Data Security of Network Communication Information Based on Multiple Chaotic Mappings

Yi Liu*, Quan Long, Yan Liu, Yadong Fu,
Jianqi Li and Yiyang Fu

Information and Communication Branch of Chongqing Zhiwang Technology Industry Development Co., Ltd., Yubei District, Chongqing, 401100, China
E-mail: tgzhuanyong202309@163.com; LLL06102025@163.com; xingguang20242025@163.com; yi_liu001@outlook.com; liuyy2025202506@163.com; lyw2025333@163.com; fyy2024202506@163.com
**Corresponding Author*

Received 30 December 2024; Accepted 29 April 2025

Abstract

To lessen the strain on network nodes' storage, a group encryption technique is used in this paper to propose a data security encryption algorithm for network communication messages based on multi-chaotic mapping. The ciphertext feedback method is employed, effectively safeguarding the system against selective plaintext attacks by linking the encryption key and the shift space of each round to the ciphertext in addition to the multi-chaos mapping. This encryption algorithm is further protected against exhaustive attacks by using plaintext disambiguation. Tests show that the suggested algorithm has quick encryption times, good security, and plaintext sensitivity.

Keywords: Multiple chaotic mapping, network communication information, communication information data encryption.

Journal of Cyber Security and Mobility, Vol. 14_3, 577–596.
doi: 10.13052/jcsm2245-1439.1433

1 Introduction

The Internet has developed quickly in recent years due to advancements in science and technology. The widespread use of personal computers has also prevented some state-owned enterprises and scientific research institutions from being able to access the network. This quick and easy method of communication has become widely accepted and integrated into daily life. The Internet's popularity as an information portal has resulted in a large amount of valuable data being generated and transmitted through the network, including important official information, business secrets, and even military secrets [1].The rapid rise of the Internet has greatly increased the volume of sensitive data transmitted, raising security concerns. As more personal, financial, and governmental data is exchanged online, vulnerabilities appear, making it easier for cybercriminals to intercept or manipulate data. This emphasizes the critical necessity for modern security methods, such as encryption, to safeguard data. To solve these issues, techniques such as multi-chaotic mapping encryption have been developed, which ensures data secrecy and resilience to emerging cyber threats. These portals contain a great deal of sensitive personal data. Users could suffer significant losses if network hackers manage to intercept this data during data transmission. These new offline business models that rely entirely on IT technology for transactions necessitate the encryption of personal data [2].

As a result, more Chinese researchers in related domains have studied network communication and information security. To achieve data security protection, some scholars have developed machine learning algorithms, including supervised learning techniques like decision trees and support vector machines for communication network security protection process of data encryption, which they combine with technology that is cut and reorganised to change the encryption of privacy data [3–5]. The rapid expansion of the Internet expands the size of data transmission and the number of linked devices, giving cybercriminals greater opportunity to exploit weaknesses. As more sensitive data is transferred, the attack surface increases, making it more difficult to safeguard all access points. This complexity and the necessity for strong encryption mechanisms increase the likelihood of data breaches. The larger and more complex the network, the greater the problem of protecting data from interception and misuse, emphasizing the importance of modern security measures. To create a data encryption model allowing distributed access to meet data encryption requirements, some researchers also employ multi-authority centre attribute data encryption technology.The

multi-authority centre attribute data encryption system involves multiple entities handling various encryption aspects, improving security by decentralizing key management. This architecture is critical for systems with complex access control because it eliminates a single point of failure and allows for more precise data access rights. In the study, it is combined with multi-chaotic mapping to provide a safe, adaptable encryption solution for distributed or cloud-based applications. However, there is still an opportunity for improvement in terms of plaintext sensitivity and encryption latency [6].

A recent area of interest in cryptography research is multi-chaotic mapping confidential communication, which can improve encryption effectiveness and be applied more broadly in cryptography,multi-chaotic mapping to generate unpredictable encryption keys. The multi-chaotic mapping encryption technique improves security by utilizing several chaotic mappings to increase unpredictability, ciphertext feedback to avoid selective plaintext assaults, and key expansion to create unique encryption keys. It is highly sensitive to plaintext changes, increases resistance to cryptanalysis, and follows the confusion and diffusion principles. Furthermore, it is designed for efficient application in resource-constrained contexts such as wireless sensor networks, providing a secure and practical encryption option. Consequently, to offer some technical support for network communication security, this paper suggests a secure encryption technique based on multi-chaotic mapping for network communication information.Multi-chaotic mapping improves security by employing dynamic, non-linear encryption with keys that are affected by both beginning conditions and ciphertext feedback. This unpredictability and extra complexity make it more resistant to attacks and provide better protection than traditional approaches such as AES.

2 Principle of Chaotic Mapping Encryption

Because they are sensitive to properties like initial value, parameter, state ergodicity, mixing, and similar randomness, chaotic mappings are widely used for data confidentiality in network communication.

The fundamental idea behind chaotic mapping encryption is as follows: the sender overlays one or more chaotic mapping signals on the plaintext of the network communication data that needs to be transmitted. Then, the ciphertext is transmitted via the transmission channel, realising the encryption of the network communication data. The chaotic mapping sequence produced by the chaotic mapping generator acts as the key to encrypt the network communication data plaintext, giving the signals on the

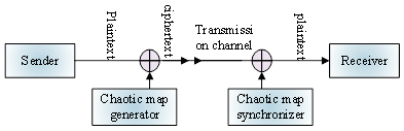

Figure 1 Chaos map encryption principle diagram.

t correspondence [7]. Figure 1 illustrates the chaotic mapping encryption concept.

Chaotic mapping synchronisation is essential for precisely recovering the plaintext signals of the sent network communication message data, as can be observed from the chaotic mapping encryption schematic diagram [8]. The synchronization of chaotic mappings is essential for accurate decryption. It assures that the receiver's chaotic system matches the sender's by starting under the same conditions. This alignment ensures the decryption key is appropriately reproduced, allowing the encrypted data to be recovered. The feedback system linked to the ciphertext aids in synchronization by rectifying any differences in real-time. As a result, synchronization assures proper decryption and increases security by preventing errors and external threats..The same chaotic system as the transmitter is obtained by applying the chaotic mapping synchroniser and setting the same initial value at the receiver, which synchronises the two systems.The diagram represents a cryptographic communication system in which the sender encrypts plaintext with a chaotic map generator, resulting in ciphertext. The ciphertext is delivered via a channel to the recipient, who decrypts it using a chaotic map synchronizer. This technique enables safe communication by synchronized chaotic maps between sender and recipient.

The symmetric encryption regime includes the chaotic mapping encryption technique, which satisfies the standards of contemporary cryptography. The multi-chaotic mapping-based encryption technique provides strong security, resists attacks such as differential analysis, and is appropriate for resource-constrained applications. However, it has limitations, such as slower encryption speeds than AES and DIOS, more sophisticated key management, and potential scalability concerns in big networks. Despite its security, computing requirements and complexity may limit its application.This system's security depends on the correlation between random quantities and the key sequence produced by chaotic mapping [9, 10]. The encryption's security is based on the randomness of the key sequence produced by chaotic mappings. The more random the key sequence, the more difficult it is for attackers to predict or reverse-engineer, increasing the system's resistance to brute force

and cryptanalysis attacks. Chaotic systems are especially successful because they are sensitive to beginning conditions, ensuring that slight changes in the input result in drastically diverse outputs, making it difficult for adversaries to understand the encryption. This randomization increases encryption by expanding the number of possible keys and providing protection against numerous attack methods. The encryption is stronger and more secure the more random the key sequence is.

3 Multi-chaos Mapping Encryption Method

3.1 Ciphertext Map

The expression of the multi-chaos mapping ciphertext can be obtained by using g to represent the network communication message data and $g(x, y)$ to denote the coordinate value.

$$Z_{ab} = g(a, b) = g(x = a, y = b) \tag{1}$$

Equation Z_{ab} indicates a particular element composition in the vector. The magnitude information and the elements through multi-chaos mapping can be used to create a network communication information data association matrix using Equation (1).

$$z_{ab} = \begin{bmatrix} z_{11} & z_{12} & \cdots & z_{1n} \\ z_{21} & z_{22} & \cdots & z_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ z_{n1} & z_{n2} & \cdots & z_{nn} \end{bmatrix} \tag{2}$$

As can be seen, each legitimate element in the multi-chaotic mapping ciphertext requires symmetric encryption, with the same key used for both encryption and decryption. At this point, the matrix transformation of the position depicted in Figure 2 can be obtained based on the multi-chaotic mapping of all the ciphertexts in the network communication information data location of all the disruptions.

According to Figure 2, the diffusion operation explicitly allows you to modify the multi-chaotic mapping ciphertext's grey value. At this point, the encryption algorithm's correlation with the global disruption parameters of mobile network communication information data can be expressed using formula (3):

$$\begin{pmatrix} d_f \\ p_f \\ q_f \end{pmatrix} = \begin{pmatrix} 1 & 1 & d_f \\ 1 & p_f + 1 & 1 \\ q_f & 1 & 1 \end{pmatrix} \bmod B \tag{3}$$

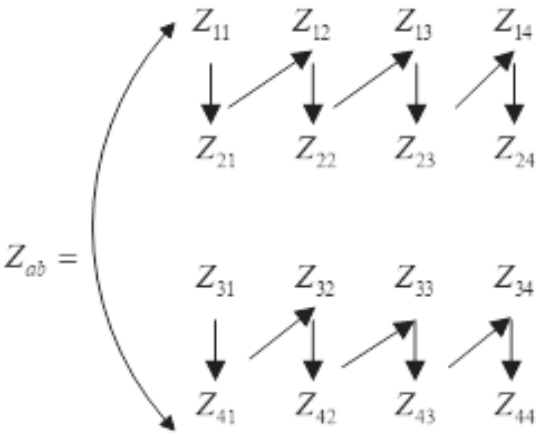

Figure 2 Matrix transformation position.

Where B indicates the data parameters of the network communication information, p_f shows the number of rows in the node-set, q_f suggests the number of columns in the node-set, and d_f indicates the total number of stored nodes in the multi-chaos mapping algorithm. The values of p_f and q_f can be computed directly because the parameters in the function have a one-to-one correspondence.

3.2 Ciphertext Feedback

Based on this, an algorithm is suggested that obtains the encryption key needed at algorithm execution time by utilising the ciphertext message's feedback mechanism against the plaintext. Using the ciphertext's feedback, the encryption key is generated at each key expansion by taking the starting positions of the random sequences produced by the 128-bit Linear Congruent Random Number Generator and the composite sequences produced by the 128-bit Logistic Integer Chaos Mapping and Cubic Integer Chaos Mapping to be different.The 128-bit Linear Congruential Random Number Generator (LCRNG) creates pseudo-random numbers for key expansion. The Logistic and Cubic Integer Chaos Mappings introduce nonlinearity and sensitivity to the initial conditions, enhancing unpredictability. Together, they provide a safe composite key that improves encryption and resists attacks.

The first 128 bits of the composite sequence are produced by the Logistic Integer Chaos Mapping and the Cubic Integer Chaos Mapping. The interplay between the linear congruential random sequence and the composite chaos

sequences is critical for improving encryption security. These sequences function together in the key expansion process, with the linear congruential sequence providing efficient randomness and the composite chaos sequences (logistic and cubic integer chaos) enhancing sensitivity to initial conditions. This combination ensures that each encryption round uses a distinct key, rendering the system immune to brute force and differential assaults. The ciphertext feedback technique increases this interaction by ensuring unpredictability and strong encryption security.The first 128 bits of the random sequence produced by the linear congruent random number generator are used to implement the encryption algorithm. The Linear Congruential Random Number Generator (LCRNG) and Logistic and Cubic Integer Chaos Mappings are critical to enhancing the encryption technique. The LCRNG generates pseudo-random numbers that drive the key expansion process, assuring randomness and protecting against attacks such as selective plaintext assaults. Chaotic mappings introduce complicated, sensitive sequences that strengthen the encryption's confusion and diffusion qualities, resulting in extremely unexpected ciphertext. Together, they improve security by improving unpredictability and resistance to cryptanalysis, making encryption more resilient. This method generates grouped ciphertext when there is no ciphertext feedback. But after creating a ciphertext $C_j = [A, B]$ (the first 64 bits for ciphertext A and the second 64 bits for ciphertext B), the aforementioned key expansion is carried out once more after the sum of the aforementioned control parameters m and n, is determined using formulas like (4) and (5).

$$m = c_{A1} + c_{A2} + c_{A3} + c_{A4} \tag{4}$$

$$n = c_{B1} + c_{B2} + c_{B3} + c_{B4} \tag{5}$$

Where $C_{j,4}/C_{jB}$ is the A/B part of the jth block and $C_{j,4}/C_{jB}(i = 1, 2, 3, 4)$ is the value of the ith byte of $C_{j,A}/C_{jB}$.

The ciphertext feedback is used to guarantee the security of the encryption system by the data association matrix encryption design principle for network communication information, which follows the principles of confusion property and diffusion property [11–13]. Ciphertext feedback alters each encryption round based on previous outputs, enhancing security. The ciphertext feedback approach enhances security by dynamically changing the encryption process. It feeds the ciphertext back into the system, which generates fresh encryption keys, making each encryption unique. This makes it impossible for attackers to predict or deduce key sequences, even with access to several ciphertexts. Connecting the encryption key to the ciphertext

successfully protects against selective plaintext assaults, resulting in stronger and more unpredictable encryption.

3.3 Encryption Process

As illustrated in Figure 3, the encryption procedure of the communication message data of the multi-chaos mapping network is established following the implementation of the ciphertext feedback.

Step 1: Use the key expansion algorithm to generate the encryption key (A_j) and the number of shift bits (D_j);

Step 2: Divide the plaintext M. Each group has an $\mathrm{L} = 8$ byte.

$$M = \underbrace{m_0 m_1 \ldots m_{L-1}}_{h0} \underbrace{m_L \ldots m_{2L-1}}_{h1} m_{2L} \ldots \tag{6}$$

m_j denotes the jth byte value; $m_j m_{j+1} K m_{j+L-1}$ and m_j are combined to form a binary plaintext block; 333 represents this 8 -byte chunk;

Step 3: Preprocess block M_j of the plaintext to create a new block M'_j by cyclically shifting it left by D_j bits.

Step 4: Using the encryption key $A_j : C_j = M'_j \oplus A_j$, perform an iso-or to create a ciphertext for the new block M'_j.

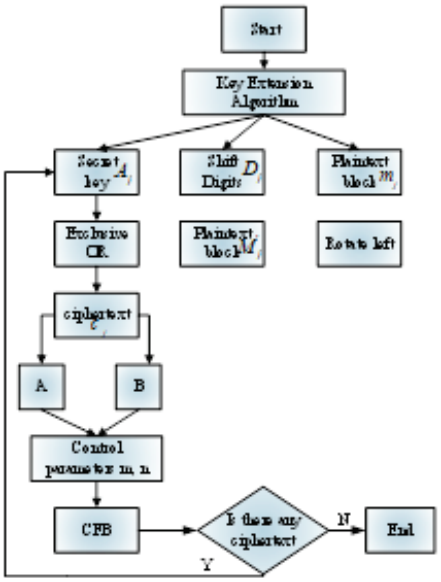

Figure 3 Multiple chaotic maps are used to create an encryption flowchart.

Step 5: Create m, n in line with the generation method of control parameters m, n, for ciphertext feedback, and divide the generated 64-bit ciphertext $C_j = c_j c_{j+1} \ldots c_{j+7}$ into two parts A and B , where $A = c_j c_{j+1} c_{j+2} c_{j+3}, B = c_{j+4} c_{j+5} c_{j+6} c_{j+7}$.

Step 6: The encryption process is complete if all plaintext has been encrypted; if not, move on to step 2 to encrypt the remaining ciphertext.

Due to the different encryption keys used in this algorithm, even the same plaintext will yield different ciphertexts at each iteration, resulting in different m and n. Finally, different encryption keys A_j, i.e., A_j, are generated, effectively preventing the encryption system's security vulnerability in the case of a selective plaintext attack. Due to their large space, it is impossible to decipher shift sequences using exhaustive methods in a selective plaintext attack. Simple shift and all-or operations are the only ones used throughout the encryption process, making it appropriate for WSN nodes with constrained node energy and processing capability.

The ability to map and feedback the ciphertext is essential when using multiple chaotic mapping methods to encrypt network communication information. This allows for the decryption of plaintext information during the encryption process's reverse operation.

4 Experiments and Analyses

4.1 Implementation of Multiple Chaotic Mapping Group Encryption Algorithm

The encryption and decryption algorithms are implemented in code here to demonstrate the effect of encryption and decryption and to test the security performance of the designed multi-chaotic mapping group encryption algorithm. The multi-chaotic mapping technique enhances security by integrating ciphertext feedback into the encryption process, so linking the encryption key and shift parameters to the ciphertext. This dynamic shift protects against selective plaintext attacks by making it impossible for attackers to predict or manipulate the key, even with known portions of the plaintext. Furthermore, using numerous chaotic maps assures that identical plaintexts generate distinct ciphertexts in each encryption, complicating potential attacks and increasing the key space, making exhaustive attacks more difficult. The results are obtained by encrypting an image experimentally, as shown in Figure 4.

The encryption algorithm produces better results, as shown by the encryption effect on the network communication message data in Figure 4, and any

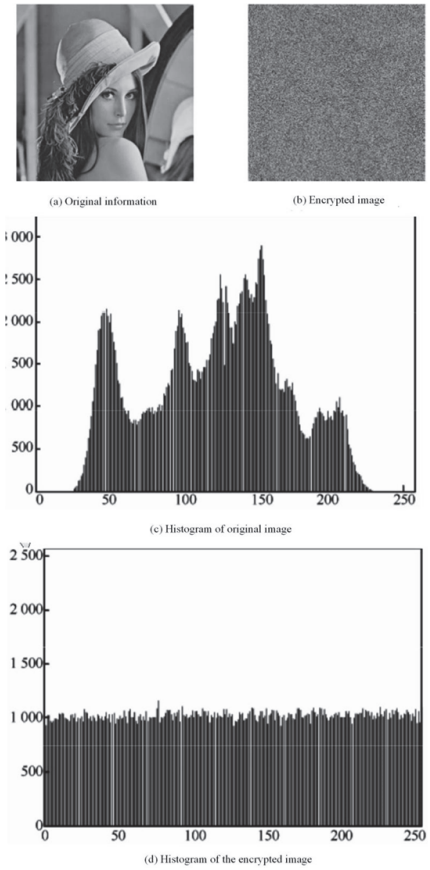

Figure 4 Information histogram before and after encryption.

pertinent information from the original plaintext cannot be retrieved from the encryption result. You cannot obtain any information about the plaintext even if you manage to decrypt the ciphertext using a key that differs by a tiny amount. Even if a portion of the key can be obtained, the entire key cannot be deduced due to the complexity of the key expansion algorithm. The encryption key and the shift space for each round will remain unknown even in the unlikely event that the entire key is recovered due to the inability to deduce the key expansion algorithm [14–16]. Shift space introduces cyclic shifts in the plaintext, further complicating the encryption. No details regarding the original ciphertext will be revealed, even if the incorrect decryption key differs slightly from the correct one.

4.2 Ciphertext Distribution and Randomness Analysis

The distribution characteristics of the plaintext and ciphertext, as well as the randomness of the ciphertext's 0–1 binary sequence, are important indicators to gauge how well the data encryption algorithm performs for network communication messages with multiple chaotic mappings.Chaotic mapping improves encryption by being extremely sensitive to beginning conditions, allowing little adjustments to create dramatically different results. Its parameterization increases flexibility, while inherent randomization assures unpredictable encryption keys, which improves security. These qualities make chaotic mapping a useful method for secure data encryption. If the ciphertext's distribution is not sufficiently random or homogeneous, the decoder can completely take advantage of this to crack the encrypted file and then decrypt it [17]. This paper encrypts an English text with a size of 8KB to reflect the performance of the encryption algorithm as accurately as possible. The corresponding histograms of the plaintext and ciphertext obtained by the encryption algorithm's action are given in the following: Figures 5 and 6.

The figure makes it evident that the plaintext and ciphertext's ASCII value spatial distributions are significantly different from one another. Since the encrypted data exhibits average homogeneous characteristics while the original plaintext data has large statistical characteristics, the information in

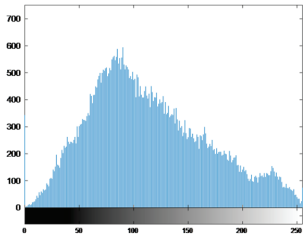

Figure 5 Clear text histogram.

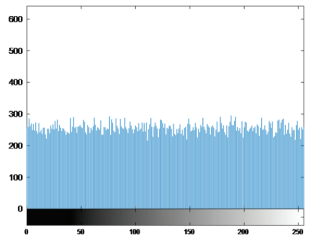

Figure 6 Cryptographic histogram.

the data can be well concealed, making it well protected against attacks based solely on cryptography.

4.3 Explicit Sensitivities

To conceal the statistical structure of the plaintext, a change in the plaintext bits of a network communication message data can result in a significant change in the ciphertext. This is because plaintext sensitivity is related to the diffusion property of multi-chaotic mapping cryptography and reacts to the encryption algorithm's resistance to differential parsing. Differential parsing—a well-known plaintext attack that takes advantage of the relationship between a particular difference and the corresponding ciphertext difference to obtain the maximum number of cypher keys—is inapplicable to this cryptosystem if a small alteration in the plaintext can result in a significantly different ciphertext.

Two sets of 250-byte plaintexts with slight variations are chosen as follows to compare the plaintext sensitivity analysis between the network communication information data encryption algorithm based on multi-chaos mapping proposed in this paper and the network communication information data encryption algorithm without multi-chaos mapping.The multi-chaotic mapping encryption algorithm provides various security benefits over older methods. It increases resilience to assaults such as selective plaintext attacks by employing a ciphertext feedback mechanism, making it difficult for attackers to decipher encryption keys. The technique also improves plaintext sensitivity, ensuring that little changes in the input result in considerable ciphertext changes, preventing differential analysis. Furthermore, using several chaotic systems increases key randomization and security while maintaining high encryption speeds, making it appropriate for resource-constrained environments such as wireless sensor networks (WSNs).

The ciphertexts produced by M1 and M2 using the data encryption algorithm for network communication messages without multi-chaos mapping and the algorithm proposed here respect it. The resulting ciphertext differencing is measured using a correlation distribution for distributivity and randomness. Figure 7 displays the ciphertext differencing, and the attached Figure 8 shows its columnar structure.

The results demonstrate that the processed ciphertexts have improved consistency and random consistency. The difference between the two encrypted ciphertexts is indicated by the result, and this significant difference suggests that the cryptographic method is more sensitive to the plaintext. The

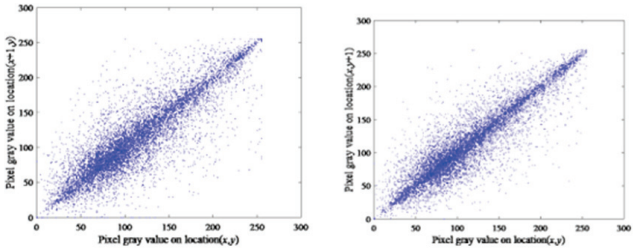

Figure 7 Data encryption algorithm for network communication information: encrypted ciphertext difference without multi-chaotic mapping (horizontal and vertical orientation).

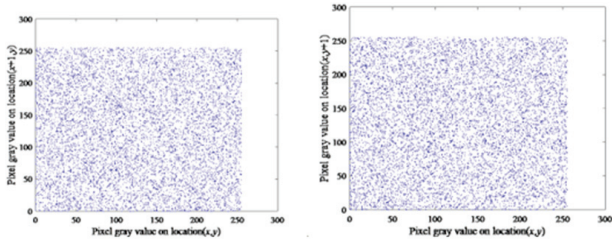

Figure 8 Network communication information data encryption algorithm based on multiple chaotic maps: encrypted ciphertext (horizontal and vertical orientation).

encrypted ciphertext created by multi-chaotic mapping is very random and uniformly distributed. Unlike plaintext, which has distinct statistical patterns, ciphertext appears uniform, making it resistant to attacks such as frequency analysis. This unpredictability is critical for secure communication because it prevents attackers from deducing information about the plaintext. The chaotic systems utilized in the encryption process ensure unpredictability, which protects the system from cryptographic attacks. These features are critical for ensuring confidentiality and preventing illegal data decryption. Figure 6 illustrates that if the plaintext remains unchanged, the network communication information data encryption algorithm without multi-chaos mapping yields the same encryption result. Conversely, Figure 7 demonstrates that if the plaintext remains unchanged, the multi-chaos mapping network communication information data encryption algorithm suggested in this paper may yield significantly different encryption outcomes. The multi-chaotic mapping network communication information data encryption algorithm indicated in this paper strengthens plaintext obfuscation. It has better sensitivity to plaintext and resistance to differential analysis, as demonstrated by a comparison of Figures 6 and 7.

4.4 Encryption Time Analysis

Since each encryption in this paper is block encryption and requires the creation of 68-bit plaintext preprocessing sequences, the packet encryption algorithm uses ciphertext feedback to affect the generation of multiple chaotic mapping sequences for each encryption. As a result, from the standpoint of encryption time, this encryption algorithm will undoubtedly increase the decryption time. The multi-chaotic mapping encryption algorithm enhances security by using plaintext sensitivity, which allows slight changes to result in significant ciphertext modifications, hence defying differential assaults. Its ciphertext feedback mechanism protects against selective plaintext attacks by changing encryption keys. The algorithm's confusion and diffusion qualities boost unpredictability, increasing resistance to cryptanalysis. Furthermore, the complex key expansion process and chaotic systems make it resistant to exhaustive attacks, providing strong security for network communication data. The encryption algorithm's increased usability in WSNs is offset by the increased security it achieves at the cost of encryption time.

The standard AES encryption algorithm, the DIOS encryption algorithm and IIBE are used and tested in conjunction with the method of this paper to confirm the efficacy of the method proposed. The comparison between AES and DIOS was most likely made because these algorithms are often used and well-established in network encryption, particularly in wireless sensor networks. AES is known for its robust security, but DIOS is regarded as efficient in resource-constrained applications. This comparison helps to validate the suggested algorithm's performance and applicability in comparable situations. The AES, DIOS and IIBE are encryption techniques that work well in wireless sensor networks and can effectively meet the networks' need for a certain amount of encryption time. Five thousand bytes of plaintext data are encrypted using three encryption algorithms. The encryption and decryption time consumption is displayed in Figure 9 for these three encryption

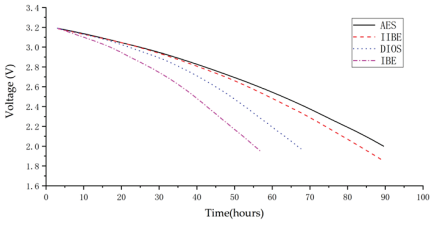

Figure 9 Comparison of encryption time among three encryption algorithms.

algorithms, which split the 5000 bytes into groups of 8 bytes to be encrypted 625 times.

The time comparison graph in Figure 9 illustrates how long it takes the AES, DIOS, and IIBE, respectively, to encrypt 5000 bytes of data: 0.976 S, 0.493 S, and 0.338 S. The IBE (our method) has significantly faster encryption and decryption speeds than both the AES and DIOS. As a result, DIOS can be used to encrypt network communication data faster than AES and IIBE.

5 Conclusion

The main topic of this paper is the encryption method for network communication information data security based on multiple chaotic mapping. It is much more secure than existing encryption methods and can withstand known plaintext attacks. The paper proposes a highly secure and practical data security encryption method for network communication information based on multi-chaotic mapping. However, the work on this topic is still very limited, and there are still many issues to be resolved in designing multi-chaotic mapping packet encryption algorithms and network communication security. This is because the security of the encryption system depends on the security of the cryptographic system, so when designing encryption algorithms, the right key management scheme must be chosen to ensure the security of the encryption system. We can investigate the multi-chaos mapping short cycle problem and learn how to create high-performance multi-chaos mapping by examining the encryption algorithm.

Declarations

Funding

Authors did not receive any funding.

Conflicts of Interests

Authors do not have any conflicts.

Data Availability Statement

No datasets were generated or analyzed during the current study.

Code Availability

Not applicable.

Authors' Contributions

Yi Liu, Quan Long, and Yadong Fu are responsible for designing the framework, analyzing the performance, validating the results, and writing the article. Yan Liu, Jianqi Li, and Yiyang collected the information required for the framework, providing software, critical review, and administer the process.

References

[1] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen. Dynamic analysis of digital chaotic maps via state-mapping networks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 66(6):2322–2335, 2019.

[2] C. Zhang, G. Shan, and B.H. Roh. Communication-efficient federated multi-domain learning for network anomaly detection. *Digital Communications and Networks*, 2024.

[3] M. Khan and F. Masood. A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimedia Tools and Applications*, 78:26203–26222, 2019.

[4] K.A. Korba, D. Abed, and M. Fezari. Securing physical layer using new chaotic parametric maps. *Multimedia Tools and Applications*, 80(21-23):32595–32613, 2021.

[5] K.S. Khalaf, M.A. Sharif, and M.S. Wahhab. Digital Communication Based on Image Security using Grasshopper Optimization and Chaotic Map. *International Journal of Engineering*, 35(10):1981–1988, 2022.

[6] J. Cui, Y. Wang, J. Zhang, Y. Xu, and H. Zhong. Full session key agreement scheme based on chaotic map in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 69(8):8914–8924, 2020.

[7] Z. Zhang, C. Zhang, M. Li, and T. Xie. Target positioning based on particle centroid drift in large-scale WSNs. *IEEE Access*, 8:127709–127719, 2020.

[8] M. Alawida, J.S. Teh, A. Mehmood, and A. Shoufan. A chaos-based block cypher based on an enhanced logistic map and simultaneous confusion-diffusion operations. *Journal of King Saud University-Computer and Information Sciences*, 34(10):8136–8151, 2022.

[9] C. Cao, Y. Tang, D. Huang, W. Gan, C. Zhang, and J. Su. IIBE: An Improved Identity-Based Encryption Algorithm for WSN Security. *Security and Communication Networks*, 2021.

[10] S. Zhu and C. Zhu. Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map. *IEEE Access*, 7:147106–147118, 2019.

[11] X. Luo, C. Zhang, and L. Bai. A fixed clustering protocol based on a random relay strategy for EHWSN. *Digital Communications and Networks*, 9(1):90–100, 2023.

[12] S. Qiu, D. Wang, G. Xu, and S. Kumari. Practical and provably secure three-factor authentication protocol based on extended chaotic maps for mobile lightweight devices. *IEEE Transactions on Dependable and Securlightweight*, 19(2):1338–1351, 2020.

[13] Y. Luo, J. Yu, W. Lai, and L. Liu. A novel chaotic image encryption algorithm based on improved baker and logistic maps. *Multimedia Tools and Applications*, 78:22023–22043, 2019.

[14] C.K. Kumar and N. Ramachandran. Intrusion Detection Model Using Chaotic MAP for Network Coding Enabled Mobile Small Cells. *Computers, Materials & Continua*, 78(3), 2024.

[15] S. Zhu and C. Zhu. A visual security multi-key selection image encryption algorithm based on new four-dimensional chaos and compressed sensing. *Scientific Reports*, 14(1):15496, 2024.

[16] M. Alawida. Enhancing logistic chaotic map for improved cryptographic security in random number generation. *Journal of Information Security and Applications*, 80:103685, 2024.

[17] R. Soni, M.K. Thukral, and N. Kanwar. A relative investigation of one-dimensional chaotic maps intended for lightweight cryptography in smart grids. *e-Prime-Advances in Electrlightweightring, Electronics and Energy*, 7:100421, 2024.

Biographies

Yi Liu graduated from Chongqing University in 2009 and is currently working at the Information and Communication Branch of Chongqing Zhiwang Technology Industry Development Co., Ltd. His research interests focus on electricity information.

Quan Long graduated from Chongqing University in 2003 and is currently employed at the Information and Communication Branch of Chongqing Zhiwang Technology Industry Development Co., Ltd. His research interests include the intelligentization of electricity.

Yadong Fu graduated from Southwest University of Political Science and Law in 2009 and is currently employed at the Information and Communication Branch of Chongqing Zhiwang Technology Industry Development Co., Ltd. His research interests include the intelligentization of electricity.

Yan Liu graduated from Sichuan University in 2008 and is currently employed at the Information and Communication Branch of Chongqing Zhiwang Technology Industry Development Co., Ltd. Her research interests include electrical automation.

Jianqi Li graduated from Chongqing University of Posts and Telecommunications in 2021 and is currently employed at the Information and Communication Branch of Chongqing Zhiwang Technology Industry Development Co., Ltd. His research interests include electronic information.

Yiyang Fu graduated from Chongqing University of Posts and Telecommunications in 2020 and is currently employed at the Information and Communication Branch of Chongqing Zhiwang Technology Industry Development Co., Ltd. His research interests include electronic information.