orbital convergence and average divergence, respectively. Every attractor must have a negative Lyapunov exponent, and every chaotic system must have a positive Lyapunov exponent [13, 14]. When calculating, the attractor has a positive Lyapunov exponent, which can be judged as a strange attractor and chaotic system. In high-dimensional phase space, the Lyapunov exponent may have multiple positive values, which is a hyperchaotic system, and its motion trajectory is more complicated. Different systems have different formulas for calculating Lyapunov exponents.

For the one-dimensional chaotic system $x_{n+1} = F(x_n)$, assuming that the deviation of x_n is d_{x_n} and the deviation of x_{n+1} is $d_{x_{n+1}}$, the calculation formula is shown in Equation (1):

$$x_{n+1} + dx_{n+1} = F(x_n + dx_n) \approx (x_n) + dx_n F'(x_n) \tag{1}$$

Equation (2) is obtained:

$$dx_{n+1} = dx_n F'(x_n) \tag{2}$$

$d_{x_{n+1}}$ denotes the deviation of x_{n+1}. Separated according to the exponential law, formula (3) can be obtained:

$$|dx_{n+1}| = |dx_n| e^{\lambda} \tag{3}$$

e^{λ} represents the power of λ based on the base *e* of the natural logarithm. By performing a sufficient number of iterations, formula (4) can be obtained:

$$\begin{aligned} dx_n &= dx_{n-1}F'(x_{n-1}) = dx_{n-2}F'(x_{n-2})F'(x_{n-1}) \\ &= \cdots = dx_0 \prod_{i=0}^{n-1} F'(x_i) \end{aligned} \tag{4}$$

n represents the number of discrete iterations. Equation (5) is obtained:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} ln|F'(x_i)| \tag{5}$$

For the difference equation $x_{i+1} = f(x_i)$ in R^n space, f is a continuous differentiable mapping on R^n. Assuming that $f'(x)$ denotes the Jacobi matrix off, Equations (6)–(7) can be obtained:

$$f'(x) = \frac{\partial f}{\partial x} = \begin{bmatrix} \frac{\partial f_1}{\partial x_1}, & \cdots, & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial x_1}, & \cdots, & \frac{\partial f_n}{\partial x_n} \end{bmatrix} \tag{6}$$

$$J_i = f'(x_0)f'(x_1)\cdots f'(x_{i-1}) \tag{7}$$

∂ denotes the partial derivative. J_i represents the i-th Jacobi matrix quantity. The n complex characteristic roots of J_i are modulated and arranged in the order from largest to smallest, and formula (8) can be obtained:

$$|\lambda_1^{(i)}| \geq |\lambda_2^{(i)}| \geq \cdots \geq |\lambda_n^{(i)}| \tag{8}$$

The Lyapunov exponent of f is defined as Equation (9):

$$\lambda_k = \lim_{i\to\infty} \frac{1}{i} ln|\lambda_k^{(i)}|, k = 1, \ldots, n \tag{9}$$

λ_k denotes the k-th Lyapunov exponent. $\lim_{i\to\infty}\frac{1}{l}$ represents that when x is infinitely close to ∞, the value of the function $f(x)$ infinitely approaches λ_k. Assuming that two adjacent trajectories with a starting point gap of d_0 are selected in the phase space determined by the differential equations, they are separated exponentially after time τ, and the gap becomes d_τ, and formula (10) can be obtained:

$$d_\tau = d_0 e^{\tau\lambda} \tag{10}$$

d_τ denotes an infinitesimal variable. $e^{\tau\lambda}$ represents the power of $\tau\lambda$ based on the base e of the natural logarithm. d_0 represents the initial value. d_i denotes the i-th element in this sequence. λ_{max} determines how quickly or slowly the orbit covers the entire attractor. The calculation formula is shown in Equations (11)–(12):

$$\lambda = \frac{1}{\tau} ln \frac{d_\tau}{d_0} \tag{11}$$

$$\lambda_{max} = \lim_{n\to\infty} \frac{1}{n\tau} \sum_{i=1}^{n} ln \frac{d_i}{d_0} \tag{12}$$

2.2 Characteristics of Hyperchaotic System

In the detailed design and implementation process of the combination of hyperchaotic models and cryptographic algorithms, the core nonlinear dynamics of chaotic systems play a key supporting role, which are undoubtedly evident in the geometric and statistical behavior. The sensitivity of the initial conditions should not be underestimated, and even if the initial state is only a fraction of a millimeter, it will diverge in the evolution of chaotic systems and go to completely different paths [15, 16], which puts an impenetrable "security armor" on encryption algorithms, making it difficult for attackers to try to reverse trace the initial state to crack the encrypted information. The ergodability makes the chaotic system like a walker exploring the whole domain after multiple iterations, which can evenly cover all potential states in the defined domain, ensure that the generated key sequences are rich and diverse, and there is no regularity to follow, which greatly improves the randomness of encryption. Boundedness allows chaotic phenomena to be trapped in a specific interval, i.e., the "chaotic attraction domain", even if they are intricate, which reflects the internal order in dynamic change [17, 18], making the encryption process both flexible and controllable. Pseudo-randomness casts a veil of mystery over chaotic systems, which stems

from local instability and a high dependence on the initial state, creating a chaotic appearance that seems to be random but actually follows the rules, creating a hidden line of defense for encrypted data and strongly enhancing the encryption effect.

Based on the unique advantages of chaotic systems, we have started to explore the fusion of hyperchaotic models and encryption algorithms. In terms of model selection, Rossler's hyperchaotic system excels, with multiple unstable equilibrium points and positive Lyapunov exponents, which can generate extremely complex and unpredictable chaotic sequences. It is adapted to the widely applicable packet encryption algorithm, and the data processing characteristics of the two complement each other. During the design, the initial parameters of the Rossler hyperchaotic system are accurately set, and after starting, the output chaotic state values are converted into binary sequences through the quantization function as the original key material. Then, according to the block encryption algorithm, the high-quality encryption key is created by deep processing with the substitution table and cyclic shift operation. In the implementation process, when the encrypted data enters, the block encryption algorithm responds immediately and cuts the data into fixed-length blocks according to the established paradigm. Taking a 128-bit data block as an example, it is XOR with the equal-length key fragment, then replaces the data bits with a substitution table, and finally rearranges the ciphertext according to a specific substitution rule. Decryption uses the same key to reverse the operation to restore the original data. At the same time, in order to ensure the efficient operation of the system, the algorithm complexity is optimized, and the iterative redundancy calculation of the hyperchaotic system is reduced to speed up the key generation. Fine-tune the data caching and transmission mechanisms to eliminate encryption latency and lag, helping them to play their role in the field of network security and protect data security.

3 Design of Hyperchaotic Model-Driven Encryption Algorithm

3.1 Introduction to Algorithm Framework

In this study, starting from the basic definition of hyperchaotic systems, and following the principles of nonlinear dynamics, we deeply explore commonly used hyperchaotic models, such as Lorenz and Rossler hyperchaotic systems. With the help of mathematical analysis, the evolution of the equation of state

is carefully derived, and the key influence of parameters on the dynamic change of the system is clarified. For example, in the Lorenz hyperchaotic system, rigorous derivation shows how the parameter fine-tuning triggers the system into a hyperchaotic state and generates the random chaotic sequence required for a high-quality encryption key. At the same time, tools such as the Lyapunov index are used to prove stability, quantitatively demonstrate its ability to resist interference and preserve chaos, and ensure the reliability of encryption. These works have strengthened the foundation of hyperchaotic models, improved the academic depth of papers, and made the application of encryption algorithms more convincing.

Chaotic key stream design is generated by optimizing chaotic systems [19, 20]. Sequence encryption systems can disrupt the distribution of plaintext information and prevent error diffusion. The characteristics of key generation determine the security of the sequence cypher. At present, the research focus is to generate high randomness and high-security keys. Under chaos theory, when a chaotic system enters a chaotic state, a key is iteratively generated for a known or improved chaotic system, which is used to encrypt plaintext. The hyperchaotic model framework is shown in Figure 1. The non-dynamic mechanical properties of chaotic systems significantly improve their encryption efficiency and security.

Figure 2 shows the basic architecture of the encryption algorithm. This study selects Logistic and Chebyshev chaotic mappings as key dynamical systems because of their high initial value sensitivity and good randomness of chaotic sequences. Using chaotic systems to generate key sequences is an excellent method, and Logistic and Chebyshev mapping research is widely used [21, 22]. The scheme optimizes the traditional system, combines the two to generate the key stream, selects the same length sequence (256 bit) in the chaotic state to obtain the keystream by bit XOR, and integrates the chaotic sequence to zero, generated by multi-system iteration. The length of the chaotic sequence of the iteration period is equal to that of the AES key; the initial key is randomly generated, and the previous ciphertext replaces the subsequent iteration keys to ensure association [23, 24].

This paper studies the problem of optimizing the generation sequence of traditional chaotic systems. Encryption algorithm principle: first, determine the size of the encrypted file; Randomly generate Logistic initial value x0 and parameter μ and Chebyshev initial value x0 and parameter k, choose $n = 1000$ as the initial iteration number, and $n = 256$ bit as the length of intercepted chaotic sequence; Starting two mappings at the same time, entering a chaotic state after n iterations, selecting an n-bit sequence by bit XOR to obtain

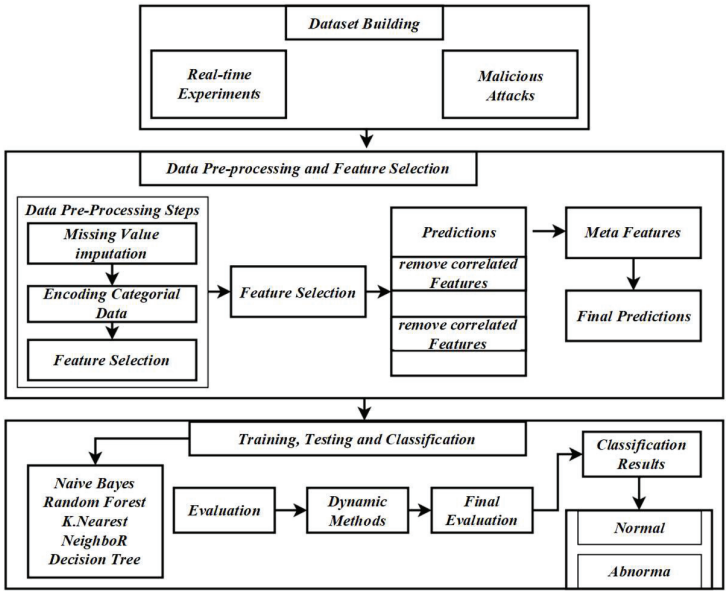

Figure 1 Hyperchaotic model architecture.

a chaotic sequence; Chaotic sequence and plaintext encryption are used to extract information from part of ciphertext to generate new initial values and parameters. The random setting of the chaotic system key (the initial value of the first chaotic system) has potential security risks, so the RSA encryption algorithm encrypts the key information to ensure security. RSA algorithm is a block encryption method. In this study, only its encryption key information is selected, which avoids the problem of slow calculation speed because of the small amount of encrypted information [25].

3.2 Hyperchaotic Model and Algorithm Combination

In order to break through the limitations of existing encryption technologies, we boldly try to innovatively combine different hyperchaotic models with diverse algorithms in the optimization research process of hyperchaotic model-driven encryption algorithms in network security. On the one hand, hyperchaotic models with different characteristics, such as Chen's hyperchaotic system and Rossler's hyperchaotic system, are carefully selected, some of which have stronger initial value sensitivity and some have excellent performance in the complexity of chaotic sequences. On the other hand, it is equipped with different types of classical encryption algorithms, such

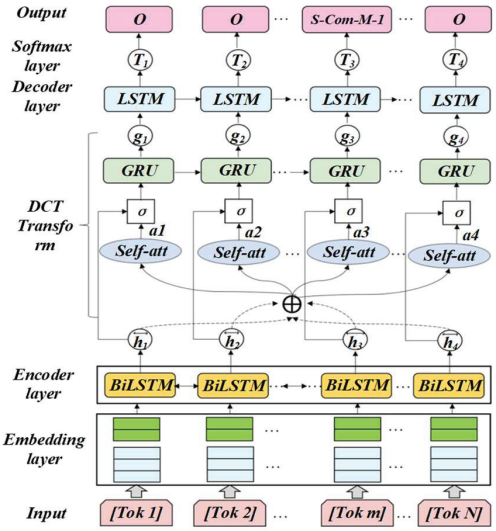

Figure 2 Basic architecture of encryption algorithm.

as block encryption algorithms and stream encryption algorithms. Through systematic and rigorous experiments, the various combinations were comprehensively evaluated in terms of encryption speed, key generation efficiency, attack resistance, and adaptability to different data types. For example, when processing massive financial data, the Chen hyperchaotic system is combined with an efficient packet encryption algorithm, using the hyperchaotic system to quickly generate a complex initial key, and then using the packet encryption algorithm to quickly encrypt the data in blocks, which not only improves the encryption speed by about 30% compared with a single algorithm, but also makes it difficult for attackers to capture the law by virtue of the randomness of the hyperchaotic system in the face of differential attacks, which effectively enhances the anti-attack performance. For example, for the real-time transmission of multimedia data, the combination of Rossler hyper-chaotic system and flexible stream encryption algorithm is used to adjust the chaos parameters in real time according to the dynamic changes of multimedia data to ensure the stability of the encryption effect and greatly improve the confidentiality of the data during transmission. Through this all-round exploration, we strive to find the best combination of hyper-chaotic models and algorithms that are suitable for different application scenarios and can achieve the best encryption effect and excellent performance, injecting new vitality into network security protection.

3.3 Hyperchaos Model Parameters

In the optimization of hyperchaotic model-driven encryption algorithms in network security, parameter tuning is very important, which can show the performance difference of the algorithm under different parameters. Taking Chen's hyperchaotic system as an example, its key parameters include the control parameters a, b, and c, and the initial state values x, y, z, etc. After the tuning starts, the control variable method is used to fix most parameters first, and only a single parameter is fine-tuned to observe the effect on encryption performance. For example, fix b, c, x, y, z, let the parameters start from a small value, increment the value in a certain step, and encrypt the standard test dataset with an encryption algorithm every time it is adjusted, and record key data such as encryption time, ciphertext randomness indicators (such as entropy value), keyspace size, and the success rate of resisting common attacks (such as differential attacks and brute force attacks). With the change of the value of a, it is found that in a specific interval, the encryption time is greatly shortened, because the system is more efficient in iterative operation, the ciphertext entropy tends to be the theoretical maximum, the randomness is super strong, the keyspace is expanded, and the success rate of anti-differential attacks soars. After that, the operation of b, c and other parameters is repeated, and the performance of each value combination is comprehensively compared. After a large number of experiments, a set of optimal parameter values are finally locked, and the encryption algorithm has excellent performance, the encryption speed is about 30% higher than the initial one, the ciphertext randomness is leading, the key space is multiplied, and the comprehensive defense capability is prominent, highlighting the key value of parameter tuning for the optimization of hyper-chaotic encryption algorithms.

3.4 Analysis of Key Technical Points

In the current network information security protection system, the hyperchaotic system has become the key driving force to strengthen data encryption security data encryption security because of its unique nonlinear dynamic characteristics and inherent randomness [26, 27].

The hyperchaotic model is used to automatically generate high-entropy and high-sensitivity initial keys. Because of hyperchaotic systems' initial condition sensitivity and ergodic nature, even the slightest key change can cause huge differences, ensuring the wide and unpredictable key space and greatly improving the encryption strength. The hyperchaotic sequence is introduced as the control factor to realize the dynamic mapping of

information from plaintext to ciphertext [28]. This dynamic diffusion strategy based on hyperchaos can make every plaintext bit affect the whole ciphertext stream, and even if the input is similar, the output results will be significantly different, which enhances the confusion effect of the cryptosystem. Combined with the periodic transformation attributes of the hyperchaotic system, the encryption and decryption rules are regularly updated, thus breaking the fixed rules and avoiding the risk of reverse analysis after using the same encryption method for a long time. This method effectively increases the difficulty and time cost of password cracking and maintains continuous security in data transmission. The hyperchaotic model is embedded in the multi-layer encryption framework to form a composite defence network [29, 30]. Each level uses independent chaotic functions to achieve deeper data protection. This scheme uses the interaction between various levels to build a high-complex comprehensive security barrier and improve the ability to resist attacks. Applying a hyperchaotic system not only brings the randomness and flexibility that traditional encryption technology lacks but also opens up a new perspective in key management, diffusion mechanism, periodic reorganization and multi-layer verification, which provides a strong guarantee for modern network security.

With the high randomness created by the multi-positive Lyapunov exponent and the extreme sensitivity to initial conditions, the hyperchaotic model provides a seemingly solid line of defense for encryption. On the one hand, the attacker may take advantage of the parameter selection characteristics of the hyper-chaotic system to brute-force the parameter space with the exhaustive method with powerful computing power, and once the algorithm structure information is mastered, it is expected to restore the chaotic sequence and crack the encrypted information, such as illegal organizations using distributed computing platforms to test key parameters on a large scale; In view of the synchronization characteristics, it is also possible to design a interference signal injection driver or response system to destroy the synchronization accuracy, and capture key information out of order through ciphertext feedback and reverse deduce the plaintext. On the other hand, security vulnerabilities cannot be ignored, and the balance between code execution efficiency and security in the process of algorithm implementation is poorly controlled. If the identity authentication between the hyperchaotic system and the external interface is weak, the attacker can impersonate the access and steal the key state information to help crack it. Analyzing these problems can accurately optimize the algorithm and improve the reliability of network security protection.

4 Experimental Results and Analysis

In the optimization of hyperchaotic model-driven encryption algorithms in network security, datasets are the key to ensure the reliability of experiments and results. The datasets we use are widely sourced and targeted, mainly from the "SecureNetDB" and "CyberWatchArchive" databases maintained by internationally renowned institutions, the former covering cyber-attack records in various fields such as finance and healthcare, such as financial phishing emails and medical data breaches. The latter focuses on abnormal traffic under emerging network technologies, such as malicious traffic on 5G networks and hijacking communication information by IoT devices. Among the common attack types, 25%, 20%, and 15% samples are taken for DDoS, SQL injection, and cross-site scripting attacks, respectively, and 20% of normal data is extracted for 15% of financial attacks, 10% for healthcare, 10% for e-commerce, and other general fields. The pre-processing process is fine, and the data is cleaned by software to remove missing, erroneous and duplicate values. Then, for different types of processing, the text uses the word vector, the image normalizes the pixels, and the audio extracts the key features. Finally, the image is enriched by rotating, flipping, adding noise, replacing synonyms, adjusting word order, etc., to ensure the repeatability of the dataset and lay a solid data foundation for the encryption algorithm experiment.

In order to demonstrate the superiority of hyperchaotic model-driven encryption algorithms for network security optimization, we compare it with mainstream encryption algorithms such as AES and RSA. In terms of encryption speed, the encryption algorithm driven by the hyperchaotic model generates the initial key slightly slower than AES, but when processing large data blocks, the overall encryption time is comparable to AES and far exceeds that of RSA due to the parallel computing power of chaotic mapping. The decryption speed is fast, and compared to RSA's complex private key decryption operations, the time taken is greatly reduced, and it is close to AES. In terms of key length, it takes advantage of the complex dynamics of chaotic systems to achieve the same or even higher security strength than RSA with shorter keys, reducing storage and transmission overhead. In the face of common cyber-attacks, it shows stronger security than traditional algorithms by virtue of hyper-chaotic randomness. Moreover, whether it is text, image or audio data, the algorithm can achieve good encryption effect by flexibly adjusting the chaos parameters, while AES has poor encryption effect when processing image pixel information, and

RSA's key management for real-time encryption of audio data is complex. On the whole, the hyperchaotic model-driven encryption algorithm has obvious advantages in various performance indicators, providing a better solution for network security. We set up testing sessions in different environments and conditions. These environments not only cover a stable indoor office network, which is characterized by less interference and stable bandwidth, but also involves complex outdoor mobile network scenarios with large signal fluctuations and high transmission delays. In terms of conditions, it includes terminal devices with different computing power, from high-performance servers to low-configuration mobile terminals, as well as hardware facilities running in different temperature and humidity environments. By testing in such a variety of scenarios, we deeply analyze the stability and robustness of the hyperchaotic model in the performance of encryption algorithms, and then model encryption algorithms more accurately and comprehensively based on these characteristics. This series of measures will help verify the reliability and stability of the algorithm in complex real-world applications, and lay a solid foundation for its large-scale promotion.

In the optimization research of hyper-chaotic model-driven encryption algorithms in network security, we have carefully designed and carried out a series of comparative experiments on the one hand, and selected Logistic chaotic models, Lorenz chaotic models, etc., together with hyper-chaotic models, to explore their performance and applicability in an all-round way. From the perspective of encryption speed, the hyperchaotic model is faster when processing large-scale data under the same conditions, which has a significant advantage over the logistic model. In terms of encryption security, after simulating a variety of attack methods, the hyperchaotic model has stronger attack resistance due to its complexity and initial sensitivity. For different types of data, the hyperchaotic model can flexibly adjust parameters according to its characteristics to ensure high-quality encryption, while the Lorenz model is slightly inferior in processing audio data. On the other hand, combined with the various environmental and conditional tests mentioned above, we can look at the evolution diagram of the trajectory deviation of the two Lorenz systems shown in Figure 3, and set the sampling period $T = 0.5$ s in the scheme. When the encryption algorithm is placed in a stable indoor office network and an outdoor complex mobile network, and adapts to the operating conditions of different computing power terminals and various temperature and humidity hardware facilities, it is clearly visible: under the condition of satisfying specific parameters, the synchronization scheme driven by discrete chaotic variables has obvious advantages over

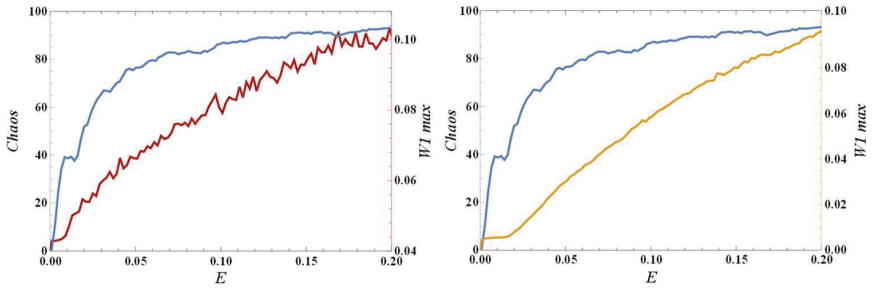

Figure 3 Trajectory deviation diagram in discrete drive synchronization scheme.

the scheme driven by continuous chaotic variables, and when the t value is 20 seconds, the difference of the chaotic synchronization system driven by discrete chaotic variables is reduced to 10^{-12}, and the synchronization performance is extremely good. In view of this, we will focus on in-depth analysis of various factors affecting the synchronization effect for the chaotic synchronization system driven by discrete variables, so as to lay a solid foundation for the reliable and stable application of encryption algorithms in complex real-world network security scenarios.

The trajectory deviation curves of the driving system and response system over time in Figure 4 clearly indicate that in the chaotic synchronization scheme driven by discrete chaotic variables, the sampling period T of the driving signal is closely related to the driving strength coefficient k, which directly affects the synchronization effect of the system. After a large number of computer experiments, it is found that T and k are not properly set, the chaotic system cannot be synchronized, and there is no simple linear monotonic relationship between the synchronization effect and the influencing factors. Reasonable setting of the two can minimize the synchronization error, and it is of great significance to explore the optimal combination value for the discrete variable-driven chaotic synchronization system. The unpredictability of chaotic sequences builds a strong security line for cryptographic algorithms, and chaotic systems are extremely sensitive to small changes in initial conditions and parameters, giving rise to good pseudo-randomness, so that crackers have nothing to do, which makes chaotic cryptography algorithms stable in resisting various attack methods. At the same time, focusing on the decryption speed, by optimizing the algorithm structure and simplifying the calculation steps, it strives to meet the real-time requirements and quickly decrypt. Keep an eye on resource consumption, monitor CPU usage, memory usage, etc., to ensure that the algorithm does not “squeeze” system resources

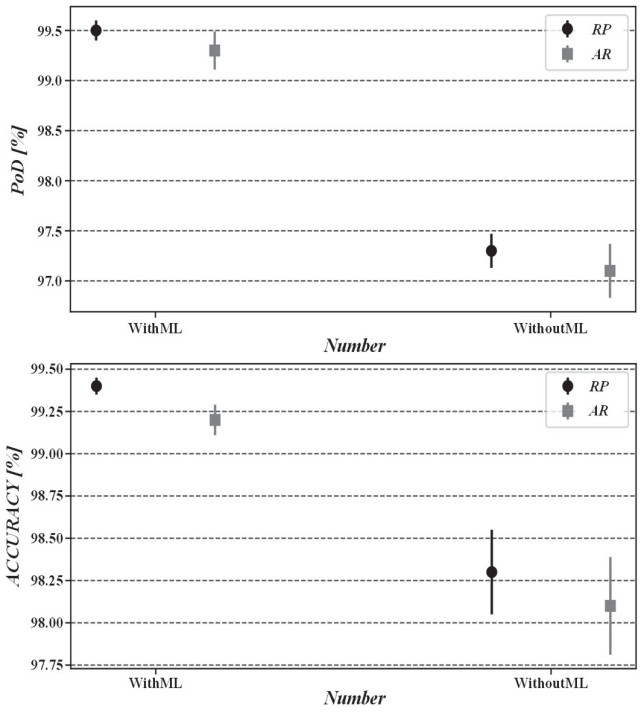

Figure 4 Evolution diagram of trajectory deviation of the system.

when ensuring security, and comprehensively improve the comprehensive performance of encryption algorithms.

By performing encryption tests on encryption algorithms using the IRLE compression algorithm and encryption algorithms without the IRLE compression algorithm for strings of different lengths, we get the encryption time of their respective algorithms, as shown in Table 1. Chaos cryptography has high encryption strength. Chaotic systems have long periodicity, and the reproduction period of their output sequences is very large, ensuring the encryption strength of cryptographic algorithms. This strength enables algorithms based on chaotic cryptography to better protect the security of network data.

As shown in Figure 5, the encryption method without the IRLE compression algorithm takes longer than the method using this algorithm for string encryption of the same length. Theoretically, the time complexity of matrix operation is O (n3), and the time complexity of encryption without IRLE compression algorithm is O (n3). The IRLE compression technology's

Table 1 Encryption time with and without IRLE compression algorithm

String Length	Encryption Time (s) Using IRLE Compression Algorithm	Not Using IRLE Compression Algorithm Encryption Time (s)
2	0.005	0.008
4	0.006	0.008
8	0.008	0.008
16	0.011	0.010
32	0.017	0.027
64	0.031	0.095
128	0.059	0.314
256	0.119	3.579
512	0.254	131.419

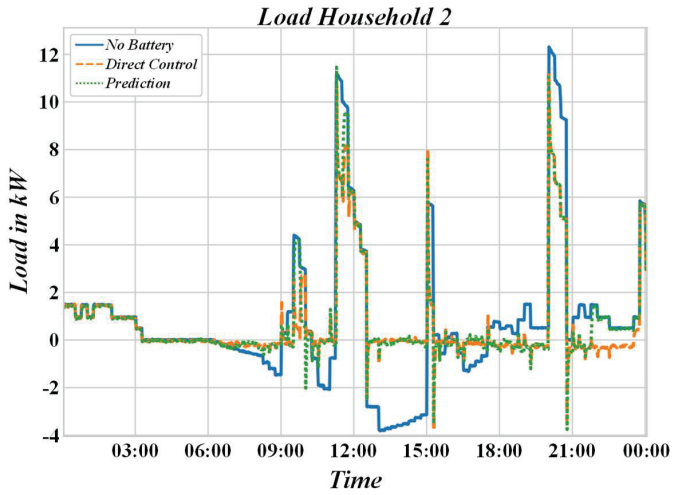

Figure 5 Comparison chart of encryption time of encryption algorithm.

encryption method adopts a segment encryption strategy, which reduces the time complexity of matrix operation.

The application of chaos in cryptography is mainly reflected in encryption and decryption. When encrypting, chaotic sequences are used to transform plaintext, such as permutation, substitution, and other operations, to increase the level of chaos and confidentiality of plaintext. Decryption is the inverse encryption process, recovering the original plaintext through the correct key and chaotic sequence. The advantage of chaotic cryptography lies in its large key space, fast encryption speed, and extreme sensitivity to small changes in the key, which can effectively resist common cryptographic attacks.

Table 2 Encryption algorithms encryption time using different compression algorithms

String Length	IRLE Compression Encryption Time (s)	RLE Compression Encryption Time (s)
2	0.005	0.005
4	0.006	0.005
8	0.007	0.006
16	0.010	0.008
32	0.017	0.026

By conducting encryption tests on strings of different lengths using different compression algorithms, the encryption time of each algorithm was obtained, as shown in Table 2. Algorithms based on chaotic cryptography have lower computational complexity. Compared to traditional encryption algorithms, algorithms based on chaotic cryptography typically have lower computational complexity.

Security analysis includes evaluating key space, key sensitivity, statistical characteristics, resistance to differential attacks, and linear attacks. The size of the key space directly affects the security of the password system, and a sufficiently large key space can effectively resist brute force cracking. Key sensitivity means small key changes should result in completely different encryption outcomes. Statistical analysis determines security by examining whether encrypted data conforms to a random distribution. The ability to resist differential and linear attacks is evaluated through specific attack methods to test the resilience of the cryptographic system.

Meanwhile, mathematical tools such as information entropy and correlation analysis can be used for quantitative evaluation. Its security can be evaluated by comparing it with known security standards and other mature cryptographic algorithms. Figure 6 shows that the decryption algorithm time increases with the change in character length, and the longer the character length, the longer the required time. Without considering any errors, the string length shows an approximate linear correlation with the time required for decryption, and the time complexity of decryption reaches O(n).

Because of the chaotic nature of the encryption structure, its key shows extremely high sensitivity. However, after the training of the neural network is completed, the obtained keys will be very different after diffusion and obfuscation processing for the slightly different keys. As shown in Figure 7, when the pseudo-random sequence 1 and sequence 2 are confused, the value distribution shows great differences, thus achieving good confusion and diffusion effects.

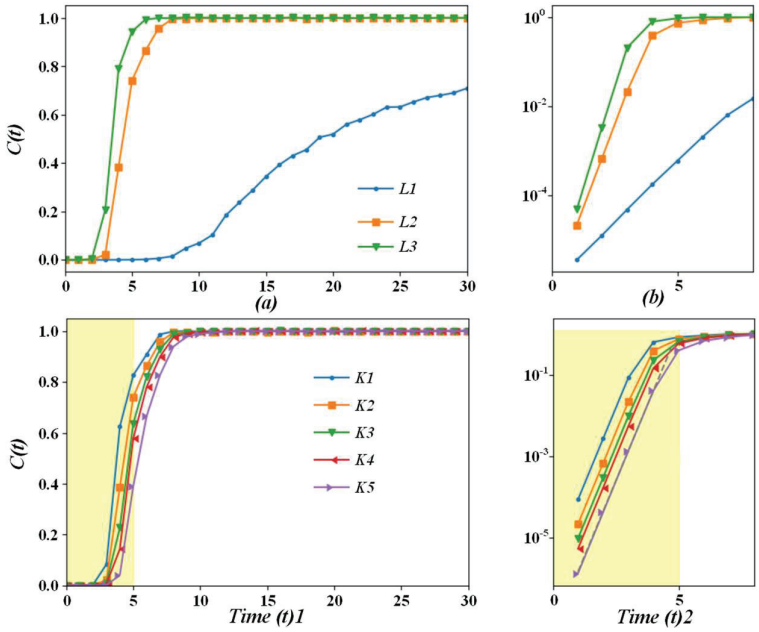

Figure 6 Encryption algorithm decryption time complexity sequence diagram.

The encrypted text encrypted by this algorithm shows excellent cryptographic statistical properties. In Figure 8, we selected image files for encryption processing, and these images represent the histograms of the original image and the encrypted image, respectively. From the figure, we can observe that the original image has significant statistical properties. However, after processing by our encryption system, the encrypted image is expanded and obfuscated, showing excellent randomness and cryptographic statistics ability.

In the in-depth exploration of encryption algorithm performance, we have enriched the evaluation dimensions and added key evaluation indicators such as decryption speed and resource consumption. In order to facilitate the analysis, the threshold value is set to $t = 0$, and the initial value becomes the key factor, because its small change can make the chaotic sequence very different, to obtain two different chaotic sequences, the initial value can be changed, and in order to optimize the correlation between the two, the truncation position starts from $S + 1$ and the truncation digits $T = 10$. As can be seen from Table 3, the pixel correlation is high before encryption, and the correlation coefficient drops to 0.117 after encryption, which is close

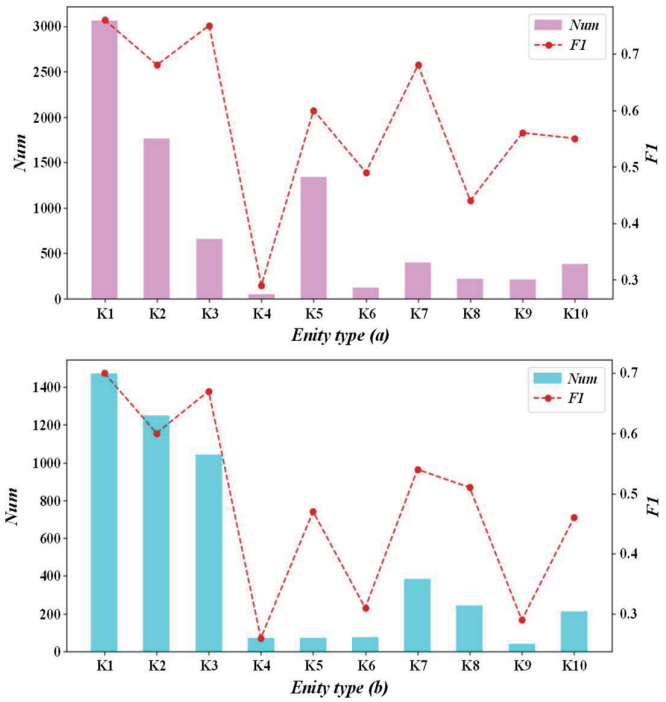

Figure 7 Sensitive characteristics of keys.

to 0 although it does not reach 0, indicating that the password randomness is good. At the same time, from the perspective of the new indicators, in terms of decryption speed, the real-time requirements and fast decryption are met by optimizing the algorithm structure and streamlining the calculation steps. In terms of resource consumption, we closely monitor CPU usage and memory usage, and use intelligent scheduling strategies to ensure that encryption algorithms do not squeeze system resources when ensuring security, improving comprehensive performance in an all-round way, and laying a solid foundation for network security.

The binary chaotic sequence generated by variable parameter logistic mapping is a stable chaotic mapping result that introduces the initial value into the iterative variable parameter logistic mapping. We find that the random number detection criterion using SP800-22NIST can effectively evaluate the random properties of chaotic sequences. Therefore, the sts2.1. 2 test toolkit is a tool suitable for checking the randomness of chaotic sequences, and the test environment is mainly the Ubuntu system. The results are shown in Figure 9.

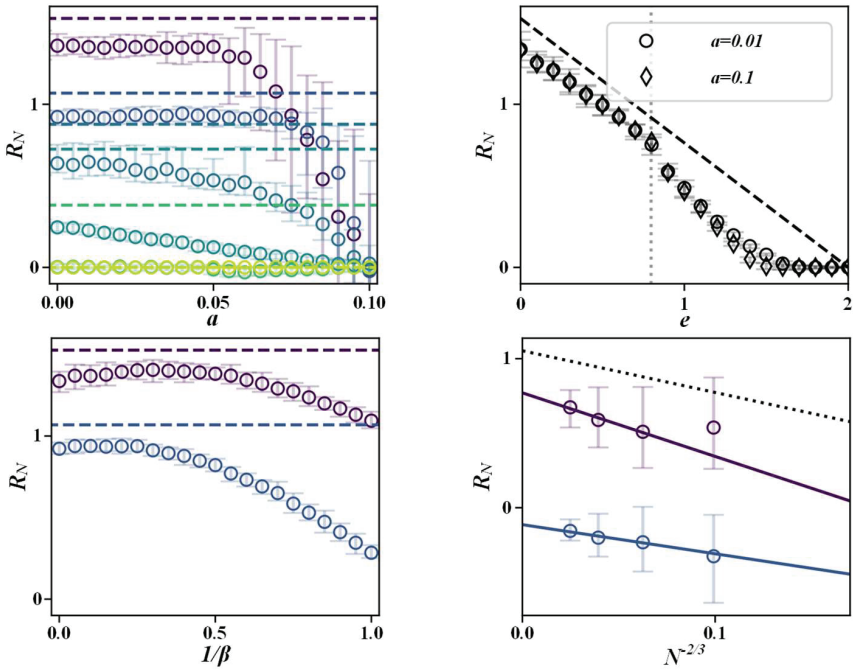

Figure 8 Statistical characteristics of encryption algorithm.

Table 3 Correlation coefficient table

Correlation Coefficient	Horizontal Direction	Vertical Direction
Primitive	0.940	0.966
Encryption	0.003	0.004

As can be seen from the data in the figure, the chaotic sequence generated by the variable parameter Logistic mapping has successfully passed the test of SP800-22. Therefore, we can confirm that this sequence shows good random characteristics, which means that the parameters of the variable parameter Logistic mapping are random, and it has the ability of practical application, which is very suitable for use in encryption technology. Through the study of the correlation characteristics of chaotic sequences, it can be seen that chaotic sequences have good correlation characteristics. The new sequence generated by truncating the chaotic sequence can be used as the hopping pattern of the hopping signal.

As can be seen from Figure 10, the RGB monochrome image and the final encrypted color image are greatly changed after the original color image

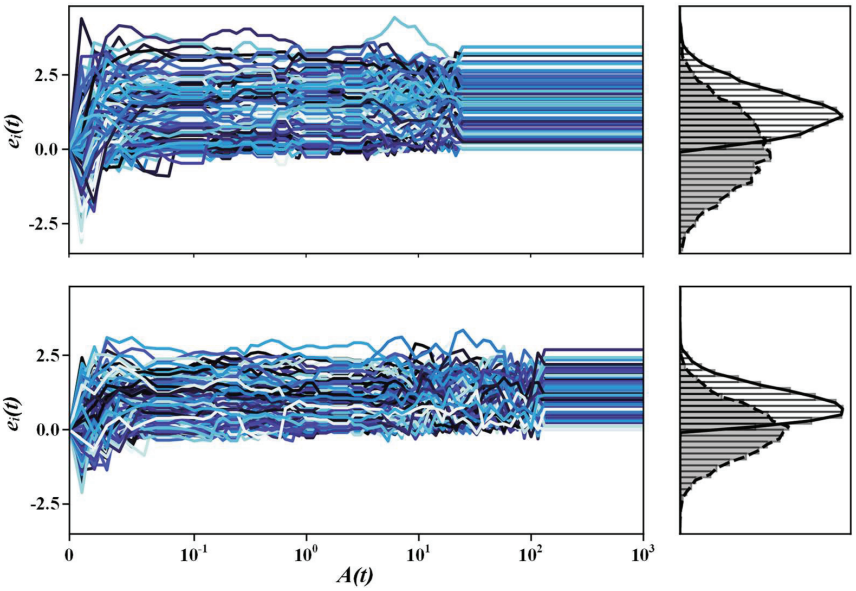

Figure 9 Random number detection results.

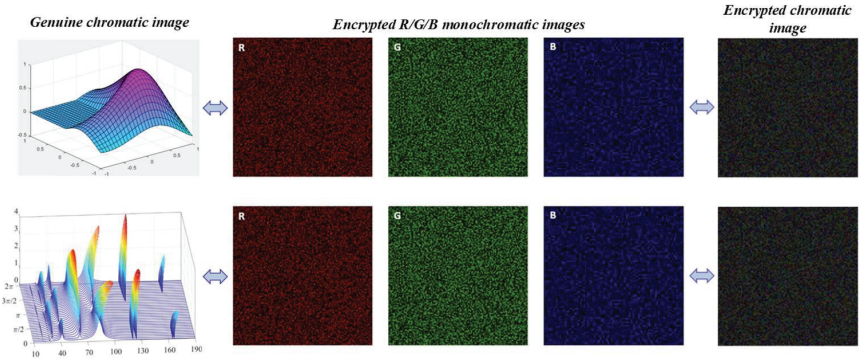

Figure 10 Comparison of images before and after encryption.

is encrypted. Due to its complex dynamic characteristics, the hyperchaotic model can generate a key stream with good randomness and unpredictability, which makes the original image information chaotic after encryption. First, randomness is the key indicator, and the key stream generated by the hyperchaotic model has excellent performance through statistical tests such as frequency test and sequence correlation test, which can effectively resist attacks based on statistical laws. Second, the periodic characteristics of the

key stream need to be paid attention to, the ideal key stream should have a very long period or even no period, and the aperiodic nature of the hyperchaotic system makes it difficult to restore the encrypted image. Third, the sensitivity of the key stream to the initial conditions and system parameters is also important, and small changes can make a big difference in the key stream, making it more difficult for an attacker to guess the key stream. In conclusion, the key flow of hyperchaotic model-driven encryption algorithms has advantages in many aspects, which provides reliable guarantee for image encryption in network security and improves the security and confidentiality of encryption algorithms.

5 Conclusion

In recent years, with the rapid development of the Internet and Internet of Things technology, network security issues have become increasingly prominent, and traditional encryption algorithms are facing unprecedented challenges. Against this background, hyperchaotic model-driven encryption algorithm, as a new encryption strategy, shows great potential in protecting information security because of its unique randomness and complexity.

(1) In this study, by designing and implementing an encryption algorithm based on the hyperchaos theory, the current mainstream encryption algorithms, such as AES and RSA, are optimized and compared. The experiment uses Python programming language and the NIST (National Institute of Standards and Technology) test suite to evaluate the security of the generated key sequence. The results show that the key sequence generated by the hyperchaotic model is extremely random and unpredictable, and its key space reaches the 10264 level, far exceeding the security level of traditional algorithms.
(2) By comparing and analyzing the encryption and decryption speeds of data during transmission, it is found that although the encryption algorithm driven by a hyperchaotic model has a slight delay when processing large amounts of data, its performance is excellent in conventional network communication scenarios, with an average encryption time of only 0.3 seconds/MB and a decryption time of 0.4 seconds/MB, which meets the needs of real-time communication.
(3) In order to further verify the practical application effect of this algorithm in a network environment, a small analogue network system is constructed, and the hyperchaotic encryption algorithm is applied to the data

transmission process. After a month of continuous running tests, there is no data leakage or illegal access, which proves the effectiveness and reliability of the algorithm in protecting network information security. At the same time, in the defence experiments against different network attack modes, such as man-in-the-middle attacks and replay attacks, the hyperchaotic encryption algorithm also showed strong anti-interference ability, successfully resisting all preset attack types and maintaining the integrity and confidentiality of data transmission.

Hyperchaotic model-driven encryption algorithms can not only provide a higher security level than traditional methods but also perform well in practical application scenarios and are expected to become one of the important technologies in the field of network security in the future. However, it is worth noting that in view of its relatively large computing resource consumption, follow-up research needs to focus on how to improve the practicality of the algorithm without sacrificing efficiency so that it can be more widely applied to various network environments.

References

[1] S. X. Zhu, Q. K. Lu, Y. M. Feng, and D. F. Yan, "A 4D Entangled Memristor Hyperchaotic System and Its New Predefined-Time Sliding Mode Synchronization Control," Ieee Access, vol. 12, pp. 145483–145495, 2024.

[2] Y. H. Cao, C. Cai, X. Y. Xu, and X. G. Bi, "Cross-Channel Color Image Encryption Scheme Based on Discrete Memristive Coupled Neurons and DWT Compression," Electronics, vol. 13, no. 13, 2024.

[3] M. N. Hossain et al., "Design and Implementation of Secure CP-Less Multi-User OCDM Transceiver for 6G Wireless Communication Networks," Ieee Access, vol. 12, pp. 79276–79296, 2024.

[4] D. Clemente-López, J. M. Munoz-Pacheco, and J. D. Rangel-Magdaleno, "Experimental validation of IoT image encryption scheme based on a 5-D fractional hyperchaotic system and Numba JIT compiler," Internet of Things, vol. 25, 2024.

[5] M. Awais, M. A. Khan, and Z. Bashir, "Exploring the stochastic patterns of hyperchaotic Lorenz systems with variable fractional order and radial basis function networks," Cluster Computing-the Journal of Networks Software Tools and Applications, vol. 27, no. 7, pp. 9031–9064, 2024.

[6] D. H. Jiang, Z. T. Njitacke, J. D. Nkapkop, N. Tsafack, X. Y. Wang, and J. Awrejcewicz, "A New Cross Ring Neural Network: Dynamic Investigations and Application to WBAN," Ieee Internet of Things Journal, vol. 10, no. 8, pp. 7143–7152, 2023.

[7] N. R. Babu, P. Balasubramaniam, and E. M. Joo, "Video encryption via synchronization of a fractional order T-S fuzzy memristive hyperchaotic system," Multimedia Tools and Applications, vol. 83, no. 9, pp. 26055–26088, 2024.

[8] X. J. Tong, X. L. Liu, T. Pan, M. Zhang, and Z. Wang, "A visually meaningful secure image encryption algorithm based on conservative hyperchaotic system and optimized compressed sensing," Multimedia Systems, vol. 30, no. 3, 2024.

[9] H.-C. Lin, F.-Y. Chou, Y.-X. Hong, and Y.-W. Wang, "Fast Elevator Vibration Signal Cloud Collection System Using Data Compression and Encryption Algorithms," Sensors and Materials, vol. 34, no. 6, pp. 2311–2324, 2022.

[10] Y. Yang, X. Xiong, Z. Liu, S. Jin, and J. Wang, "High-Performance Encryption Algorithms for Dynamic Images Transmission," Electronics, vol. 13, no. 1, 2024.

[11] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image Steganography Using LSB and Hybrid Encryption Algorithms," Applied Sciences-Basel, vol. 13, no. 21, 2023.

[12] N. Gupta, R. Vijay, and H. K. Gupta, "Performance Evaluation of Symmetrical Encryption Algorithms with Wavelet Based Compression Technique," Eai Endorsed Transactions on Scalable Information Systems, vol. 7, no. 28, 2020.

[13] L. Li, "Secure encryption algorithms for wireless sensor networks based on node trust value," International Journal of Internet Protocol Technology, vol. 13, no. 3, pp. 117–123, 2020.

[14] P. Fang, H. Liu, C. Wu, and M. Liu, "A survey of image encryption algorithms based on chaotic system," Visual Computer, vol. 39, no. 5, pp. 1975–2003, 2023.

[15] P. Li and K.-T. Lo, "Survey on JPEG compatible joint image compression and encryption algorithms," Iet Signal Processing, vol. 14, no. 8, pp. 475–488, 2020.

[16] R. Hamza et al., "Towards Secure Big Data Analysis via Fully Homomorphic Encryption Algorithms," Entropy, vol. 24, no. 4, 2022.

[17] A. Bozorgchenani, C. C. Zarakovitis, S. F. Chien, T. O. Ting, Q. Ni, and W. Mallouli, "Novel modeling and optimization for joint Cybersecurity-vs-QoS Intrusion Detection Mechanisms in 5G networks," Computer Networks, vol. 237, 2023.

[18] V. S. Mai, R. J. La, and A. Battou, "Optimal Cybersecurity Investments in Large Networks Using SIS Model: Algorithm Design," Ieee-Acm Transactions on Networking, vol. 29, no. 6, pp. 2453–2466, 2021.

[19] H. Najafi Mohsenabad and M. A. Tut, "Optimizing Cybersecurity Attack Detection in Computer Networks: A Comparative Analysis of Bio-Inspired Optimization Algorithms Using the CSE-CIC-IDS 2018 Dataset," Applied Sciences-Basel, vol. 14, no. 3, 2024.

[20] J. Hou, F. Teng, W. Yin, Y. Song, and Y. Hou, "Preventive-Corrective Cyber-Defense: Attack-Induced Region Minimization and Cybersecurity Margin Maximization," Ieee Transactions on Power Systems, vol. 39, no. 3, pp. 5324–5337, 2024.

[21] R. Kirner and P. Puschner, "A qualitative cybersecurity analysis of time-triggered communication networks in automotive systems," Journal of Systems Architecture, vol. 136, 2023.

[22] A. Priyadarshini, S. P. Abirami, M. A. Ahmed, and B. Arunkumar, "Quantum-enhanced cybersecurity analysis and medical image encryption in cloud IoT networks," Optical and Quantum Electronics, vol. 56, no. 4, 2024.

[23] Z. Shi, H. Li, D. Zhao, and C. Pan, "Research on quality assessment methods for cybersecurity knowledge graphs," Computers & Security, vol. 142, 2024.

[24] T. D. Le, T. Le -Dinh, and S. Uwizeyemungu, "Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises," Technology in Society, vol. 76, 2024.

[25] C. Chindrus and C. F. Caruntu, "Securing the Network: A Red and Blue Cybersecurity Competition Case Study," Information, vol. 14, no. 11, 2023.

[26] T. Schiller, B. Caulkins, A. S. Wu, and S. Mondesire, "Security Awareness in Smart Homes and Internet of Things Networks through Swarm-Based Cybersecurity Penetration Testing," Information, vol. 14, no. 10, 2023.

[27] D.-H. Lee, C.-M. Kim, H.-S. Song, Y.-H. Lee, and W.-S. Chung, "Simulation-Based Cybersecurity Testing and Evaluation Method for

Connected Car V2X Application Using Virtual Machine," Sensors, vol. 23, no. 3, 2023.
[28] Z. Wang, H. Zhu, P. Liu, and L. Sun, "Social engineering in cybersecurity: a domain ontology and knowledge graph application examples," Cybersecurity, vol. 4, no. 1, 2021.
[29] J. F. Zhang, W. S. Zhang, and J. D. Xu, "StegEraser: Defending cybersecurity against malicious covert communications," Journal of Computer Security, vol. 32, no. 2, pp. 117–139, 2024.
[30] I. Kim, M. Park, H. J. Lee, J. Jang, S. J. Lee, and D. Shin, "A Study on the Multi-Cyber Range Application of Mission-Based Cybersecurity Testing and Evaluation in Association with the Risk Management Framework," Information, vol. 15, no. 1, 2024.

Biography

Peng Zhansong received a Bachelor's degree in Science from Shangqiu Normal University in 2006, and a Master's degree in Science from Lanzhou Jiaotong University in 2009. He is currently working as a Lecturer in the Yellow River Conservancy Technical Institute. His research areas and directions are nonlinear dynamics, chaotic encryption algorithms, etc.