

A novel image cryptosystem for biomedical images and secured storage by randomized chaotic encryption scheme

K Paramesha¹, Karthik V^{2*}, Prashanth M V³, Sathisha M S⁴, Bhargav H K⁵, Ranjan Kumar H S⁶, Raju K⁷, Kiran Puttegowda⁸

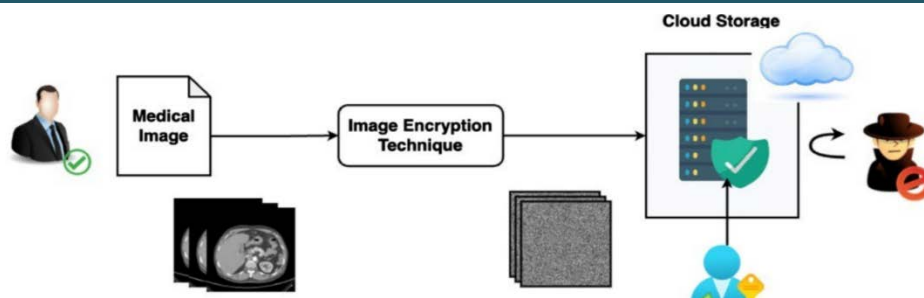
¹Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India. ²Department of Information Technology, Manipal Institute of Technology, Bengaluru, Manipal Academy of Higher Education, Manipal, India. ³Department of Information Science Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India. ⁴Department of Artificial Intelligence and Machine Learning, Navkis College of Engineering, Hassan, Karnataka, India. ⁵Department of Computer Science and Engineering, Shridevi Institute of Engineering and Technology, Tumakuru, Karnataka, India. ⁶Department of Artificial Intelligence and Data Science, Shri Madhwa Vadiraja Institute of Technology and Management Bantakal, Udupi, Karnataka, India. ⁷Department of Computer Science and Engineering, NMAM Institute of Technology (NMAMIT), NITTE (Deemed to be University), Nitte, Karnataka, India. ⁸Department of Electronics and Communication Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India.

Submitted on: 27-Aug-2024, Accepted and Published on: 14-Feb-2025

Article

ABSTRACT

Medical images transfer sensitive elements about diagnosis along with patient information across public networks between doctors and hospitals and patients. Secure storage and transmission methods must be implemented for image protection which addresses patient privacy. The proposed system introduces an elaborate image encryption method that uses chaotic and rotational systems for performing inter-block shuffling operations. A 2D sine map system with random behavior allows the algorithm to transform target images by performing scaling and rotational transformations and randomly reshuffling arrays. The chaotic system applies scaling and rotation operations as its first step before processing the medical image to reduce pixel dependencies. Permutation of the image produces an encrypted file through the S-box which applies a diffusion operation to the rearranged data. A chaotic system generates both unpredictability and sensitive initial condition reactions that produces a large key space that makes brute-force attacks less successful. Real-time operations are possible because the algorithm operates with fast data processing while using minimal resources. Evaluation results show that grayscale medical images perform better under security tests as the NPCR and UACI value reached above 98.53% and 34.33% throughout the testing phase.



Keywords: 2D sine map, Rotation, Medical Image, Security, Encryption

INTRODUCTION

Healthcare systems today rely intensely on medical image transmission and storage because these procedures both bolster clinical decisions and enable the operation of telemedicine along with EHRs. Patient data from MRI and CT scans and X-ray imaging

technologies produces overwhelming volumes that need advanced security systems to protect against unlawful data access and modification and breaches. A rising number of healthcare system cyber-attacks requires medical pictures to implement robust security solutions because medical image protection integrity and accessibility remain vital operational requirements. Medical procedures that require speed encounter problems with delays because standard encryption makes data secure even though it leads to time-consuming processing.

Data encryption follows a conventional process that treats data as binary digits before subjecting them to cryptographic algorithms like DES or AES for encryption purposes. Secure general data

*Corresponding Author: Karthik V, Department of Information Technology, Manipal Institute of Technology, Bengaluru, Manipal Academy of Higher Education, Manipal, India. Email: v.karthik@manipal.edu

Cite as: J. Integr. Sci. Technol., 2025, 13(5), 1103.
URN:NBN:sciencein.jist.2025.v13.1103
DOI:10.62110/sciencein.jist.2025.v13.1103



©Authors CC4-NC-ND, ScienceIN <https://pubs.thesciencein.org/jist>

through mathematical operations applied to binary data inputs for achieving confidentiality and integrity protection. The encryption of digital images stands different from other data types especially when the images use high-resolution formats that frequently occur in medical diagnostics. Data that exists as images demonstrates properties which separate it from generic text or binary information. Image data contains two default characteristics such as high redundancy and pixel correlation. The patterns between adjacent pixels tend to match since their color and intensity values remain closely related. The large size of images creates an obstacle for traditional encryption methods as they fail to achieve effective or efficient results during processing of extensive datasets.¹

Image encryption using substitution ciphers fails to achieve adequate security because its results prove insufficient. The application of substitution cipher encryption only alters the color space of images without entirely obscuring their original visual appearance. The shift in data does not lead to substantial data confusion or diffusion because these aspects form critical components of cryptography to prevent recognizable encryption. An opponent who understands the encryption procedure can decrypt or understand the original image even lacking access to the decryption key. Traditional encryption methods prove ineffective in safeguarding image data because they do not effectively hide what lies beneath the surface according to studies.²

Medical image encoding functions lack sufficient security protection according to present encryption regulations. Medical images bypass traditional encryption because they possess several characteristics that consist of repetitive pixel patterns related to picture memory combined with extensive file sizes. A successful encryption method must safeguard medical images at the same time preserve efficient resource handling from storage to transmission. The research field calls for immediate work on a contemporary encryption system which resolves security risks along with technical problems to achieve swift high-level protection against current threats.

The proposed article introduces a novel image encryption algorithm designed specifically to address the security challenges of medical images. The key contributions of this work include:

- A new encryption approach using chaotic and rotational system methods presents itself in this paper as an answer to medical image encryption problems.
- The algorithm performs image transformation tasks through chaotic 2D sine map systems which demonstrate unpredictable behaviour to apply medical image scaling rotation and randomization thus reducing pixel correlation while strengthening encryption techniques.
- A large key space emerges from the chaotic system because of its unpredictability and sensitivity to initial conditions which leads to better protection against brute-force attacks and enhances total encrypted image security.
- The S-box diffusion operation enables an encrypted image to become more challenging to decipher because it creates sophisticated relationships between original and encrypted information.

The proposed encryption method shows suitable performance for real-time applications since it operates quickly with large medical image files and requires minimal computational effort..

LITERATURE SURVEY

K. N. Bharath et al.³ developed work that applies region-based lossless image compression instead of encryption methods. Medical image compression optimization under this method utilizes specific region-based techniques but adds no new encryption processes compared to normal methods. Medical image encryption as described by Muhammad Fahad Khan et al.⁴ utilizes region-based encryption methods for DICOM images that safeguard essential parts while achieving faster encryption rates and complete privacy security during healthcare information transmission. B Suvitha, D. Murugan et al.⁵ introduced research about applying homomorphic encryption together with deep learning methods to protect medical image transmission during real-time telemedicine examinations to achieve enhanced system efficiency and encrypted image quality security features. Through pixel thresholding Qamar Natsheh et al.⁶ developed a selective encryption system to protect DICOM images by automatically choosing regions for encryption which used encryption algorithms based on specific importance levels. Rong-Yuan Chen et al.⁷ created an image encryption system with dual protection capabilities that protects full images as well as region of interest (ROI) through integrated cascade chaos and an optimized Joseph traversal method. Abhishek et al.⁸ developed an encryption algorithm that protects crucial medical images from end to end to provide secure protection of sensitive medical network information. L. Salman et al.⁹ introduces a region of interest (ROI) specific image encryption system for medical imaging which uses chaos maps and polynomial-based secret image sharing methods to achieve improved healthcare system security and reduced transmission costs. Bing Zhang et al.¹⁰ developed a plain-image correlative semi-selective medical image encryption scheme which fully protects region of interest but only applies partial encryption to background areas to overcome medical image transmission speed and security limitations of current selective encryption approaches. Xin Meng et al.¹¹ presents a medical DICOM image encryption framework that uses chaotic systems to generate keystreams and adds a combination of scrambling and bi-directional diffusion steps to improve healthcare transmission security. Kiran P et al.¹² developed an advanced encryption process for medical images through the combination of Laplacian edge detection with Arnold cat map and Duffing system encryption to simultaneously protect data and minimize transmission costs in healthcare environments. Xing Qing Wang et al.¹³ developed an encryption scheme that protects medical image ROI data to reduce vulnerability to chosen plaintext attacks. The algorithm achieves secure medical image transmission through pixel swapping and diffusion methods that use chaotic sequences for encryption. The study of Amaithi et al.¹⁴ focuses on secure medical image transmission using homomorphic encryption where key generation utilizes ResNet50 for cryptographic functions. The system protects database security by safeguarding private patient information and maintaining data integrity although it lacks specific solutions for regional selective

encryption. S. A medical image encryption protocol based on the use of hyperbolic chaotic systems with bit-shifting-flipping methods achieves improved security levels according to Rajendran et al.¹⁵. The system works efficiently based on security analysis outcomes demonstrating attack resistance and key sensitivity through statistical methods. A secure medical image transfer system was developed by Sahay et al.¹⁶ through splitting images into Region of Interest (ROI) and Not-a-Region of Interest (NROI) parts. The system maintains the preservation of ROI features along with watermarking methods that embed patient data along with secret keys in NROI sections. The combined application of SCAN and chaotic-map technology developed by Kiran P et al.¹⁷ provides healthcare platforms with better system availability and confidentiality and integrity throughout medical image transmission. Yiru Wu et al.¹⁸ created a DNA computing system that utilizes random identification strategies together with spatial pattern modification to protect complete medical image data. Losing data integrity through lossless encryption techniques during medical image security only operates on specific areas. Renuka Devi P et al.¹⁹ explained lossy compression techniques outside of this region for cost-effective security implementations. The security solution by Jamal et al.²⁰ embeds protected medical data within predefined Region of Interest areas. The method provides improved privacy and data integrity throughout communication by solving established encryption as well as watermarking obstacles which affect real-time processes. Sudheesh et al explained block-based partial image encryption technique with the help of Henon Map. In this work, randomly select and encrypt image blocks based on specified encryption requirements.²¹ K Prabhavathi et al explained An efficient homomorphic encryption algorithm for medical images ensures the protection of medical plaintext data against unauthorized access while preserving data confidentiality and enabling secure computations²². Mohit Dua et al proposed one-dimensional STC map, combined with a shared key develop a permutation-based medical image encryption scheme²³. Saba Inam proposed that securing sensitive patient data in the Internet of Medical Things (IoMT) requires encryption to maintain confidentiality, prevent tampering, ensure authenticity, and protect data transmission.²⁴ Prabhavathi et al. proposed a region-based medical image encryption method that utilizes a 2D Logistic Sine Map (2DLSM) combined with an advanced Zig-Zag transform to enhance the security of medical images.²⁵ Zezong Zhang et al proposed a medical image encryption algorithm that integrates Josephus scrambling and dynamic cross-diffusion techniques to enhance patient privacy protection.²⁶ Bofeng Long et al provides insights into deep learning-based medical image encryption and introduces a novel end-to-end encryption scheme that utilizes feature encoding and decoding for secure image encryption and decryption²⁷. 2D Sine MAP

The 2D sine map serves as a mathematical function that chaos theory along with nonlinear dynamics uses to depict time-based system progression. The map extends the 1D sine system¹⁵ by applying two-dimensional mapping instead of one. A standard 2D sine map appears in the form described below.

$$\begin{aligned} x_{i+1} &= \sin\left(\pi(4\theta x_i(1-x_i) + (1-a)\sin(\pi y_i))\right) \\ y_{i+1} &= \sin\left(\pi(4\theta y_i(1-y_i) + (1-b)\sin(\pi x_{i+1}))\right) \end{aligned} \quad (1)$$

Where θ is the control parameter and $\theta \in [0, 1]$. The system dynamics function based on how a and b . The system will demonstrate different patterns of motion from periodic to chaotic patterns based on parameter adjustments. People often employ this system for both modelling simulations and fractal production and studying nonlinear systems behaviours. The Lyapunov exponent diagram of the Sine map as shown in figure 1.

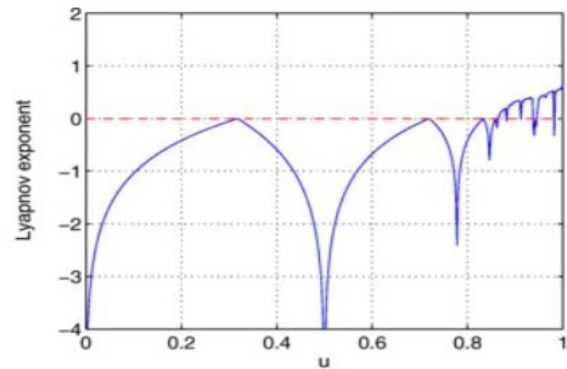


Figure 1. The Lyapunov exponent diagram of the Sine map.

PROPOSED METHODOLOGY

Figure 2 illustrates the block diagram of the proposed medical image encryption method, which consists of three main stages: segmentation, blockwise shuffling, and an S-box based diffusion process. The encryption process begins with the segmentation of the input medical image into 10 equal parts. The second phase starts with the generation of 10 random rotational angles through the utilization of a sine map. The fragmented image blocks receive individual rotations based on assigned random angles which creates the confused output. The diffusion process creates an S-box by applying the sine map to a secret key to produce the final stage of the algorithm. The encrypted medical image emerges from combining the S-box with both confused image data and randomly selected S-box pixel values through XOR operations. Security in medical images remains enhanced through encryption stages combining random structure confusions with pixel value diffusion processes. Sbox for the proposed work as shown in figure 3.

Performance evaluation

Security and effectiveness evaluations of the proposed encryption scheme depend on multiple statistical and mathematical tests applied to processed images. Research on image encryption relies on these tests to generate metrics which become standard references in academic publications. The researcher provides a detailed explanation before conducting an analysis of test outcomes which pertain to the proposed encryption system. The results are measured against those obtained from related studies to assess how the algorithm matches up with different encryption methods. The testing section utilized exclusively images from the Open-i database according to the specifications listed in Table 1.

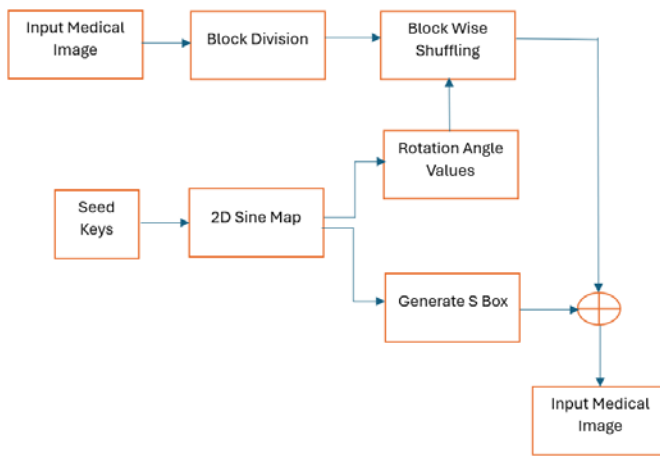
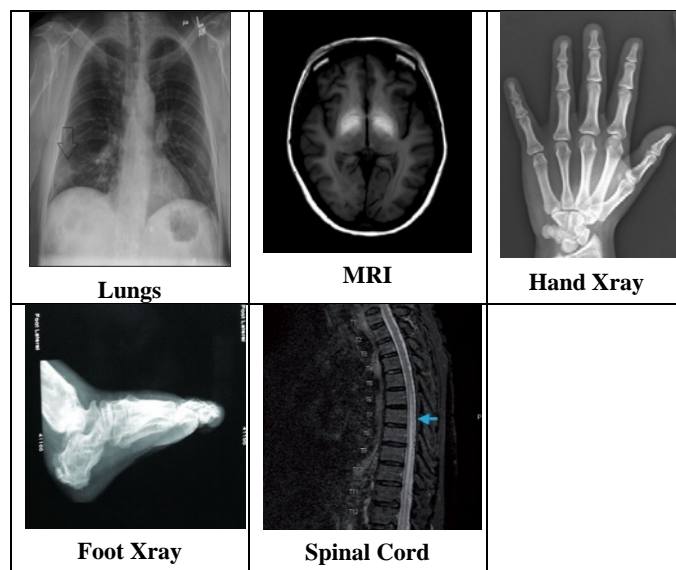


Figure 2. Proposed selective encryption scheme

74	164	153	189	80	104	89	76	65	119	245	156	224	32	38	255
108	20	106	162	235	184	115	187	211	190	42	8	213	117	70	29
96	203	113	13	241	75	175	217	69	166	126	174	139	178	4	146
71	238	212	31	90	88	250	128	173	105	35	131	137	82	230	52
122	44	118	232	236	199	21	234	141	85	121	191	144	221	53	168
143	73	163	0	186	98	112	161	40	155	92	33	95	208	145	169
100	34	152	124	127	6	41	240	109	204	248	215	177	94	3	226
225	147	157	222	254	39	185	206	67	209	242	218	2	140	60	183
167	79	62	202	114	252	28	11	46	200	48	59	220	5	26	87
101	24	23	251	172	64	36	9	49	150	14	216	247	129	132	99
228	160	77	103	47	171	229	176	93	219	86	149	165	58	253	83
195	110	78	205	27	107	54	134	182	111	18	239	51	16	19	136
210	133	207	22	188	120	123	227	158	72	125	7	181	179	233	43
15	196	102	249	63	116	68	130	81	198	30	66	194	12	244	148
50	170	237	197	138	37	246	214	55	45	57	142	61	17	84	154
243	151	1	223	231	25	91	10	135	201	193	180	159	192	56	97

Figure 3. Proposed 2D sine map-based S-box

Table 1. Datasets used for proposed work



A. Histogram analysis

A histogram displays pixel frequency distribution through a visual representation. The distribution of pixel frequencies in

securely encrypted images should appear as uniform throughout the histogram. The encryption method shows an equal pixel distribution which demonstrates its ability to shuffle data points and protect the image structure from potential attacker analysis.

B. Entropy Analysis

The quantification of image information unpredictability or randomness through entropy appears in¹². Higher entropy serves as a standard for evaluating encryption methods because it signifies better randomness and security.

$$H(S) = \sum_{i=0}^{2^M-1} P(si) \log_2 \frac{1}{P(si)} \quad (2)$$

Random images should exhibit an entropy value of 8 because this quantity indicates complete unpredictability. A low entropy value indicates reduced randomness in the image while increasing the odds of predicting its contents.

Mean Square Error

The Mean Squared Error (MSE) represents a standard calculation in image processing because it measures the average square value between plaintext images and their encrypted counterparts¹². The MSE evaluates image encryption success by using the following calculation:

$$MSE = \frac{1}{MXN} \sum_{i=1}^M \sum_{j=1}^N [X(i,j) - Y(i,j)]^2 \quad (3)$$

C. Number of Pixel Change Rate (NPCR)

The original image corresponds to C1 while its encrypted version stands as C2. Both C1(i, j) stand for original image pixels and C2(i, j) represent encrypted image pixels. The defined metric for NPCR¹³ (Number of Pixels Change Rate) is given by.:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MXN} \times 100\% \quad (4)$$

Where D is bipolar array.

$$D(i,j) = \begin{cases} 1, & C1(i,j) \neq C2(i,j) \\ 0, & \text{otherwise} \end{cases}$$

D. Peak Signal to Noise Ratio (PSNR)

The Peak Signal-to-Noise Ratio (PSNR) measures image quality in decibels (dB) and shows a direct opposite relationship to Mean Squared Error (MSE). To determine the PSNR value we use this formula.

$$PSNR = 10 \log_{10} \frac{255}{MSE} \quad (5)$$

E. Unified average changed intensity (UACI)

This metric functions as an evaluation tool to determine image encryption technique success. This average metric calculates the intensity difference between the original image (plain image) and the encrypted image (cipher image) following encryption to evaluate pixel value changes during processing.

$$UACI = \frac{1}{N} \left[\sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255} \right] \quad (6)$$

F. Time Efficiency

The proposed scheme executes at different speeds depending on the quantity of processed data. The table reveals encryption run times that measure different sizes of medical images. The encryption process requires an amount of time to perform the encryption of input images. Fast execution times occur in the scheme due to its efficient scaling and rotation operations.

Table 2. Histogram Analysis of proposed system

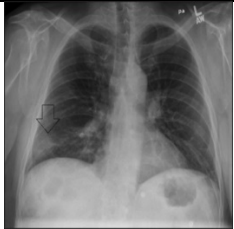
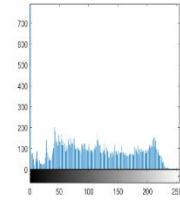
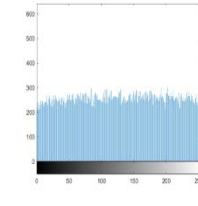
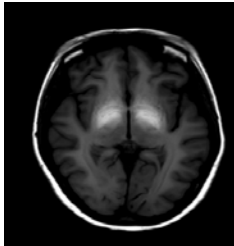
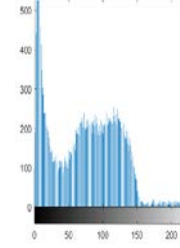
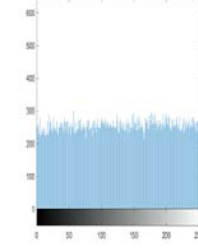

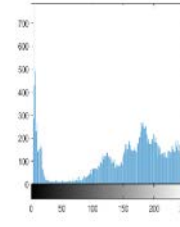
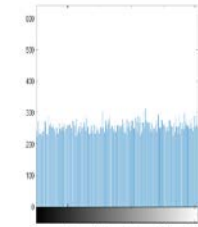

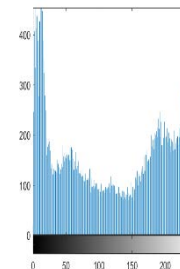
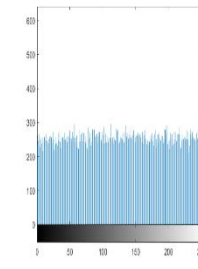

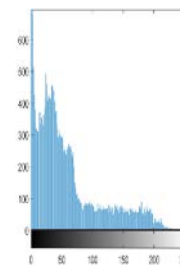
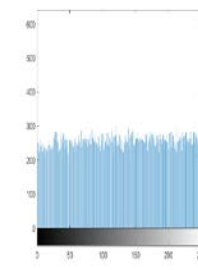
Input	Histogram of Input	Histogram of Cipher
		
		
		
		
		

Table 3. Input image and cipher image of the proposed system

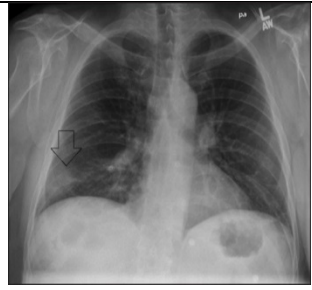
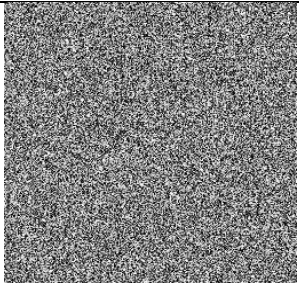
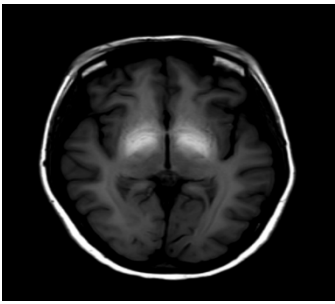
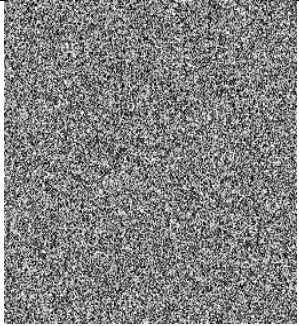

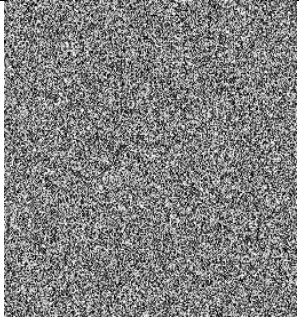

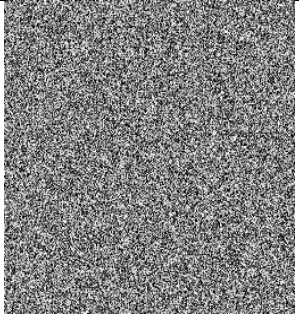

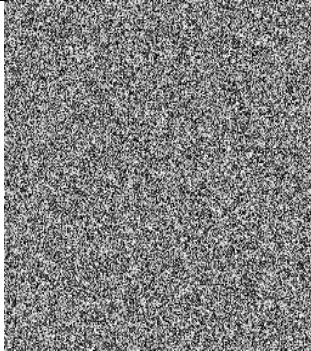
Images	Cipher Image
	
	
	
	
	

Table 4: Entropy analysis of the proposed method

Input	Input Entropy	Cipher Entropy
Chest	4.3658	7.9943
MRI	5.0221	7.8351
Hand Xray	3.2422	7.9881
Foot Xray	4.6327	7.7889
Spinal Cord	4.2513	7.9578

Table 5. NPCR and UACI of proposed method

Input	NPCR (%)	UACI (%)
Chest	98.71	32.43
MRI	98.79	33.53
Hand Xray	98.54	34.38
Foot Xray	98.67	35.55
Spinal Cord	98.99	36.52

Table 6. MSE and PSNR analysis of proposed method

Input	MSE	PSNR (db)
Chest	56.6143	20.2384
MRI	58.2644	21.4579
Hand Xray	52.2310	22.6531
Foot Xray	64.3521	24.2526
Spinal Cord	53.3784	23.4643

The proposed method demonstrates uniform distribution of histogram patterns for original images together with cipher images and decrypted images which resemble white noise behavior as shown in Table 2. Security depends on the encryption process provided by Table 3 which shows the original image with its encrypted form and its decoded output.

Performance-related analyses of the proposed method can be found in Tables 4-6. The encryption method achieves its purpose when entropy values of encrypted images match their theoretical values while maintaining security parameters such as MSE, PSNR, NPCR, and UACI within industry norms. Our encryption system demonstrates robustness against differential attacks because the security assessment verifies its necessary requirements. Table 7 shows the encryption time for the various medical images and depending on the size of the image execution time varies. Proposed system achieves fast execution for real time applications.

Table 7. Encryption time of proposed work for different medical images

Image Name	Encryption Time (sec)
Chest	0.6231
MRI	0.7134
Hand Xray	0.8277
Foot Xray	0.7058
Spinal Cord	0.6237

Table 8. Comparative analysis with state of art methods

Input	Proposed Method			Existing Method [16]		
	Entropy	NPCR	UACI	Entropy	NPCR	UACI
MRI	7.8351	98.79	33.53	7.5649	97.45	29.13

Table 8 performs an exhaustive performance analysis that examines the proposed methodology and existing methodologies by assessing entropy values and NPCR and UACI measurements. The results demonstrate that the new method delivers better results when compared to conventional methods for every area considered. The results of performance assessment demonstrate the superior capabilities of the proposed approach because it achieves higher entropy values and NPCR measures along with UACI metric scores than previous methodologies. Image encryption developed through technological improvements enables the proposed method to outperform earlier approaches regarding their performance and reliability standards.

DISCUSSION

The proposed encryption method effectively ensures the security of medical images by exhibiting a uniform distribution of histogram patterns for original, encrypted, and decrypted images. This behaviour, resembling white noise, enhances resistance to statistical attacks. The robustness of the encryption process is further validated through security assessments, as illustrated in Table 3, which highlights the successful encryption and decryption of images.

Performance metrics play a crucial role in evaluating the effectiveness of the encryption system. The entropy values of encrypted images align with their theoretical expectations, confirming the unpredictability and randomness of encrypted data. Additionally, key security parameters such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI) are maintained within industry standards, reinforcing the reliability of the encryption technique.

The Mean Squared Error (MSE) quantifies the difference between the original and encrypted images, with higher values signifying greater distortion and stronger encryption. Conversely, the Peak Signal-to-Noise Ratio (PSNR) measures the quality of the encrypted image in comparison to the original; lower PSNR values indicate a more secure encryption process as they suggest greater deviation from the original data.

Moreover, two widely used metrics for assessing the sensitivity of encryption to changes in plaintext and keys are the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). NPCR measures the percentage of pixels that change when a single pixel in the original image is modified, ensuring that minor changes in input result in significant alterations in the encrypted output. A high NPCR value (close to 99%) suggests strong diffusion characteristics. UACI, on the other hand, evaluates the average intensity variation between the original and encrypted images, with optimal values demonstrating effective encryption.

CONCLUSION AND FUTURE WORK

The proposed encryption method demonstrates its effectiveness in tackling medical image issues because it encrypts medical data characteristics which stem from interconnected pixels. The algorithm protects patient data security through its chaotic and rotational systems and ensures fast operations are essential for real-time capabilities. The unpredictability of chaotic systems results in a large key field that protects against brute-force attacks. The scheme keeps medical information secure using high NPCR and UACI values while requiring computer systems to perform minimal tasks. The researcher suggests developing optimized methods for processing large image datasets as well as conducting system tests on multiple medical imaging formats that include three-dimensional and multicolor images. Improvements to the encryption system could be achieved by using deep learning methods for key generation and adaptive encryption protocols based on image characteristics which would result in advanced security features and system performance outputs.

AUTHOR CONTRIBUTIONS

K Paramesha and Karthik V contributed to the **conceptualization** and **methodology**, ensuring the study's framework and research direction were well-defined. Prashanth M V and Sathisha M S were responsible for **software development** and **validation**, implementing the computational aspects and verifying the accuracy of the results. Bhargav H K and Ranjan Kumar H S played a key role in **formal analysis** and **investigation**, conducting in-depth examinations and drawing meaningful conclusions. Raju K and Kiran Puttegowda provided essential **resources** and contributed to **writing – review & editing**, refining the manuscript for clarity and coherence.

CONFLICT OF INTEREST STATEMENT

Authors declare that there is no conflict of interest for publication of this work.

REFERENCES

1. S. Inam, S. Kanwal, R. Firdous, K. Zakria, F. Hajje. A new method of image encryption using advanced encryption Standard (AES) for network security. *Phys. Scr.* **2023**, 98 (12), 126005.
2. S.D. Sanap, V. More. Design of efficient S-box for Advanced Encryption Standard. *J. Integr. Sci. Technol.* **2022**, 10 (1), 39–43.
3. K.N. Bharath, K.S. Babu, V. Ravi. Security of Magnetic Resonance Medical Images Using Region-Based Lossless Image Compression in Healthcare Information Systems. *Open Public Heal. J* **2024**, 17 (1).
4. S.S. Jamal, M.M. Hazzazi, M.F. Khan, et al. Region of interest-based medical image encryption technique based on chaotic S-boxes. *Expert Syst. Appl.* **2024**, 238.
5. B. Suvitha, D. Murugan. Integrating Deep Learning and Homomorphic Encryption for Secure Image Transmission. *J. Mach. Comput.* **2024**, 4 (4), 1206–1219.
6. Q. Natsheh, A. Sălăgean, D. Zhou, E. Edirisinghe. Automatic Selective Encryption of DICOM Images. *Appl. Sci.* **2023**, 13 (8), 4779.
7. R. Chen, X. Li, L. Teng, X. Wang. Selective region medical image encryption algorithm based on cascade chaos and two-dimensional Joseph traversal. *Phys. Scr.* **2023**, 98 (3), 98.
8. Abhishek, H.K. Tripathy, S. Mishra. A Succinct Analytical Study of the Usability of Encryption Methods in Healthcare Data Security. In *Studies in Computational Intelligence*; Springer Nature Singapore, Singapore, **2022**; Vol. 1039, pp 105–120.
9. L.A. Salman, A.T. Hashim, A.M. Hasan. Selective Medical Image Encryption Using Polynomial-Based Secret Image Sharing and Chaotic Map. *Int. J. Saf. Secur. Eng.* **2022**, 12 (3), 357–369.
10. B. Zhang, B. Rahmatullah, S.L. Wang, Z. Liu. A plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-logistic map. *Multimed. Tools Appl.* **2023**, 82 (10), 15735–15762.
11. X. Meng, J. Li, X. Di, Y. Sheng, D. Jiang. An Encryption Algorithm for Region of Interest in Medical DICOM Based on One-Dimensional $e\lambda$ -coscot Map. *Entropy* **2022**, 24 (7), 901.
12. P. Kiran, B.D. Parameshachari. Resource Optimized Selective Image Encryption of Medical Images Using Multiple Chaotic Systems. *Microprocess. Microsyst.* **2022**, 91 (1), 1–20.
13. X. Wang, Y. Wang. Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points. *Expert Syst. Appl.* **2023**, 213, 118924.
14. A. Amaithi Rajan, V. V. M. Raikwar, R. Balaraman. SMedIR: secure medical image retrieval framework with ConvNeXt-based indexing and searchable encryption in the cloud. *J. Cloud Comput.* **2024**, 13 (1), 139.
15. S. Rajendran, C. Baskar, G. Gugapriya, S. Sridharan. A robust medical image cryptosystem based on hyperbolic chaotic system and circular bit-shifting-flipping techniques. *Alexandria Eng. J.* **2024**, 97, 169–183.
16. M.M. Sayah, K.M. Redouane, K. Amine. Secure transmission and integrity verification for color medical images in telemedicine applications. *Multimed. Tools Appl.* **2022**, 81 (30), 43613–43638.
17. P. Kiran, B.D. Parameshachari, K. V. Sudheesh, D.S. Sunil Kumar. Resource optimized Region Based Image Encryption Using Chaotic Maps. *Int. J. e-Collaboration* **2022**, 18 (1), 1–20.
18. Y. Wu, L. Zhang, S. Berretti, S. Wan. Medical Image Encryption by Content-Aware DNA Computing for Secure Healthcare. *IEEE Trans. Ind. Informatics* **2023**, 19 (2), 2089–2098.
19. P. Renukadevi, M.S. Mohamed. Medical Image Segmentation Based Image Compression with Secure Cloud Data Storage. *Math. Stat. Eng. Appl.* **2022**, 71 (3), 1074–1095.
20. S.S. Jamal, M.M. Hazzazi, M.F. Khan, et al. Region of interest-based medical image encryption technique based on chaotic S-boxes. *Expert Syst. Appl.* **2024**, 238, 122030.
21. K. V. Sudheesh, S.B. Santhosha, K. Puttegowda. Henon Maps based selective image encryption approach for enhanced control and security. *J. Integr. Sci. Technol.* **2025**, 13 (2), 1034–1034.
22. K. Prabhavathi, M.B. Anandaraju, Kiran. An efficient medical image encryption algorithm for telemedicine applications. *Microprocess. Microsyst.* **2023**, 101, 104907.
23. M. Dua, R. Bhogal. Medical image encryption using novel sine-tangent chaotic map. In *e-Prime - Advances in Electrical Engineering, Electronics and Energy*; **2024**; Vol. 9, p 100642.
24. S. Inam, S. Kanwal, A. Anwar, N. Fatima Mirza, H. Alfraihi. Security of End-to-End medical images encryption system using trained deep learning encryption and decryption network. *Egypt. Informatics J.* **2024**, 28, 100541.
25. P. K, A. M B, V. Ravi. Region based medical image encryption using advanced zigzag transform and 2D logistic sine map (2DLSM). *Int. J. Cogn. Comput. Eng.* **2023**, 4, 349–362.
26. Z. Zhang, J. Tang, F. Zhang, T. Huang, M. Lu. Medical image encryption based on Josephus scrambling and dynamic cross-diffusion for patient privacy security. *IEEE Trans. Circuits Syst. Video Technol.* **2024**.
27. B. Long, Z. Chen, T. Liu, et al. A Novel Medical Image Encryption Scheme Based on Deep Learning Feature Encoding and Decoding. *IEEE Access* **2024**, 12, 38382–38398.