ZKG INTERNATIONAL
ISSN / eISSN 2366-1313
Publisher BAUVERLAG BV GMBH, AVENWEDDER STR 55, GUTERSLOH, GERMANY, 33311
Volume 25-Issue 1-(2025)
https://doi.org/10.63386/619485

OPEN ACCESS

Data security of network communication information based on multiple chaotic mappings

Check for updates

Yijiao Yang[1,a], Jingjing Xie[1,b*]

[1]Department of Information Department, Shanghai Proton and Heavy Ion Center, Shanghai Key Laboratory of Radiation Oncology, Shanghai Engineering Research Center of Proton and Heavy Ion Radiation Therapy Shanghai 201321,China ;

[a]Email: yijiao.yang@sphic.org.cn

[b]Email: jingjing.xie@sphic.org.cn

Abstract: In order 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 used, which effectively prevents the system from being harmed by a selective plaintext attack by tying 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 the use of 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

0. 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]. 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. In order to achieve data security protection, some scholars have developed machine learning algorithms 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]. In order to create a data encryption model that allows for distributed access to meet data encryption requirements, some researchers also employ multi-authority centre attribute data encryption technology. However, there is still opportunity for improvement in terms of plaintext sensitivity and encryption latency[6].

A recent area of great interest in cryptography research is multi-chaotic mapping confidential communication, which has the potential to improve encryption effectiveness and be applied more

broadly in cryptography. Consequently, in order 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.

1. Principle of Chaotic Mapping Encryption

Because of their sensitive system 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 t correspondence [7]. Fig. 1 illustrates the chaotic mapping encryption concept.

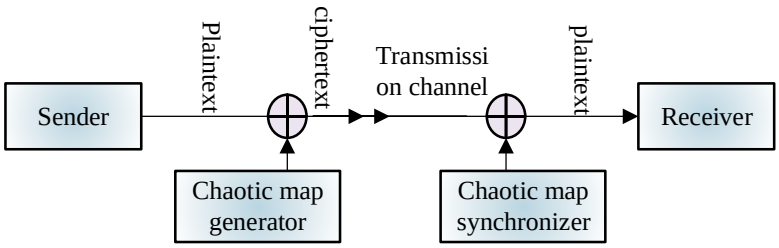


Figure 1 Chaos Map Encryption Principle Diagram

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 same chaotic system as the transmitter is obtained by applying the chaotic mapping synchroniser and setting the same initial value at the receiver; this results in the synchronisation of the two systems.

The symmetric encryption regime includes the chaotic mapping encryption technique, which satisfies the standards of contemporary cryptography. This system's security depends on the correlation between random quantities and the key sequence produced by chaotic mapping [9–10]. The encryption is stronger and more secure the more random the key sequence is.

2. Multi-chaos mapping encryption method

2.1 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.

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

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

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

As can be seen, each legitimate element in the multi-chaotic mapping ciphertext requires symmetric encryption in the multi-chaotic mapping, with the same key being 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 disruption.

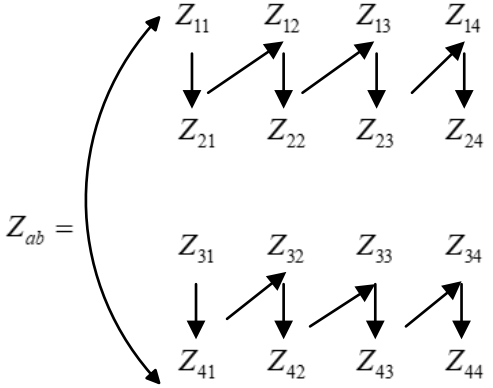


Figure 2 Matrix Transformation Position

According to Figure 2, the diffusion operation allows you to explicitly 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):

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

Where B indicates the data parameters of the network communication information, p_f indicates the number of rows in the node set, q_f indicates 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.

2.2 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 first 128 bits of the composite sequence produced by the Logistic Integer Chaos Mapping and the Cubic Integer Chaos Mapping, as well as the first 128 bits of the random sequence produced by the linear congruent random number generator, are used to implement the encryption algorithm. This is the same method used to generate the first 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).

$$m = c_{A1} + c_{A2} + c_{A3} + c_{A4} \quad (4)$$

$$n = c_{B1} + c_{B2} + c_{B3} + c_{B4} \quad (5)$$

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

The ciphertext feedback is used to guarantee the security of the encryption system in accordance with the data association matrix encryption design principle for network communication information, which follows the principles of confusion property and diffusion property[11-13].

2.3 Encryption process

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

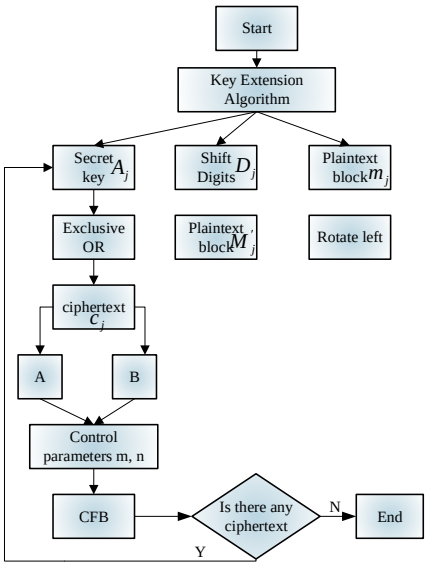


Figure 3 Multiple chaotic maps are used to create an encryption flowchart

The six steps that make up the encryption algorithm created in this paper to encrypt network communication message data with multiple chaotic mappings are as follows:

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 L=8 byte.

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

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 $M_j^{'}$.

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 $C_j = c_j c_{j+1} ... c_{j+7}$ 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 of the 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 encryption 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, which effectively prevents the encryption system's security vulnerability in the case of a selective plaintext attack. It is impossible to decipher shift sequences using exhaustive methods in a selective plaintext attack due to their large space. 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.

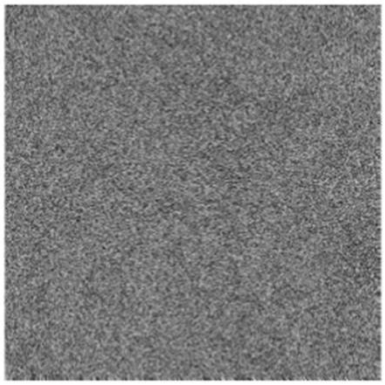
The ability to map and feedback the ciphertext is essential when using multiple chaotic mapping methods to encrypt network communication information data. This allows for the decryption of plaintext information during the encryption process' reverse operation.

3. Experiments and analyses

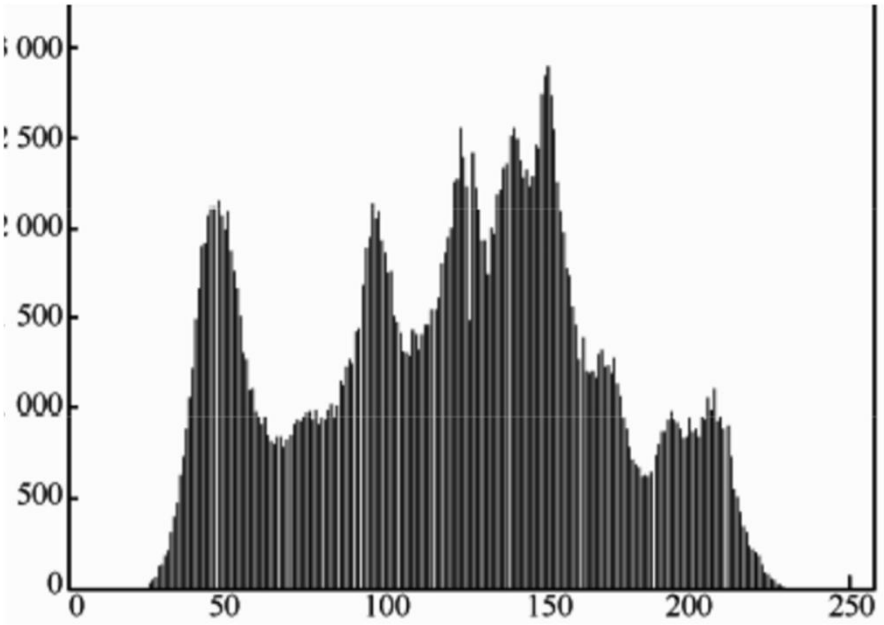
3.1 Implementation of Multiple Chaotic Mapping Group Encryption Algorithm

The encryption and decryption algorithms are implemented in code here in order to demonstrate the effect of encryption and decryption and to test the security performance of the designed multi-chaotic mapping group encryption algorithm. The results are obtained by encrypting an image experimentally, as shown in Fig. 4.

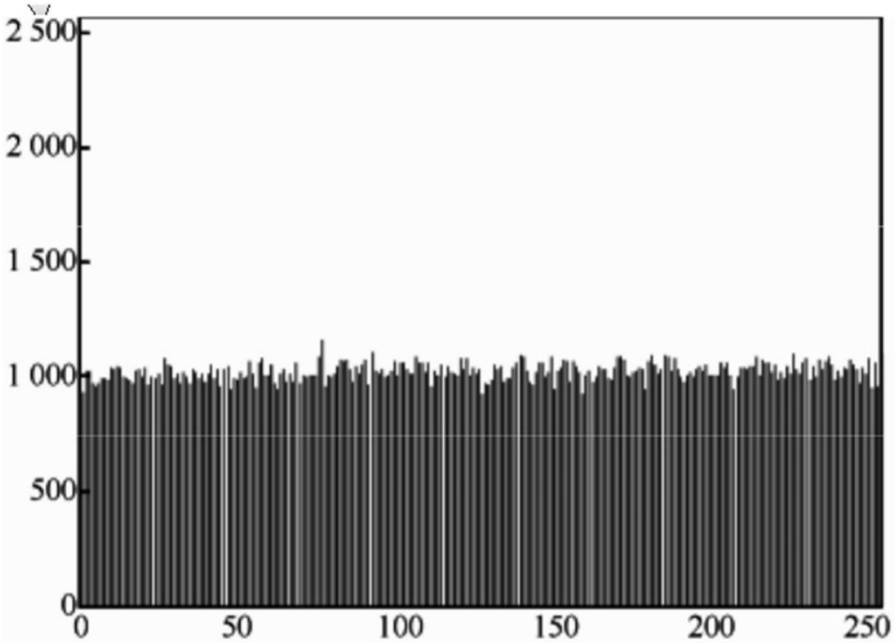
(a) Original information



(b) Encrypted image



(c) Histogram of original image



(d) Histogram of the encrypted image

Figure 4 Information histogram before and after encryption

The encryption algorithm produces better results, as shown by the encryption effect on the network communication message data in Fig. 4, and any pertinent information from the original plaintext cannot be retrieved from the encryption result at all. 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]. No details regarding the original ciphertext will be revealed, even if the incorrect decryption key differs slightly from the correct one.

3.2 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. 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 in order to as accurately reflect the performance of the encryption algorithm as possible. The corresponding histograms of the plaintext and the ciphertext obtained by the encryption algorithm's action are given in the following Fig. 5 and Fig. 6, respectively.

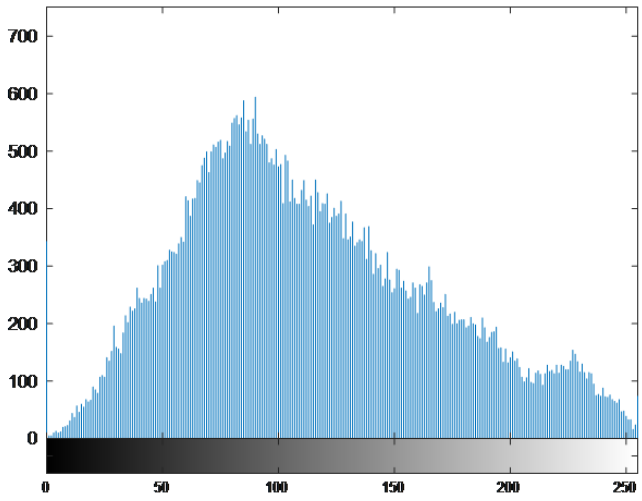


Figure 5 Clear Text Histogram

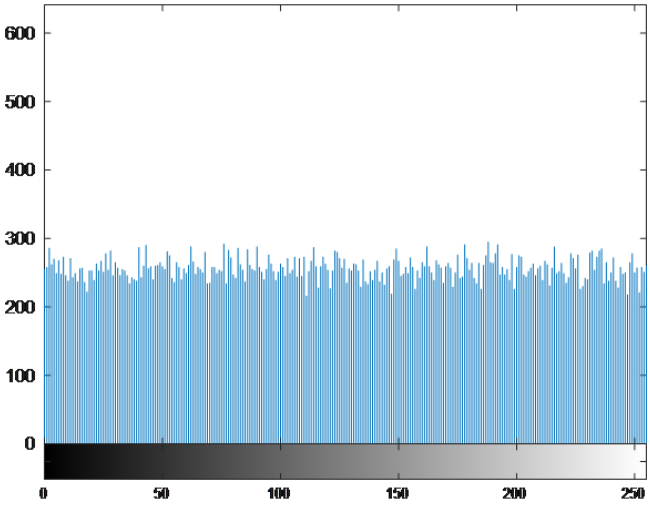


Figure 6 Cryptographic Histogram

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

3.3 Explicit sensitivities

In order 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 [18]. It is evident that 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[21,22,23].

Two sets of 250-byte plaintexts with slight variations are chosen as follows for the purpose of comparing 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 ciphertexts produced by M1 and M2 using the data encryption algorithm for network communication messages without multi-chaos mapping and the algorithm proposed here are respectively differenced. The resulting ciphertext differencing is measured using correlation distribution for distributivity and randomness. The resulting ciphertext differencing is displayed in the Figures 7, and the columnar structure of the ciphertext differencing is displayed in the attached Figures 8.

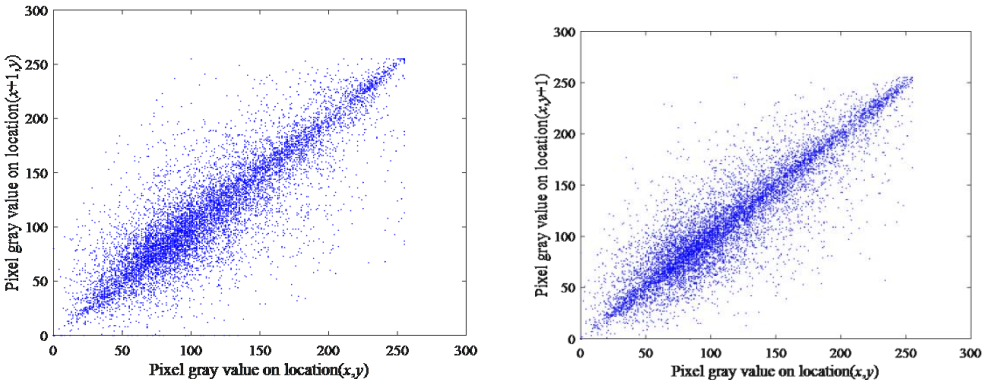


Figure 7 Data encryption algorithm for network communication information: encrypted ciphertext difference without multi-chaotic mapping (horizontal and vertical orientation)

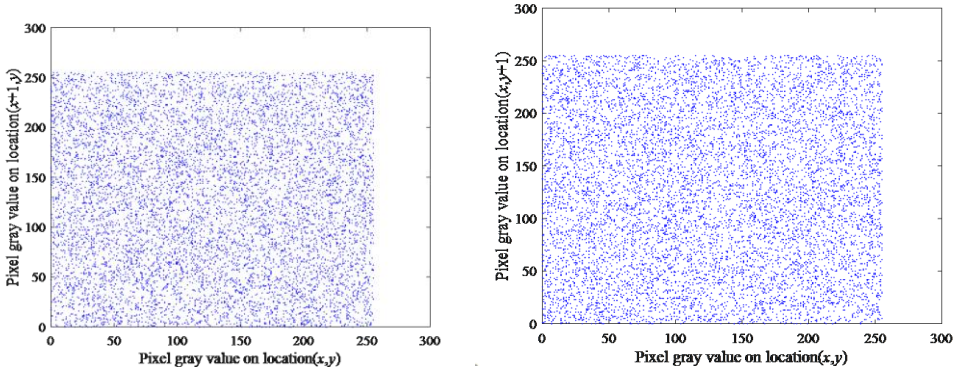


Figure 8 Network communication information data encryption algorithm based on multiple chaotic maps: encrypted ciphertext (horizontal and vertical orientation)

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. Figure 6 illustrates that, in the event that 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, in the event that 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 suggested in this paper strengthens plaintext obfuscation and has better sensitivity to plaintext and resistance to differential analysis, as demonstrated by a comparison of Figs. 6 and 7.

3.4 Encryption time analysis

Since each encryption in this paper is a 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 [19–20]. 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 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. 5000 bytes of plaintext data are encrypted using each of three encryption algorithms. The encryption and decryption time consumption is displayed in Fig. 9 for these three encryption algorithms, which split the 5000 bytes into groups of 8 bytes to be encrypted 625 times.

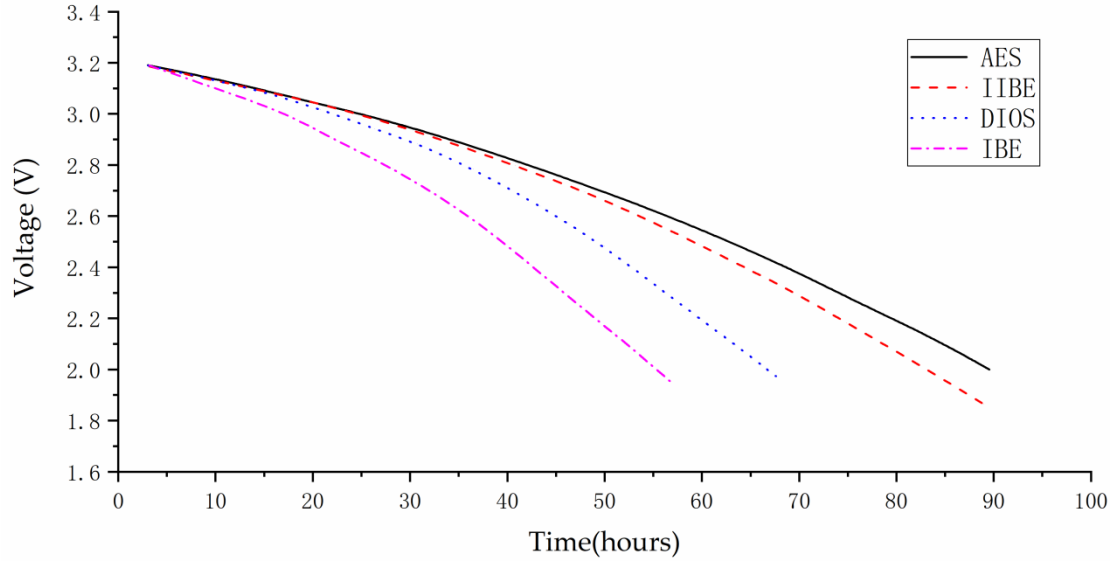


Figure 9 Comparison of encryption time among three encryption algorithms

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 at a faster rate than AES and IIBE.

4. Conclusion

The encryption method for network communication information data security that is based on multiple chaotic mapping is the main topic of this paper. 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 to date on this topic is still very limited, and there are still many issues to be resolved in the design of 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.

References

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

[2] Khan, M., & Masood, F. (2019). A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimedia Tools and Applications*, *78*, 26203-26222.

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

[4] Lin, Z., Yu, S., Lü, J., Cai, S., & Chen, G. (2014). Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system. *IEEE Transactions on circuits and systems for video technology*, *25*(7), 1203-1216.

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

[6] Zhang, C., Shan, G., & Roh, B. H. (2024). Fair Federated Learning for Multi-Task 6G NWDAF Network Anomaly Detection. IEEE Transactions on Intelligent Transportation Systems.

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

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

[9] ChunHua Cao, YaNa Tang, DeYan Huang, WeiMin Gan, Chunjiong Zhang, and Jian Su. 2021. IIBE: An Improved Identity-Based Encryption Algorithm for WSN Security. Sec. and Commun. Netw. 2021 (2021). https://doi.org/10.1155/2021/8527068

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

[11] El Assad, S., & Farajallah, M. (2016). A new chaos-based image encryption system. *Signal Processing: Image Communication*, *41*, 144-157.

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

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

[14] Ahmad, J., & Hwang, S. O. (2016). A secure image encryption scheme based on chaotic maps and affine transformation. *Multimedia Tools and Applications*, *75*, 13951-13976.

[15] Luo, Y., Yu, J., Lai, W., & Liu, L. (2019). A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia Tools and Applications*, *78*, 22023-22043.

[16] Jingchun Zhou, Qian Liu, Qiuping Jiang, Wenqi Ren, Kin-Man Lam*, Weishi Zhang. Underwater image restoration via adaptive dark pixel prior and color correction. International Journal of Computer Vision, 2023. DOI :10.1007/s11263-023-01853-3.