ADBA
Computers and Electronics in Medicine
Cutting-Edge Scientific Solutions

e-ISSN: 3023-8609
RESEARCH ARTICLE
Vol.2 / No.2 / 2025 / pp.53-59
https://doi.org/10.69882/adba.cem.2025074

A Chaos-Based Encryption Scheme for Secure Medical X-ray Images

Yasin Kaya *,[1] **and Zeynep Gürkas Aydin** *,[2]
[1]Istanbul University-Cerrahpaşa, Department of Computer Engineering, Istanbul, Türkiye.

ABSTRACT Data privacy in healthcare system is getting more importance day by day. In this study we introduce a novel chaos-based encryption scheme for medical X-ray images. We used a double Lorenz map as chaotic system to produce random key streams in confusion phase and in diffusion phase. We also used hash value of the original file to determine initial parameters of second chaotic map. So, our scheme is highly resistant to differential attacks. In confusion phase, we employed row-based and column-based shift operation to confuse original data. In diffusion phase we used XoR operation to encrypt data. Since Lorenz map has 3 dimensions, we used each one for different purposes like X dimension is for row-based shift operation, Y dimension is for column-based shift operation, Z dimension is for data distribution, XoR operation etc. On average, our scheme generates a NPCR value exceeding 99.66% and an UACI value of approximately 33.39% when there is a one-pixel alteration in the plaintext. Additionally, it yields an average information entropy value greater than 7.9976. Since our method utilizes a double Lorenz map, it is resilient against brute force attacks. The results from our tests and analyses indicate that our schema is pretty fast, dependable, resilient, practical, and effective. It serves as a solid encryption scheme option for medical images.

KEYWORDS
Nonlinear dynamics
Chaos
Medical image encryption
Hash-Code
Security

INTRODUCTION

Medical image encryption has been a hot topic for several decades in terms of patient data privacy. Numerous encryption methods have been developed based on different ideas and systems to protect data from prying eyes or unauthorized access. One of the most popular systems is chaotic systems. Because of their anatomical characteristics, such as pseudo-randomness, ergodicity, high sensitivity to initial conditions and parameters, and aperiodicity, chaotic systems have become more popular in cryptography in recent years. Researchers have long benefited from chaotic systems in their studies since these characteristics are necessary for a strong encryption scheme (Malik *et al.* 2020; Mohammed *et al.* 2023; Abdelli *et al.* 2024).

In order to achieve much more successive and robust outcomes, researchers prefer using chaotic systems with other mathematical models like DNA (deoxyribonucleic acid) (Chai *et al.* 2017, 2019; Liu and Liu 2020; Wang *et al.* 2019; Zhou *et al.* 2022), Fourier Transform (Farah *et al.* 2020), Generative Adversarial Networks (Fang *et al.* 2021), Hilbert Curves and H-Fractals (Zhang *et al.* 2019), Knuth–Durstenfeld (Wang *et al.* 2020), Transcendental Numbers (Silva Garcia *et al.* 2019), Particle Swarm Optimization (Alibrahim and Ludwig 2021), Latin Square (Machkour *et al.* 2015), Rotor Machine (Rehman *et al.* 2020), and Discrete Wavelet Transform (DWT) (Oteko Tresor and Sumbwanyambe 2019).

In this study, we propose a chaos-based image encryption scheme to protect medical X-ray images. We used a dual Lorenz map, where the XOR operation is applied using the outcome of the second map and the number of shift steps for both rows and columns is determined using the first map. The secret key is the only source of input parameters for the first Lorenz map, whereas the hash value of the plaintext and the secret key are combined to provide the input parameters for the second Lorenz map. Our technique is highly resistant to differential attacks by using the plaintext hash value to set the input parameter for the second Lorenz map. When a single pixel in the plaintext changes, it typically generates a value of over 99.66% NPCR (number of pixels change rate) and over 33.39% UACI (unified average changing intensity). Additionally, it generates an average information entropy value of more than 7.9976.

When we look at the literature, we see that researchers have been using chaotic systems extensively in medical image encryption for several decades. Demirkol *et al.* (2024) proposed a novel locally active memristor-based chaotic circuit model and presented a real-time hybrid image encryption application developed on a PYNQ-Z1 (Python Productivity for Zynq) low-cost FPGA board using Jupiter programming environment. The proposed hybrid algorithm combines memristor-based chaos with a DNA encryption algorithm exploiting diffusion-confusion techniques.

Manuscript received: 26 May 2025,
Revised: 20 July 2025,
Accepted: 20 July 2025.

[1]ysnky@yahoo.com (**Corresponding author**)
[2]zeynepg@iuc.edu.tr

Kanwal *et al.* (2024) offered an IoT-Blockchain system based on chaos smart healthcare image encryption scheme using Tinkerbell mapping to ensure medical data integrity and authenticity. The suggested approach was examined to assess performance parameters such as key space analysis, key sensitivity analysis, Information Entropy (IE), histogram, correlation of adjacent pixels, Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and Structural Similarity Index (SSIM). John and Kumar (2023) proposed a hybrid chaotic model, 2D Lorentz Chaotic model coupled with the Logistic chaotic model for the encryption/decryption of medical DICOM CT images. Prior to encryption, preprocessing was done by the median filter. The hybrid chaotic model scrambles the rows and columns of the image and bitwise XOR operation is carried out to generate the encrypted image. Ismail *et al.* (2018) proposed a medical image encryption algorithm based on pseudo-random sequence generation using the proposed generalized DH map offering secure communication transfer of medical MRI and X-ray images. Security analyses are carried out to consolidate system efficiency including key sensitivity and key-space analyses, histogram analysis, correlation coefficients, MAE, NPCR and UACI calculations.

Several other notable works have contributed to this field. Vijayakumar and Ahilan (2024) offered a new medical image encryption technology based on chaotic map substitution boxes (S-box) and cellular automata (CA). Qobbi *et al.* (2023) proposed a new method for medical image encrypting of arbitrary sizes and formats based on chaos with an S-box construction. Rehman *et a* (2023) presented a color medical image encryption scheme that integrates multiple encryption techniques, including alternate quantum random walks and controlled Rubik's Cube transformation Roy *et al.* (2025) offered an innovative framework that integrate healthcare engineering, chaotic encryption, and artificial intelligence (AI) to address the privacy issue of medical data. Dua and Bhogal (2024) proposed a medical image cryptosystem using one-dimensional novel Sine-Tangent Chaotic (STC) map and shared key. Masood *et al.* (2021) proposed a lightweight cryptosystem based on Henon chaotic map, Brownian motion, and Chen' chaotic system. Clemente-Lopez *et al.* (2024) proposed a chaos based lightweight encryption scheme for IoT healthcare system with a primary application in the encryption of wearable devices Kaya *et al.* (2025) proposed a novel lightweight encryption scheme for platforms with limited resources utilizing chaotic systems with a double logistic map, hash code of original file and cycle rotation.

The remainder of this paper is organized as follows. Section II presents the proposed encryption algorithm with chaotic map and the detailed methodology. Section III presents all experimental results and security analysis comparisons with other schemes. The conclusion is presented in the last section.

PROPOSED ALGORITHM

Numerous chaotic maps, ranging from basic to intricate architectures, exist, including the Henon, Lorenz, Tent, Arnold Cat, and Logistic maps. In our study we used 3-D Lorenz map in confusion and diffusion phase as pseudo random number generator. Each dimension of the map is used for a different process like X dimension is used for row-based shift operation while Y dimension is used for column-based shift operation and Z dimension is used for XoR operation. Two distinct Lorenz maps with various starting parameters were employed. Only the secret key is utilized to determine the first Lorenz map's initial parameter, and rows and columns of the plaintext are shuffled by using this key stream data for shift operations. We combined the hash value of the plaintext with the secret key to generate the initial parameters of the second Lorenz map and key stream data is utilized for XoR operation because our scheme needs to be sensitive to plaintext changes in order to withstand differential attacks.

Lorenz map

The Lorenz map is one of the most popular and widely used 3-D chaotic map, which is formulated as shown below in Eqs. (1)-(3):

$$\frac{dx}{dt} = \sigma(y - x) \tag{1}$$

$$\frac{dy}{dt} = x(\rho - z) - y \tag{2}$$

$$\frac{dz}{dt} = xy - \beta z \tag{3}$$

Here, σ, ρ and β are constant parameters and generally used the values $\sigma = 10$, $\rho = 28$, and $\beta = \frac{8}{3}$. When these (and similar) values are present, the system behaves chaotically. Lorenz map attractor can be viewed in Figure 1.

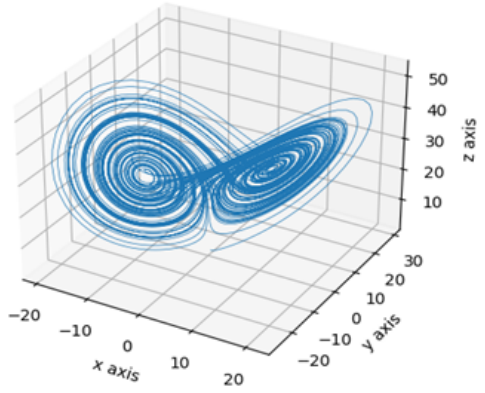

Figure 1 : Lorenz map attractor

Hash function

The fundamental purpose of hash functions is to obtain a tiny input data signature. The hash value is the result of the hash function. A successful hash function must be sensitive to even the smallest changes in the input data, meaning that even small changes should result in noticeably different hash values. Many hash functions, including SHA-1, SHA-2, SHA-3, MD5, BLAKE, xxHash and others, are now in use. Since xxHash is known as the speediest hash function we choose it in our study.

Shuffling algorithm

In the permutation phase, we employed row-based and column-based shift operations to shuffle the plaintext. Each row and each column are shifted n times which are generated by the first Lorenz map X dimension and Y dimension respectively. In decryption process we applied column-based and row-based shift operations in reverse direction to obtain unshuffled data from shuffled data.

Encryption Process

Initially, we calculate the plaintext's hash value, pick just the first two bytes of this value, and refer to it as H_2. To create pseudo random values that will be utilized in the XOR operation a step later, we utilize H_2 with a secret key as input parameters of the second Lorenz map. Next, we use key stream for row-based and column-based shift operations in the permutation phase, and we start the first Lorenz map with just a secret key as an input parameter. Then, we use a second Lorenz map key stream to perform the XOR operation on this shuffled data.

Using the H_2 value we create 1-byte validation value and used it with H_2 value as 3-byte HV_3 value. The repeating HV_3 values are then added to a new row that is added at the bottom of the matrix. Assuming, for instance, that the matrix column size is 210, the newly inserted row will have 70 times HV_3 values sequentially $(210/3 = 70)$. To safeguard the HV_3 values, we then execute the XOR operation to this row using the first Lorenz map key stream. In the final phase, we use the indexes produced by the first Lorenz map to distribute this new row data into the XORed matrix by swap operation. Consequently, the final ciphertext was acquired. Figure 2 shows all encryption processes.

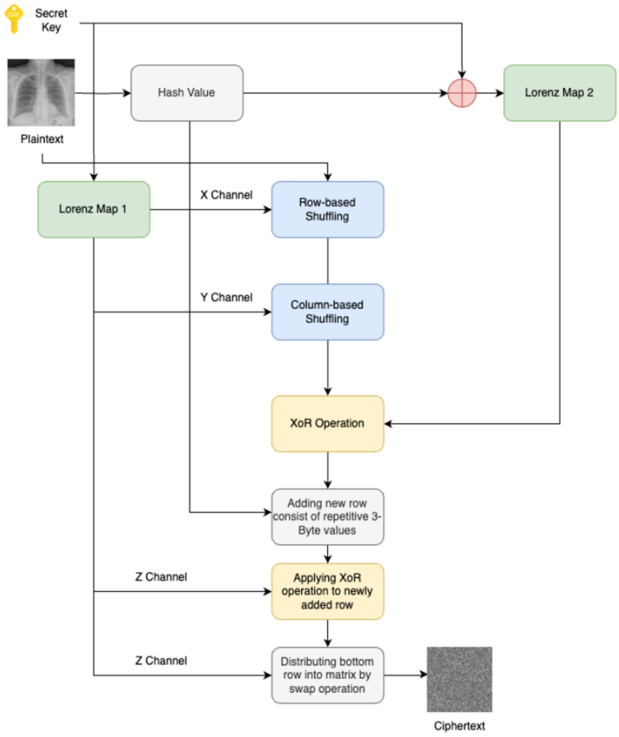

Figure 2 :Encryption process of proposed scheme

Decryption Process

To decrypt the ciphertext, the encryption operations are applied in reverse order. First, using the indices generated by the first Lorenz map, a swap operation is performed to retrieve the XORed HV_3 values and place them at the bottom row of the matrix. To recover the original HV_3 sequence, an XOR operation is then applied to this row using the corresponding key stream. Since the data may be affected by external factors such as noise or cropping attacks, validating the integrity of the HV_3 value is essential.

A validation procedure is carried out to ensure the correctness of HV_3, and only the most frequently occurring valid HV_3 value is accepted. Once the valid HV_3 value is identified, the last row is removed from the matrix, and its final byte is discarded to retrieve the H_2 value. This extracted H_2, in combination with the secret key, is then used to initialize the second Lorenz map. The resulting key stream is used to perform an XOR operation on the encrypted matrix to reverse the diffusion process.

Finally, inverse shift operations are performed on the resulting matrix — first column-based and then row-based — using the key streams generated by the first Lorenz map. As a result, the original plaintext is successfully recovered. All decryption steps are illustrated in Figure 3.

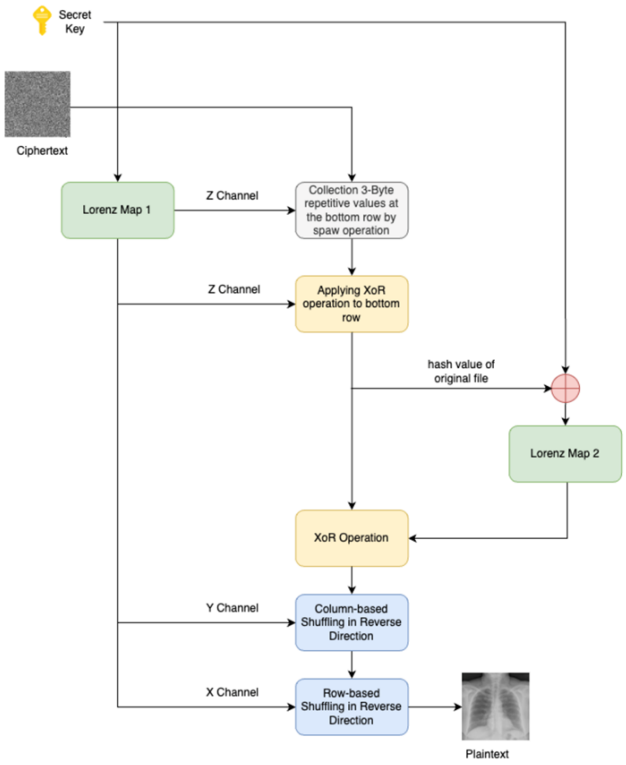

Figure 3 :Decryption process of proposed scheme

Figure 4 presents the original X-ray image (256×256 grayscale), the encrypted image obtained using the proposed scheme, and the corresponding decrypted image, respectively.

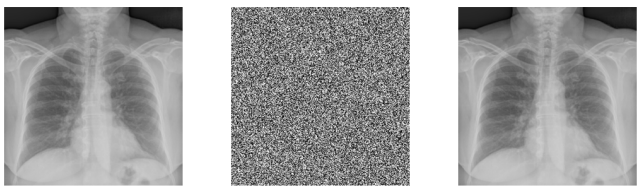

Figure 4 Scheme outputs: (a) plaintext, (b) ciphertext, (c) original plaintext.

EXPERIMENTAL RESULTS

In this section, we have conducted numerous simulated analyses and experimental tests to assess the safety, effectiveness, and robustness of our method. In our tests, we used some of medical X-ray images, like "Chest", "Foot", "Hand" and "Joint" in 256x256

grayscale format. These data are publicly available and taken from Kaggle. We tested our algorithm on a Mac OS X (Sequoia) with Apple M1 pro processor and 16 GB of RAM after developing it with Python 3.9.2.

Information Entropy Analysis

A cryptosystem's entropy value indicates how resilient the algorithm is against entropy attacks. Entropy essentially measures how randomly the pixels in an image are distributed. The calculation of information entropy is given below equation:

$$H(X) = \sum_{i=1}^{n} P_r(x_i) \log_2 \left(\frac{1}{P_r(x_i)} \right)$$

where X denotes the input image, x_i denotes a pixel value, and $P_r(x_i)$ denotes the probability of x_i. Truly random entropy value for a 2^n symbol data is n. Since there are 256 different colors and $2^8 = 256$, the truly random entropy value is 8 for a grayscale image. The algorithm appears more secure when the entropy value converges to a truly random entropy value, which is 8 in this case. Our test results are shown in Table 1 and represent satisfactory results by converging to a truly random entropy value of 8.

Table 1 Information Entropy Values of Plain and Encrypted Medical Images

Image	Size	Plain Image Entropy	Cipher Image Entropy
Chest	256×256	7.037043	7.996937
Foot	256×256	6.924769	7.997189
Hand	256×256	7.000145	7.997503
Joint	256×256	7.206429	7.997263

Histogram Analysis

The distribution of pixel frequencies in an image can be seen by histogram analysis. Histogram analysis is crucial for an encrypted image, and a balanced pixel value distribution is intended to withstand statistical attacks. The histogram leaks information about the original image and provides attackers with hints about it if it lacks a balanced distribution. The histogram analysis of both plain and encrypted images is shown in Figure 5. In contrast to the original images' histograms, the encrypted images' histograms show a distribution that is comparatively uniform.

Correlation Analysis

In terms of diagonal, vertical, and horizontal neighborhoods, there is a strong association between neighboring pixels in an image. It provides attackers with a wealth of information about the original image. Therefore, these correlations must be destroyed by a secure encryption scheme. This is measured using the correlation coefficient value between Eqs.(5)-(8) that is computed as follows:

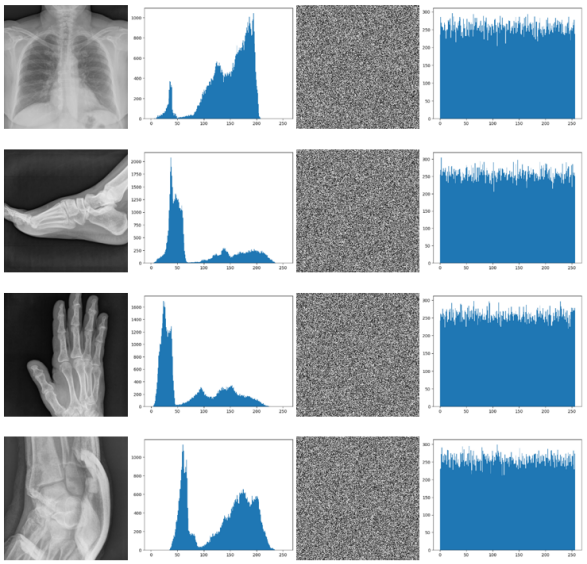

Figure 5 : Histogram analysis; the first column is original images, the second column is histograms of the original images, the third column is encrypted images, the fourth column is histograms of the encrypted images

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5}$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{6}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{7}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{8}$$

where two neighboring pixels in the image have grayscale values denoted by x and y. 10,000 neighboring pixels were chosen at random for our test in order to compute the horizontal, vertical, and diagonal correlations for each plain and encrypted image. Figure 6 displays the outcomes of our tests, and Table 2 lists the correlation coefficient values. The correlation analysis results produced by our scheme are satisfactory.

Table 2 Correlation Coefficient Values of Plain and Encrypted Images

Image	Plain H	Plain V	Plain D	Enc. H	Enc. V	Enc. D
Chest	0.9957	0.9937	0.9912	0.0139	0.0052	-0.0124
Foot	0.9970	0.9916	0.9895	-0.0134	0.0002	0.0016
Hand	0.9874	0.9965	0.9856	0.0145	-0.0181	-0.0052
Joint	0.9909	0.9969	0.9897	-0.0029	0.0108	-0.0002

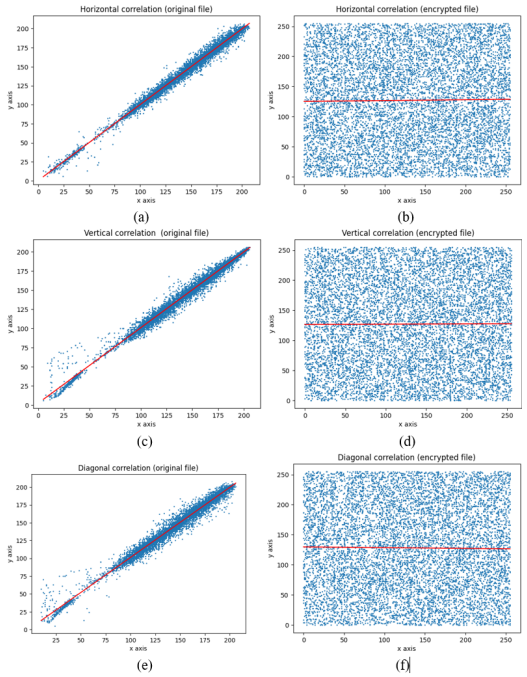

Figure 6 Correlation analysis of Chest image: (a) plain image horizontal correlation, (b) encrypted image horizontal correlation, (c) plain image vertical correlation, (d) encrypted image vertical correlation, (e) plain image diagonal correlation, (f) encrypted image diagonal correlation.

Differential attack analysis

Attackers try everything to find out the original data. In one method, the input plain image is slightly altered, and then both the original and altered images are encrypted. Next, a significant association between the plain and encrypted images is found. To assess the effect of altering a single pixel in the plaintext on the encrypted image, two metrics, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) have been created. NPCR is defined as the proportion of different pixel intensities between the plain and cipher images. Conversely, UACI is the average strength of the differences between the plain and cipher images. NPCR is formulated as in Eq. (9),

$$\text{NPCR} = \frac{\sum_{i,j} S(x,y)}{N \times M} \times 100\% \tag{9}$$

where M and N are the dimensions of the image and $S(x,y)$ is expressed as in Eq. (10):

$$S(x,y) = \begin{cases} 1, & \text{if } C_1(x,y) \neq C_2(x,y) \\ 0, & \text{if } C_1(x,y) = C_2(x,y) \end{cases} \tag{10}$$

where C_1 is the first encrypted image, and C_2 is the encrypted image after one pixel has been changed in the original image. UACI is calculated as in Eq. (11):

$$\text{UACI} = \frac{1}{nm}\left(\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100\% \tag{11}$$

where C_1 is the first encrypted image, C_2 is the encrypted image after one pixel in the original file has changed, and n and m are the image's dimensions. The NPCR and UACI values of some test images are shown in Table 3. Given that a successful encryption scheme requires an NPCR value of more than 99% and a UACI value of roughly 33%, it indicates that these values are generally good for our encryption system.

Table 3 NPCR and UACI Values of Encrypted Medical Images

Image	Size	NPCR (%)	UACI (%)
Chest	256×256	99.597215	33.499561
Foot	256×256	99.639773	33.452925
Hand	256×256	99.594175	33.434233
Joint	256×256	99.582016	33.428475

Robustness analysis

Images that are encrypted may suffer harm during network transmission. Even when some data has been lost, a strong encryption scheme should be able to restore the original image. The degree of similarity between the original and decrypted images is measured by the Peak Signal-to-Noise Ratio (PSNR). This value is infinite for the same images. Two images are said to be very similar if the PSNR value converges to infinity; if not, the similarity is low. The PSNR value is determined using Eq. (12) as follows:

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{(255 \times 255)}{\text{MSE}}\right) \quad \text{(dB)} \tag{12}$$

where MSE is the Mean Square Error value between two images, m is the width of the image and n is the height of the image. It is calculated as follows in Eq. (13):

$$\text{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n} \|I_1(i,j) - I_2(i,j)\|^2 \tag{13}$$

Cropping attack

A cropping attack substitutes all white or all black values for a portion of the encrypted image. The cropped image is then decrypted, and it is anticipated that the original image will be recovered. The missing data is then evenly spread throughout the entire image. We decrypted the cropped images after applying crop operation at four distinct ratios: 6.25%, 25%, 50%, and 75% of the full image. Despite losing 75% of the original image, our plan was able to restore the original image despite the data loss. Figure 7 lists the results of the cropping assault test, and Table 4 lists the PSNR values. These findings demonstrate how resilient our system is to cropping and data loss attack.

Table 4 PSNR Results Under Cropping Attack

Cropping Ratio	Size	PSNR (dB)
6.25%	256×256	39.876748
25%	256×256	33.914343
50%	256×256	30.909268
75%	256×256	29.150291

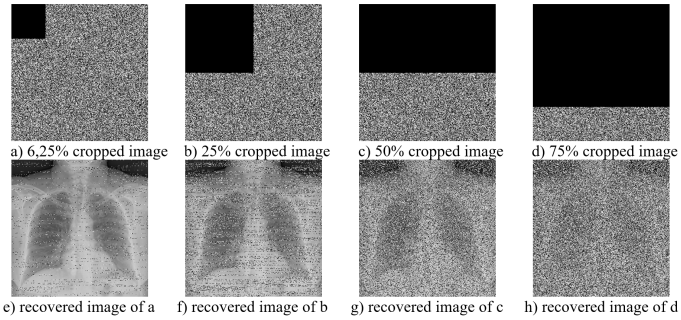

Figure 7 : Cropping attack results.

Noise attack

Some pixels of the encrypted image are randomly altered by noise attacks. Later, the encrypted image with the noise added is decoded. Despite the loss of some data, it is anticipated that the original image will be recovered. For four distinct test images, we injected noise at random in the [1000–1100] pixel range. Figure 8 displays the outcomes of the tests. We show that our approach is quite robust against noise attacks.

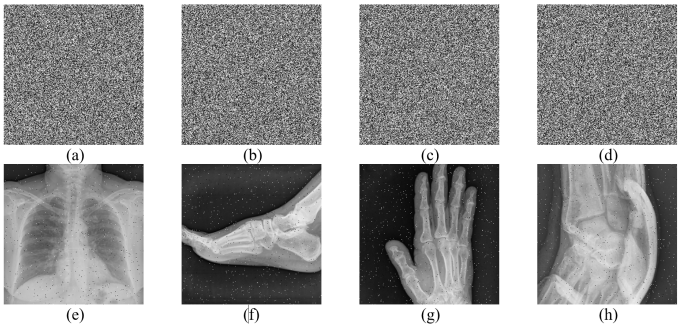

Figure 8 :Noise attack results. a) noise added encrypted image of Chest, b) noise added encrypted image of Foot, c) noise added encrypted image of Hand, d) noise added encrypted image of Joint, e) decrypted image of a, f) decrypted image of b, g) decrypted image of c, h) decrypted image of d.

THE COMPARISON OF SECURITY AND PERFORMANCE ANALYSIS

In this part, we compared our test findings with the study suggested at (Çavuşoğlu *et al.* 2017) using a 256x256 grayscale "crowd" image. They had previously compared the test results of their suggested method with those of other encryption systems using a "crowd" image; we added our test result to the study's table by using the same image. Our test results are added to Table 5 to display the result. In terms of information entropy, NPCR and UACI, our approach outperforms all others.

Table 5 Security and Performance Comparison of Encryption Algorithms

Metric	Chaos (Çavuşoğlu *et al.* 2017)	AES (Çavuşoğlu *et al.* 2017)	Ref. (Çavuşoğlu *et al.* 2017)	Ours
NPCR	99.6067	99.6325	99.6299	99.7021
UACI	31.2477	31.8724	31.8346	33.4502
Entropy	7.9545	7.9591	7.9567	7.9971

In terms of correlation coefficients, information entropy, NPCR, and UACI values, we also compared our approach with those of other studies. To ensure a fair comparison, we used a 512x512 grayscale "Barbara" image, consistent with the other algorithm tests. Table 6 summarizes all the test results. Our scheme outperforms the average of other methods in correlation coefficient values, ranks third in information entropy, holds the second-best NPCR value, and exceeds the average UACI value of the compared algorithms.

Table 6 Performance Comparison Between Our Algorithm and Other Algorithms

Scheme	Corr. H	Corr. D	Corr. V	Entropy	NPCR	UACI
Ref. Wang *et al.* (2019)	-0.0075	-0.0050	0.0040	-	-	-
Ref. Zhou *et al.* (2022)	0.0006	-0.0049	0.0005	7.9977	0.9961	0.3356
Ref. Zhang *et al.* (2019)	-0.0035	0.0025	0.0050	7.9976	0.9962	0.3337
Ref. Machkour *et al.* (2015)	0.0017	0.0023	0.0008	7.9992	0.9981	0.3332
Ref. Wang *et al.* (2016)	-0.0044	-0.0168	0.0198	-	-	-
Ref. Liu and Liu (2020)	-0.0247	-0.0031	-0.0129	7.9942	0.9950	0.3332
Ref. Bakhshandeh and Eslami (2013)	-	-	-	7.9717	0.9956	0.3357
Ref. Zhou (2021)	0.0078	-0.0164	0.0058	7.9974	0.9963	0.3353
Ref. Zhang and Tang (2017)	0.0121	0.0457	0.0389	7.9971	0.9960	0.3343
Ours	0.0045	0.0039	-0.0093	7.9976	0.9966	0.3339

CONCLUSION

This study introduces a chaos-based image encryption algorithm for medical X-ray images. We employed a double Lorenz map: one that is initialized by the secret key and used in the confusion phase, and another that is initialized by the plaintext hash value and secret key and used in the diffusion phase. Row-based and column-based shift operations were used in the confusion phase, while the XOR operation was used in the diffusion phase. To ensure our scheme was stable, resilient, and effective, we thoroughly tested and analyzed it. We evaluated our scheme against similar schemes from previous years and obtained above-average values in terms of NPCR, UACI, information entropy, and correlation coefficient. Our approach outperforms most similar schemes with an average information entropy value of 7.9976, NPCR value of 99.66%, and approximately 33.39% UACI value. All test results demonstrate that our scheme is a very strong security alternative for medical X-ray images.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

Availability of data and material

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

LITERATURE CITED

Abdelli, A., W. E. h. Youssef, F. Kharroubi, L. Khriji, and M. Machhout, 2024 A novel enhanced chaos based present lightweight cipher scheme. Physica Scripta **99**: 016004.

Alibrahim, H. and S. A. Ludwig, 2021 Image encryption algorithm based on particle swarm optimization and chaos logistic map. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*.
Bakhshandeh, A. and Z. Eslami, 2013 An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Optics and Lasers in Engineering **51**: 665–673.
Chai, X., Y. Chen, and L. Broyde, 2017 A novel chaos-based image encryption algorithm using dna sequence operations. Optics and Lasers in Engineering **88**: 197–213.
Chai, X., X. Fu, Z. Gan, Y. Lu, and Y. Chen, 2019 A color image cryptosystem based on dynamic dna encryption and chaos. Signal Processing **155**: 44–62.
Clemente-Lopez, D., J. d. Rangel-Magdaleno, and J. M. Muñoz-Pacheco, 2024 A lightweight chaos-based encryption scheme for iot healthcare systems. Internet of Things **25**: 101032.
Demirkol, A. S., M. E. Sahin, B. Karakaya, H. Ulutas, A. Ascoli, *et al.*, 2024 Real time hybrid medical image encryption algorithm combining memristor-based chaos with dna coding. Chaos, Solitons & Fractals **183**: 114923.
Dua, M. and R. Bhogal, 2024 Medical image encryption using novel sine-tangent chaotic map. e-Prime - Advances in Electrical Engineering, Electronics and Energy **9**: 100642.
Fang, P., H. Liu, C. Wu, and M. Liu, 2021 A secure chaotic block image encryption algorithm using generative adversarial networks and dna sequence coding. Mathematical Problems in Engineering **2021**: 1–26.
Farah, M. B., R. Guesmi, A. Kachouri, and M. Samet, 2020 A novel chaos based optical image encryption using fractional fourier transform and dna sequence operation. Optics & Laser Technology **121**: 105777.
Ismail, S. M., L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-Elyazeed, 2018 Generalized double-humped logistic map-based medical image encryption. Journal of Advanced Research **10**: 85–98.
John, S. and S. Kumar, 2023 2d lorentz chaotic model coupled with logistic chaotic model for medical image encryption: Towards ensuring security for teleradiology. Procedia Computer Science **218**: 918–926.
Kanwal, S., S. Inam, Z. Nawaz, F. Hajjej, H. Alfraihi, *et al.*, 2024 Securing blockchain-enabled smart health care image encryption framework using tinkerbell map. Alexandria Engineering Journal **107**: 711–729.
Kaya, Y., Z. Gurkas-Aydin, and A. Akgul, 2025 A chaos-based lightweight encryption scheme using hash-code and cyclic rotation. Physica Scripta **100**: 045203.
Liu, Q. and L. Liu, 2020 Color image encryption algorithm based on dna coding and double chaos system. IEEE Access **8**: 83596–83610.
Machkour, M., A. Saaidi, and M. L. Benmaati, 2015 A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher. 3D Research **6**.
Malik, M. G., Z. Bashir, N. Iqbal, and M. A. Imtiaz, 2020 Color image encryption algorithm based on hyper-chaos and dna computing. IEEE Access **8**: 88093–88107.
Masood, F., M. Driss, W. Boulila, J. Ahmad, S. u. Rehman, *et al.*, 2021 A lightweight chaos-based medical image encryption scheme using random shuffling and xor operations. Wireless Personal Communications **127**: 1405–1432.
Mohammed, R. A., M. A. A. Khodher, and A. Alabaichi, 2023 A novel lightweight image encryption scheme. Computers, Materials and Continua **75**: 2137–2153.
Oteko Tresor, L. and M. Sumbwanyambe, 2019 A selective image encryption scheme based on 2d dwt, henon map and 4d qi hyper-chaos. IEEE Access **7**: 103463–103472.
Qobbi, Y., A. Abid, M. Jarjar, S. E. Kaddouhi, A. Jarjar, *et al.*, 2023 Adaptation of a genetic operator and a dynamic s-box for chaotic encryption of medical and color images. Scientific African **19**.
Rehman, A. U., A. Firdous, S. Iqbal, A. Zahid, M. M. Shahid, *et al.*, 2020 A color image encryption algorithm based on one time key, chaos theory, and concept of rotor machine. IEEE Access **8**: 172275–172295.
Rehman, M. U., A. Shafique, and A. B. Usman, 2023 Securing medical information transmission between iot devices: An innovative hybrid encryption scheme based on quantum walk, dna encoding, and chaos. Internet of Things **24**: 100891.
Roy, A., D. R. Mahanta, and L. B. Mahanta, 2025 A semi-synchronous federated learning framework with chaos-based encryption for enhanced security in medical image sharing. Results in Engineering **25**: 103886.
Silva Garcia, V. M., M. D. Gonzalez Ramirez, R. F. Carapia, E. Vega-Alvarado, and E. Rodriguez Escobar, 2019 A novel method for image encryption based on chaos and transcendental numbers. IEEE Access **7**: 163729–163739.
Vijayakumar, M. and A. Ahilan, 2024 An optimized chaotic s-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map. Ain Shams Engineering Journal **15**: 102620.
Wang, S., C. Wang, and C. Xu, 2020 An image encryption algorithm based on a hidden attractor chaos system and the knuth–durstenfeld algorithm. Optics and Lasers in Engineering **128**: 105995.
Wang, X., C. Liu, and H. Zhang, 2016 An effective and fast image encryption algorithm based on chaos and interweaving of ranks. Nonlinear Dynamics **84**: 1595–1607.
Wang, X., Y. Wang, X. Zhu, and S. Unar, 2019 Image encryption scheme based on chaos and dna plane operations. Multimedia Tools and Applications **78**: 26111–26128.
Zhang, X., L. Wang, Z. Zhou, and Y. Niu, 2019 A chaos-based image encryption technique utilizing hilbert curves and h-fractals. IEEE Access **7**: 74734–74746.
Zhang, Y. and Y. Tang, 2017 A plaintext-related image encryption algorithm based on chaos. Multimedia Tools and Applications **77**: 6647–6669.
Zhou, S., 2021 A real-time one-time pad dna-chaos image encryption algorithm based on multiple keys. Optics & Laser Technology **143**: 107359.
Zhou, S., Y. Wei, Y. Zhang, and L. Teng, 2022 Novel chaotic image cryptosystem using dynamic dna coding. Research Square Platform LLC .
Çavuşoğlu, , S. Kaçar, I. Pehlivan, and A. Zengin, 2017 Secure image encryption algorithm design using a novel chaos based s-box. Chaos, Solitons & Fractals **95**: 92–101.

How to cite this article: Kaya, Y., and Aydin, Z. G Chaos-Based Encryption Scheme for Secure Medical X-ray Images. *Computers and Electronics in Medicine*, 2(2), 53-59, 2025.