Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 45 No. 6
June 2025

Secure Medical Image Encryption Using Modified Logistic Map

Amutha R[1]

[1]Department of Electronics and Communication Engineering, Sri Siva Subramiya Nadar College of Engineering,Chennai, Tamil Nadu, India. Email: amuthar@ssn.edu.in

Abstract

Secure transmission of medical images ensures that sensitive patient data, namely X-rays, or CT scans, is protected during transfer between healthcare providers. This process often involves encryption techniques to prevent unauthorized access and ensure confidentiality. This work presents a chaos based medical image encryption algorithm. Permutation and diffusion are the two main component of any encryption technique. In this work, permutation is carried out using the sequence produced by the modified map. To improve the security two levels of diffusion namely row diffusion and column diffusion is carried out. The performance of the proposed algorithm is verified using the various metrices like entropy, Histogram analysis, NPCR, UACI, Chi square value, key space etc. Simulation results show that the proposed algorithm is resistant to various attacks.

1. Introduction

Secure transmission is critical to maintaining patient privacy. It helps to maintain the integrity of sensitive data, ensuring they are not altered or corrupted during transmission. Secure transmission of medical data ensures that sensitive patient data, namely MRIs, or CT scans, is protected during transfer between healthcare providers. This process often involves encryption techniques to prevent unauthorized access and ensure confidentiality. Zargaran et al [1] discusses the ethical concerns surrounding the use of smartphones for medical image sharing. It emphasizes the risks of patient privacy breaches, inadequate security measures, and the need for proper guidelines in medical practice. The authors advocate for clear ethical frameworks to ensure secure and responsible use of smartphones in healthcare settings. Stalin, S et al [2] developed a medical image encryption using a combination of a nonlinear 4D logistic map and DNA sequences. It is proved through the simulation that the proposed method enhances the encryption speed and security. Chen, J et al [3] proposed a medical image encryption method by combining hierarchical diffusion and non-sequential encryption techniques. Because of complex, non-linear transformations decryption is not possible without the proper key. Ashwini, K et al [4] developed a compressive sensing based medical encryption and proposed a 1-D chaotic map. Through simulations the authors demonstrated that the method has reduced image size and strong encryption capabilities and high image quality.Li, J et al [5] proposed a partial encryption algorithm for medical images that combines quick response (QR) codes with reversible data hiding technology. This method encrypts only relevant parts of the medical images while preserving the remaining information. Authors have demonstrated the algorithm's ability to protect sensitive information while allowing for efficient data retrieval and image reconstruction.

Zhang, Y. L et al [6] proposed an encryption method for medical data using blockchain technology. Uddin, M et al [7] The paper introduced a DNA-based key scrambling method for encryption.Barik, R. C., & Changder, S. [8] proposed a medical encryption technique that combines multiple chaotic maps with an amino acid codon-based approach. This method enhances security by employing complex, non-linear transformations and coding techniques.

Pankaj, S., & Dua, M. [9] introduced a novel medical image encryption technique that combines a ToCC map with a two-level scrambling approach. This method enhances the security of medical images by using multiple layers of encryption, making it more resistant to unauthorized access. Stanley, H., & Amutha R [10] proposed an extended logistic map and an encryption method using a proposed map. Hong-Wei, X et al [11] proposed a color medical image encryption method that integrates image segmentation with a fractional-order hyperchaotic system. This approach enhances encryption by first segmenting the image into parts and then applying a complex chaotic system for encryption, providing

robust security. Kasim, Ö. [12] developed a secure medical image encryption method that combines the Walsh-Hadamard transform with a lightweight cryptography algorithm. Liu, Z., & Xue, R. [13], developed a medical image encryption method by integrating the biometric features with medical image data. It is demonstrated through simulations that this method achieves improved security and accuracy in medical image protection.

Dua, S et al [14] developed medical image encryption method called ICFCM-MIE. The author used a cosine fractional chaotic map and fractional-order dynamics to obscure medical data. Man, Z et al [15] proposed a rotation-based medical encryption technique utilizing a Lorenz chaos system. They introduced dynamic rotation and chaotic transformations to obscure image data, and hence the decryption without the proper key is not possible. Ali, J et al [16] introduced a fractional transformation-based S-box for image encryption. aiming to improve both security and encryption efficiency. Complexity and unpredictability of the encryption is improved by utilizing fractional transformations in the S-box. Shahid, U et al [17] developed a blockchain-driven medical image encryption technique that uses a chaotic tent map in cloud computing environments. This method integrates blockchain for authentication and chaotic encryption for data protection.

2. Bifurcation Analysis

A. Chaotic Map

A logistic map is a mathematical function represented by (1) which is chaotic from 3.57 to 4.

$$X_{n+1} = \mu X_n (1 - X_n) \quad (1)$$

Logistic map is modified to widen the chaotic region from 0 – 100. The modified map is represented by (2).

$$X_{n+1} = \left(abs\left(\mu * \left(1 - \frac{\mu}{X_n}\right)(1 - \mu^2) \right) \right) \quad (2)$$

The bifurcation plot of the logistic and modified map is depicted in Fig. 1. From the Fig. 1 it is clear that the chaotic range is larger for the modified map.

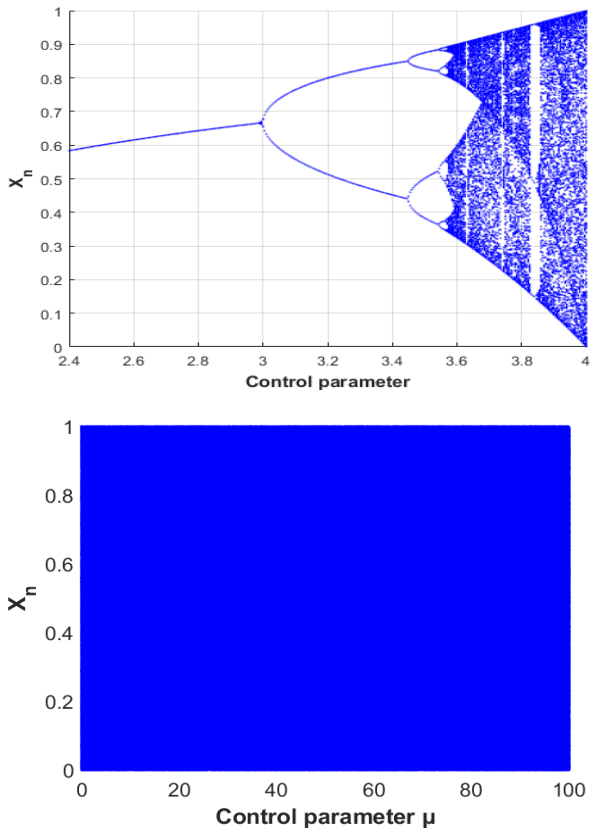


Fig. 1. Bifurcation plot of (a) Logistic (b) Modified Map

3. Methodology

Block diagram of the proposed method for the encryption of medical image is depicted in Fig. 2. The steps involved in the encryption process are listed below.

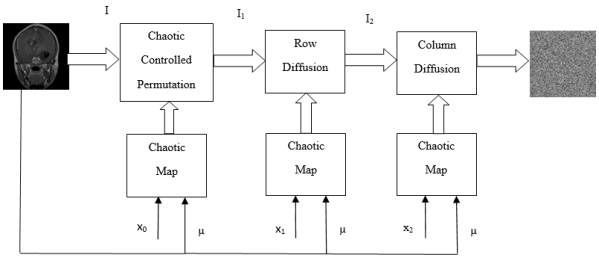


Fig. 2. Block diagram of the image encryption method

Step 1: Mean of the image I of size $M * N$ is computed. A sequence of size $M * N$ is generated using the (3) with the computed mean as the control parameter and $X_{01} = 0.5542$.

$$Mean1 = mod(floor(mean), 100) \quad (3)$$

Step 2: Sequence is arranged in ascending order and the index sequence q_1 is generated.

Step 3: Permutation of the image is carried out using the index sequence q_1. Output of the permutation is I_1.

Step 4. A sequence q_2 of size $M * N$ is generated using the modified map with the computed mean as the control parameter and $X_{02} = 0.6382$. The sequence is quantized using (4) and the quantized sequence is used for row diffusion. The output of the row diffusion is I_2.

$$t_1 = (mod(floor(q_2 x 10^4)), 256) \quad (4)$$

$$I_2 = \begin{cases} t_1 \oplus I_1(i) & i=1 \\ I_2(i-1) \oplus I_1(i) & i=2,3,....M \end{cases} \quad (5)$$

Step 5: The same procedure is repeated for column diffusion with the $X_{02} = 0.7254$. The output of the column diffusion is the cipher image.

$$t_1 = \left(mod(floor(q_2 x 10^4)), 256\right) \quad (6)$$

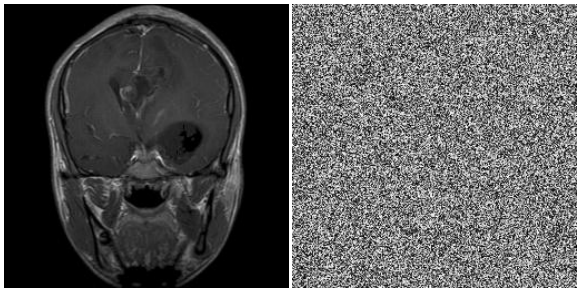
$$C = \begin{cases} t_2 \oplus I_2(i) & i=1 \\ C_{(i-1)} \oplus I_2(i) & i=2,3,...N \end{cases} \quad (7)$$

4. Simulation Results

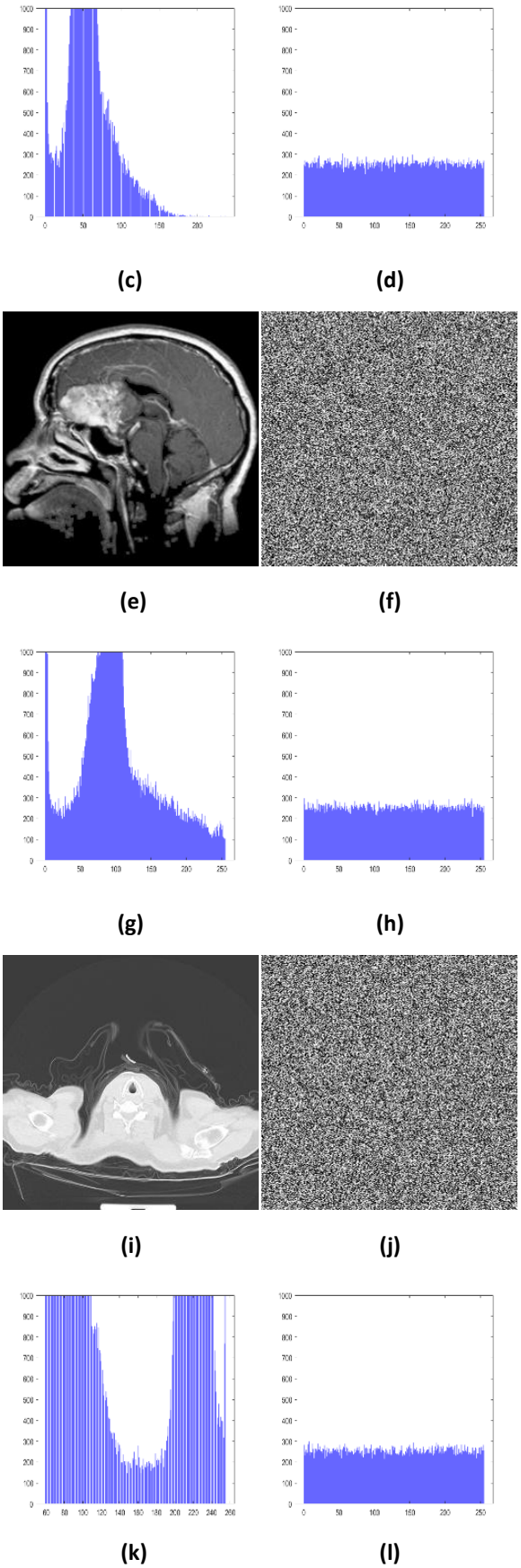
The performance of the proposed method is verified using differential attack analysis, statistical analysis, key space analysis etc. Two brain images and one lung image are used for simulation. The images are taken from https://wiki.cancerimagingarchive.net/pages/viewpage.action?pageId=70224216 and Kaggle.

A. Histogram Analysis

Histogram plot represent the distribution of pixel intensities of an image. The histogram of the brain and lung images and their cipher are shown in Fig. 3. Since the Histogram plot is there no leak of information. Hence it withstands statistical attacks.



(a) (b)



(c) (d)

(e) (f)

(g) (h)

(i) (j)

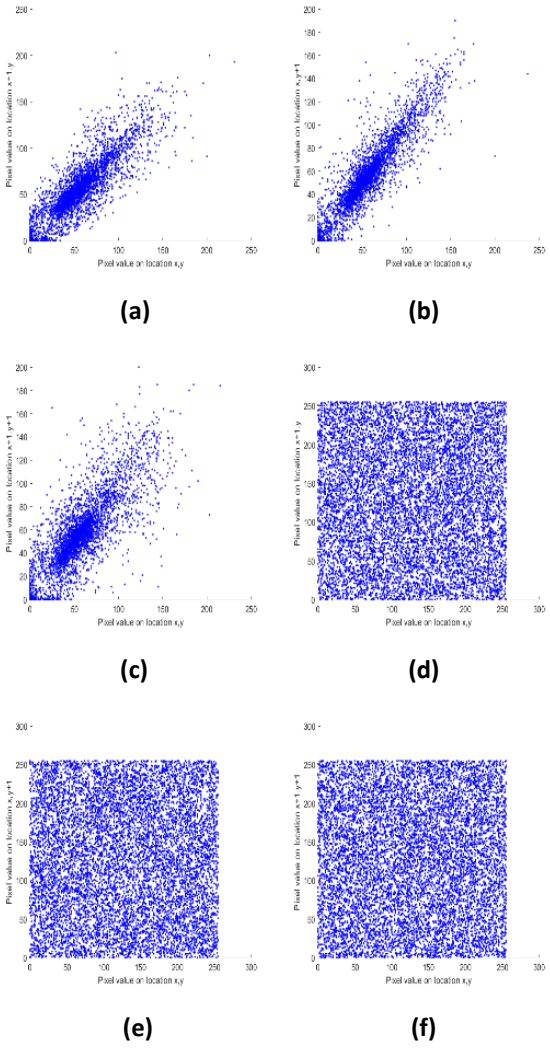
(k) (l)

Fig. 3. Plain Image (a) BrainG125 (e) BrainG1 (i) Lung, Cipher Image (b) BrainG125 (f) BrainG1 (j) Lung,

Histogram (c) BrainG125 (g) BrainG1 (k) Lung, Cipher Histogram (d) BrainG125 (h) BrainG1 (l) Lung

B. Correlation Analysis

It is used to measure the relation between neighboring pixels in an image. Fig. 4 depicts the correlation plot of the brain and its cipher in horizontal, vertical and diagonal directions. From Fig. 4 (a-c) it is clear that the neighboring pixels in the brain image in all three directions are highly correlated. It is evident from Fig 4 (d-f), that the neighboring pixels in the cipher image in all three directions are not correlated.



(a) **(b)** **(c)** **(d)** **(e)** **(f)**

Fig. 4. Pixel correlation plot of test image BrainG_125: a) horizontal, b) vertical, c) diagonal. Pixel correlation plot of cipher image BrainG125: d) horizontal, e) vertical, f) diagonal

The correlation coefficient between the brain and its cipher image is computed and listed in Table I. The coefficient value is very low and is close to zero in all three directions.

Table I. Correlation Analysis

Test Image256x256	Direction	Plain Image	Cipher Image
BrainG_125	Horizontal	0.9500	-0.0033
	Vertical	0.9658	-0.0114
	Diagonal	0.9235	-0.0026

C. Entropy Analysis

The entropy is used to measure the randomness. The entropy of the three cipher images is calculated using (9) and shown in Table II. The entropy value is close to the theoretical value 8.

$$H(S) = \sum_{i=0}^{255} p(S_i) log_2 \frac{1}{p(S_i)} \quad (8)$$

Table II. Entropy Analysis

Test Image256x256	Proposed
BrainG_125	7.9
BrainG_1	7.9
Lung_00	7.9003

D. Chi-Square Test

Chi square measures the uniform distribution of the pixel values. Smaller values (less than 249) of χ^2 represents flatter histogram. The χ^2 values for different medical images are computed using (7) and tabulated in Table III.

Table III.Chi-Square Test

Test Image256x256	Proposed
BrainG_125	247.125
BrainG_1	225.5781
Lung_00	232.2734

E. Differential Attack Analysis

Robustness against differential attacks is verified by computing Number of pixel change rate (NPCR) and Unified average change intensity (UACI). UACI and NPCR values are calculated using the equations (10) and (11) respectively and tabulated in Table IV.

$$UACI = \frac{1}{M*N} \frac{\sum_{j,k} |V_1(j,k) - V_2(j,k)|}{255} * 100\% \quad (9)$$

$$NPCR = \frac{1}{M*N} \sum_{j,k} K(j,k) * 100\% \quad (10)$$

where $K(j,k) = \begin{cases} 0, V_1(j,k) = V_2(j,k) \\ 1, V_1(j,k) \neq V_2(j,k) \end{cases}$

Table IV. NPCR and UACI Analysis

Test Image256x256	NPCR in %	UACI in %
BrainG_125	99.6154	33.4145
BrainG_1	99.6337	33.4355
Lung_00	99.6170	33.5279

F. Key Space Analysis

The proposed method uses three chaotic sequences with 16-digit precision for both control and initial value. The mean of the image is used as the control parameter for all the three chaotic sequences. The minimum key space required to avoid the brute force attack is 10^{32} . Key space of our algorithm is greater [19] and less than [18] and greater than the minimum key space.

$10^{16} * 10^{16} * 10^{16} * 10^{16} = 10^{64} \approx 2^{212}$

Table V.Key Space Analysis

Proposed Method	[18]	[19]
2^{212}	2^{260}	2^{128}

5. Conclusion

Chaos based medical image encryption algorithm is proposed for secure transmission of medical images like X-ray, CT scan etc. The performance of the proposed algorithm is verified through simulations. From the simulation results it is clear that the proposed method is resistant to statistical attacks. The key space of the proposed algorithm is very high and hence it is resistance against brute force attacks.

References

[1] Zargaran, J. Ash, G. Kerry, D. Rasasingam, S. Gokani, A. Mittal, and D. Zargaran, "Ethics of smartphone usage for medical image sharing," *Indian Journal of Surgery*, vol. 80, pp. 300-301, 2018.

[2] S. Stalin, P. Maheshwary, P. K. Shukla, M. Maheshwari, B. Gour, and A. Khare, "Fast and secure medical image encryption based on non linear 4D logistic map and DNA sequences (NL4DLM_DNA)," *Journal of Medical Systems*, vol. 43, pp. 1-17, 2019.

[3] J. Chen, L. Chen, L. Y. Zhang, and Z. L. Zhu, "Medical image cipher using hierarchical diffusion and non-sequential encryption," *Nonlinear Dynamics*, vol. 96, pp. 301-322, 2019.

[4] K. Ashwini, R. Amutha, R. R. Immaculate, and P. Anusha, "Compressive sensing based medical image compression and encryption using proposed 1-D chaotic map," in *Proc. 2019 Int. Conf. Wireless Commun. Signal Process. Netw. (WiSPNET)*, 2019, pp. 435-439.

[5] J. Li, Z. Zhang, S. Li, R. Benton, Y. Huang, M. V. Kasukurthi, and J. Huang, "A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology," *BMC Medical Informatics and Decision Making*, vol. 20, pp. 1-16, 2020.

[6] Y. L. Zhang, L. Wen, Y. J. Zhang, and C. F. Wang, "Deniably authenticated searchable encryption scheme based on Blockchain for medical image data sharing," *Multimedia Tools and Applications*, vol. 79, no. 37, pp. 27075-27090, 2020.

[7] M. Uddin, F. Jahan, M. K. Islam, and M. R. Hassan, "A novel DNA-based key scrambling technique for image encryption," *Complex & Intelligent Systems*, vol. 7, pp. 3241-3258, 2021.

[8] R. C. Barik and S. Changder, "A novel and efficient amino acid codon based medical image encryption scheme colligating multiple chaotic maps," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10723-10760, 2021.

[9] S. Pankaj and M. Dua, "A novel ToCC map and two-level scrambling-based medical image encryption technique," *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 10, no. 1, p. 48, 2021.

[10] H. Stanley and A. Ramachandran, "Extended logistic map for encryption of digital images," *International Journal of Nonlinear Sciences and Numerical Simulation*, vol. 23, no. 7-8, pp. 985-1000, 2022.

[11] H.-W. Xie, Y.-Z. Zhang, Z.-Y. Li, and H. Zhou, "Color medical image cryptography technology based on segmentation and fractional-order hyperchaotic system," *Medical & Biological Engineering & Computing*, vol. 61, no. 1, pp. 109-127, 2023.

[12] Ö. Kasim, "Secure medical image encryption with Walsh–Hadamard transform and lightweight cryptography algorithm," *Medical & Biological*

Engineering & Computing, vol. 60, no. 6, pp. 1585-1594, 2022.

[13] Z. Liu and R. Xue, "Medical image encryption using biometric image texture fusion," *Journal of Medical Systems*, vol. 47, no. 1, p. 112, 2023.

[14] S. Dua, A. Kumar, M. Dua, and D. Dhingra, "ICFCM-MIE: improved cosine fractional chaotic map based medical image encryption," *Multimedia Tools and Applications*, vol. 83, no. 17, pp. 52035-52060, 2024.

[15] Z. Man, C. Gao, Y. Dai, and X. Meng, "Dynamic rotation medical image encryption scheme based on improved Lorenz chaos," *Nonlinear Dynamics*, vol. 112, no. 15, pp. 13571-13597, 2024.

[16] J. Ali, M. K. Jamil, and R. Ali, "Extended fractional transformation based S-box and applications in medical image encryption," *Multimedia Tools and Applications*, pp. 1-17, 2025.

[17] U. Shahid, S. Kanwal, M. Bano, S. Inam, M. E. M. Abdalla, and Z. A. Shaikh, "Blockchain driven medical image encryption employing chaotic tent map in cloud computing," *Scientific Reports*, vol. 15, no. 1, p. 6236, 2025.

[18] Y. Luo, S. Tang, J. Liu, L. Cao, and S. Qiu, "Image encryption scheme by combining the hyper-chaotic system with quantum coding," *Optics and Lasers in Engineering*, vol. 124, p. 105836, Jan. 2020, doi: 10.1016/j.optlaseng.2019.105836.

[19] P. Alli and J. D. Peter, "A novel auto-encoder induced chaos based image encryption framework aiding DNA computing sequence," *Journal of Intelligent & Fuzzy Systems*, vol. 41, no. 1, pp. 181-198, Aug. 2021, doi: 10.3233/JIFS-201224.