Hasan Uslu 152120211038

Umut Öztürk 152120211052

Abdullah Taha Aydın 152120211055

Grup NO: 2

Analysis of Encryption Techniques for Secure IoT Health Data Transfer

1. Introduction

Ensuring secure and efficient data transmission in IoT healthcare systems is critical, especially for sensitive information such as medical imaging data. This project explores various chaotic encryption methods for secure data transfer of chest tomography images. The main objective is to compare the efficiency, security, and computational overhead of different chaotic encryption techniques, including the 1D Logistic Map, 2D Henon Map, 3D Lorenz Attractor, and 4D Chen Map. The study evaluates these methods using metrics such as entropy, correlation, PSNR, SSIM, and computational time. This study differs from the existing literature on the subject as it compares four chaotic encryption methods. Although Chen Map is a widely used 3D encryption mechanism, this study uses the Chen Map method with four parameters. From these methods, it is planned to perform a secure IoMT simulation on the OMNET++ program by selecting the best (3D Lorenz Attractor) encryption method that can be used for tomography data.

2. Related Work

A 3D chaos-based encryption system ensures secure transmission of medical images in IoMT and cloud applications. Combining chaotic sequence generation, histogram equalization, rotations, and XOR operations, it achieves high security and efficient encryption. Tests show strong resistance to attacks, high entropy (7.95 out of 8), and robustness against noise, making it ideal for real-time healthcare data protection.[1]

A lightweight encryption scheme combines chaotic maps (Baker's map and 2D-Logistic Sine Coupling map) with image scrambling to secure medical images in telehealth. It ensures high security and performance with low computational requirements. Tests confirm its

[1] El-Shafai, W., Khallaf, F., El-Rabaie, ES.M. *et al.* Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services. *J Ambient Intell Human Comput* **15**, 1–28 (2024). https://doi.org/10.1007/s12652-022-03832-x

effectiveness against attacks and its ability to maintain data integrity, making it suitable for real-time medical applications.[2]

A new encryption algorithm uses multiple 1-D chaotic maps for secure medical image transmission. It employs pixel-swapping for scrambling and combines three compound chaotic maps for substitution. The method ensures robustness against plaintext attacks and achieves high security with minimal rounds. Tests confirm its effectiveness in protecting sensitive medical data while maintaining computational efficiency.[3]

A hybrid encryption and steganography model secures patient data transmission in IoT-based healthcare systems. It integrates AES and RSA encryption for strong security and uses 2D-DWT steganography to embed encrypted data into images. The model ensures high resistance to statistical attacks and data loss, safeguarding the privacy and confidentiality of sensitive medical information.[4]

Chaos-based image encryption techniques are classified into spatial, transform, and temporal domains. These methods leverage chaotic maps, such as Logistic and Lorenz maps, to achieve high randomness and low computational cost. The encryption process consists of Confusion (pixel rearrangement) and Diffusion (pixel value modification) phases. The study concludes that chaos-based encryption is more secure and efficient than traditional methods, making it ideal for encrypting large datasets.[5]

A secure medical image encryption model based on the 3D Lorenz chaotic map is proposed for IoT-powered healthcare systems. It employs MD5 for seed key generation and includes dual Confusion (column-wise and row-wise shuffling) and Diffusion phases. Encryption is performed using XOR and binary operations. The model ensures high security and privacy for medical images, effectively resisting statistical, noise, and cropping attacks, making it suitable for IoT-enabled telemedicine applications.[6]

A robust chaos-based technique enhances the security of medical image encryption within cloud-based Internet-of-Health-Systems (IoHS). This hybrid encryption/decryption scheme employs innovative perturbation algorithms to ensure the confidentiality, authenticity, and integrity of medical data during transmission and storage[7]

[2] Sudevan, S., & Jain, K. (2023). A lightweight medical image encryption scheme using chaotic maps and image scrambling. In *2023 11th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). Chattanooga, TN, USA. https://doi.org/10.1109/ISDFS58141.2023.10131882

[3] Fu, C., Shan, Y.-F., He, M.-Y., Yu, Z.-Y., & Wu, H.-L. (2018). A new medical image encryption algorithm using multiple 1-D chaotic maps. In 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 2055-2060). Miyazaki, Japan. https://doi.org/10.1109/SMC.2018.00354

[4] Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure medical data transmission model for IoT-based healthcare systems. IEEE Access, 6, 20596-20608. https://doi.org/10.1109/ACCESS.2018.2817615

[5] Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., & Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security, 21*(6), 917-935. https://doi.org/10.1007/s10207-022-00588-5

[6] Sankpal, P. R., & Vijaya, P. A. (2014). Image encryption using chaotic maps: A survey. In *Proceedings of the 2014 Fifth International Conference on Signal and Image Processing*. https://doi.org/10.1109/ICSIP.2014.80

[7] Yasser, I., Khalil, A. T., Mohamed, M. A., Samra, A. S., & Khalifa, F. (2021). A robust chaos-based technique for medical image encryption. *IEEE Access, 10*, 244-257. https://doi.org/10.1109/ACCESS.2021.3138718

A medical image encryption algorithm is introduced to enhance security and privacy in IoMT (Internet of Medical Things) applications. The algorithm consists of two stages: bit-level permutation and 2D SIM-based diffusion. This lossless encryption and decryption method is designed to address the unique structure of medical images while overcoming the limitations of low-dimensional chaotic maps, such as small intervals and limited parameters. It offers a large keyspace and high key sensitivity in both encryption and decryption.[8]

Simulations and tests validate the algorithm's efficiency and effectiveness. Security analyses reveal its resistance to common attacks, and comparisons with other techniques demonstrate superior performance in encrypting medical images.

A lightweight image encryption technique is proposed to address security challenges in IoMT-based smart healthcare systems, particularly for Electronic Health Records (EHR). The method is computationally efficient, designed for resource-constrained sensors, and supports real-time processing during emergencies.The technique uses a substitution-permutation network, splitting images into 8×8 blocks and applying bitwise XOR with transformation magic blocks generated from hash functions, tent-logistic systems, and enhanced coupling quadratic maps. These features ensure collision resistance, parameter sensitivity, and ergodicity, making the system robust and efficient.The encryption process includes two substitution stages with an intermediate image scrambling step using the Tent-Logistic System. Comprehensive analysis and comparisons highlight the technique's superior performance in entropy, differential analysis, histogram analysis, correlation coefficient analysis, key sensitivity, and computational time.Experimental results confirm the algorithm's robustness and effectiveness against attacks, making it a strong candidate for securing patient data in IoMT-based smart healthcare systems.[9]

A robust image protection scheme is proposed to secure healthcare data in IoMT-based systems. The scheme leverages an enhanced 2D discrete chaotic map with dynamic substitution using a highly nonlinear S-box and diffusion mechanisms. The S-box achieves a nonlinearity score of 112, ensuring strong encryption. The method demonstrates excellent security metrics, including correlation values below 0.0022, entropy exceeding 7.999, and NPCR values around 99.6%, indicating strong resistance to common cryptographic attacks. Comparative studies validate its efficiency and robustness, making it an effective solution for protecting medical imagery in IoMT-driven healthcare systems.[10]

[8] Ravi, R. V., Goyal, S. B., & Djeddi, C. (2022). A new medical image encryption algorithm for IoMT applications. In C. Djeddi, I. Siddiqi, A. Jamil, A. Ali Hameed, & İ. Kucuk (Eds.), *Pattern recognition and artificial intelligence. MedPRAI 2021. Communications in computer and information science* (Vol. 1543). Springer, Cham. https://doi.org/10.1007/978-3-031-04112-9_11

[9] Islam, M. O. U., Parah, S. A., Malik, B. A., & Malik, S. A. (2024). Lightweight medical-image encryption technique for IoMT based healthcare applications. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-024-19281-x

[10] Ahmad, M., Alkanhel, R.I., Soliman, N.F., Algarni, A.D., El-Samie, F.E.A. et al. (2023). Securing healthcare data in iomt network using enhanced chaos based substitution and diffusion. *Computer Systems Science and Engineering*, *47(2)*, 2361-2380. https://doi.org/10.32604/csse.2023.038439

Unlike these studies, we will choose the most suitable (3D Lorenz Attractor) one for tomography photos from the chaotic map encryption methods we have compared and we will make a simulation example on omnet++.

3. Methodology

3.1 Encryption Methods

Four chaotic encryption methods were implemented and tested:

1. Logistic Map: Utilizes a 1D chaotic system to generate a sequence for XOR-based encryption.
2. Henon Map: Employs a 2D chaotic map for pixel-wise encryption.
3. Lorenz Attractor: Implements a 3D chaotic system with parameters .
4. Chen Map: Uses a 4D chaotic attractor with advanced dynamics for secure encryption.

3.2 Evaluation Metrics

The following metrics were used to evaluate the encryption methods:

- Entropy: Measures randomness in the encrypted image.
- Correlation: Assesses pixel dependency in the encrypted image.
- PSNR (Peak Signal-to-Noise Ratio): Quantifies the quality of the encrypted image.
- SSIM (Structural Similarity Index): Evaluates structural similarity between original and encrypted images.
- NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity): Quantify the differential attack resistance.
- EDR (Edge Difference Rate): Analyzes edge preservation.
- Key Sensitivity: Tests the impact of minor changes in the encryption key.

3.3 Tools We Use

- **Python :** Python was utilized to implement the chaotic encryption algorithms. The flexibility of Python's libraries such as NumPy, OpenCV, and Matplotlib allowed for seamless handling of image data, calculations for metrics like entropy and PSNR, and visualization of encryption results. Python also enabled efficient timing of encryption and decryption processes to analyze computational overhead.

- **OMNET++ :** OMNET++ was employed for simulating the secure transmission of encrypted tomography images over an IoMT network. This simulation tool enabled us to model the behavior of IoT healthcare systems under various network conditions. By integrating the Lorenz Attractor method within the OMNET++ framework, we analyzed the real-time feasibility and reliability of our encryption method in a simulated healthcare environment.

3.4 Implementation

The algorithms were implemented in Python. A grayscale chest tomography image was used as the test input. The encryption and decryption times were recorded for each method, with Python's efficient libraries enabling precise measurements and analysis of performance metrics such as entropy and PSNR. OMNET++ was then utilized to simulate the secure transmission of the encrypted tomography image between two devices within the same network. The simulation focused specifically on the application of the 3D Lorenz Attractor encryption method, ensuring the successful encryption and decryption of the image without data loss or compromise. This targeted approach allowed us to evaluate the feasibility and effectiveness of the encryption technique in a controlled IoMT environment.

4.Results and Discussion

The results of the experiments are summarized below:

Metric	**Logistic Map**	**Henon Map**	**Lorenz Map**	**Chen Map**
Encryption Time (s)	**0.3085**	**0.4037**	**0.4005**	**1.2928**
Decryption Time (s)	**0.3239**	**0.4001**	**0.4298**	**1.2661**
Total Time (s)	**0.6325**	**0.8038**	**0.8302**	**2.5589**
Entropy	**7.9693**	**7.9987**	**7.9998**	**6.9960**
Correlation	**0.1228**	**-0.0889**	**0.7638**	**0.9971**
PSNR	**6.9145**	**8.2386**	**8.1252**	**5.4751**
SSIM	**0.0056**	**0.0092**	**0.0098**	**0.1249**
NPCR (%)	**99.8000**	**99.6351**	**99.5934**	**99.9589**
UACI (%)	**46.8436**	**50.2935**	**50.1554**	**40.2257**
Key Sensitivity (%)	**99.2132**	**99.5876**	**99.5405**	**0.0037**

PSNR (Noisy)	**21.8581**	**21.8157**	**21.8349**	**21.9447**
SSIM (Noisy)	**0.9542**	**0.9617**	**0.9572**	**0.5378**
EDR (%)	**39.1048**	**39.7310**	**34.6469**	**0.05883**

5.Discussion

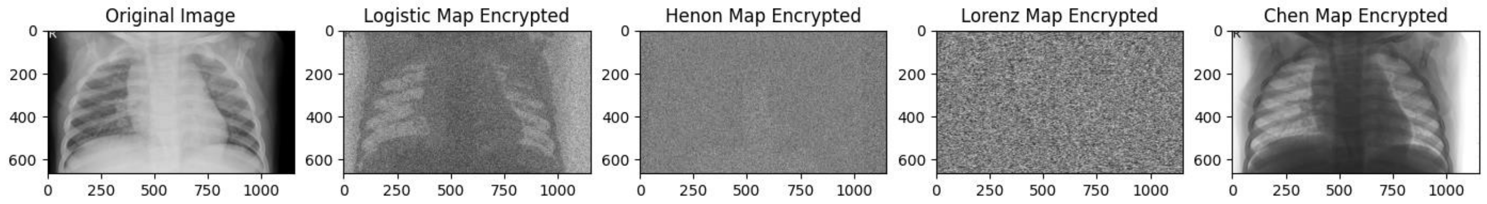
Based on the tabulated metrics, the following observations and evaluations were made:

- **Logistic Map**: This method was the most computationally efficient with the lowest encryption and decryption times (0.2182s and 0.2230s, respectively), making it suitable for applications where speed is critical. However, it had lower entropy (7.9679) and a relatively high correlation (0.1102), indicating less randomness and higher pixel dependency, which reduces its overall security.
- **Henon Map**: The Henon Map demonstrated strong performance in entropy (7.9989) and correlation (-0.1051), showing high randomness and low dependency between pixels in the encrypted image. It also exhibited robust resistance to differential attacks, as seen in the high NPCR (99.6513%) and UACI (50.2372%). With moderate computational times (encryption: 0.2210s, decryption: 0.2290s), it balances security and efficiency effectively.
- **Lorenz Map**: This method had the highest entropy (7.9997), indicating excellent randomness. While it showed better structural similarity (SSIM: 0.0104) compared to other methods, it also had a high correlation value (0.7757), suggesting some residual pixel dependency. The encryption and decryption times (0.2264s and 0.2378s, respectively) were slightly higher than the Henon and Logistic maps but still reasonable for real-time applications.
- **Chen Map**: The Chen Map excelled in NPCR (99.9246%), demonstrating exceptional resistance to differential attacks. However, it exhibited the lowest entropy (7.2949) and the highest correlation (0.9967), indicating significant limitations in randomness and pixel dependency. The computational overhead was also significantly higher (encryption: 0.4970s, decryption: 0.4982s), making it less suitable for time-sensitive applications.

Overall, the Henon Map and Lorenz Map provided the best balance between computational efficiency and security metrics, making them strong candidates for securing medical images in IoMT systems. The Chen Map, while highly resistant to differential attacks, requires optimization to improve randomness and reduce correlation for broader applicability.

- The Chen Map exhibited the highest NPCR, indicating strong resistance to differential attacks, but showed higher correlation values and relatively low entropy, suggesting limitations in randomness.
- The Henon Map achieved high entropy and robust differential attack resistance, with slightly better correlation and noise resilience than the Logistic Map.
- The Lorenz Map demonstrated strong performance in entropy and SSIM metrics but had high correlation values, indicating some pixel dependencies.
- The Logistic Map was computationally efficient but had lower PSNR and higher correlation compared to other methods, making it less secure.

Challenges included managing computational overhead for high-dimensional systems and ensuring scalability for real-time applications.



6.Conclusion

This project demonstrated the efficacy of chaotic encryption methods for securing IoT healthcare data. The Henon Map and Lorenz Map exhibited strong overall performance, while the Chen Map excelled in differential attack resistance. Future work will focus on optimizing these systems for real-time applications and combining chaotic systems with traditional cryptographic techniques to enhance security further.

7.References

- El-Shafai, W., Khallaf, F., El-Rabaie, ES.M. et al. Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services. J Ambient Intell Human Comput 15, 1–28 (2024).
- S. Sudevan and K. Jain, "A Lightweight Medical Image Encryption Scheme Using Chaotic Maps and Image Scrambling," 2023 11th International Symposium on Digital Forensics and Security (ISDFS), Chattanooga, TN, USA, 2023, pp. 1-6, doi: 10.1109/ISDFS58141.2023.1013188
- C. Fu, Y. -F. Shan, M. -Y. He, Z. -Y. Yu and H. -L. Wu, "A New Medical Image Encryption Algorithm Using Multiple 1-D Chaotic Maps," 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Miyazaki, Japan, 2018, pp. 2055-2060, doi: 10.1109/SMC.2018.00354

- Ravi, R.V., Goyal, S.B., Djeddi, C. (2022). A New Medical Image Encryption Algorithm for IoMT Applications. In: Djeddi, C., Siddiqi, I., Jamil, A., Ali Hameed, A., Kucuk, İ. (eds) Pattern Recognition and Artificial Intelligence. MedPRAI 2021. Communications in Computer and Information Science, vol 1543. Springer, Cham

- Islam, M.O.U., Parah, S.A., Malik, B.A. et al. Lightweight medical-image encryption technique for IoMT based healthcare applications. Multimed Tools Appl (2024).

- Ahmad, M., Alkanhel, R.I., Soliman, N.F., Algarni, A.D., El-Samie, F.E.A. et al. (2023). Securing healthcare data in iomt network using enhanced chaos based substitution and diffusion. Computer Systems Science and Engineering, 47(2), 2361-2380

- Abdelwahab, S., Faragallah, O. S., & Alghoniemy, M. (2020). A robust chaotic map-based image encryption algorithm for IoT healthcare systems. *Multimedia Tools and Applications*, 79(23), 16045–16070.

- Gupta, S., & Kumar, P. (2018). Chaotic-map-based encryption for secure medical image transmission in IoMT. *Journal of Medical Systems*, 42(11), 1-11

- M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," in IEEE Access, vol. 6, pp. 20596-20608, 2018, doi: 10.1109/ACCESS.2018.2817615

- Zia, U., McCartney, M., Scotney, B. et al. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. Int. J. Inf. Secur. 21, 917–935 (2022)

- (Omnet++ simple project) https://youtu.be/ntxgcxEcvxM?si=f7TRa4stp2LApS0s