Medical Image Encryption Using Chaotic Algorithms and Deep Learning

3 authors:

Zainab Salah Alhakak
University of Diyala
2 PUBLICATIONS   **0** CITATIONS

SEE PROFILE

Tariq M. Salman
Mustansiriyah University
39 PUBLICATIONS   **261** CITATIONS

SEE PROFILE

Abbas Miry
Mustansiriyah University
85 PUBLICATIONS   **498** CITATIONS

SEE PROFILE

Medical Image Encryption Using Chaotic Algorithms and Deep Learning

Zainab S. Husamuldeen[1]*   Tariq M. Salman[1]   Abbas Miry[1]

[1]*Department of Electrical Engineering, Mustansiriyah University, Iraq*
* Corresponding author's Email: zainabsalah4488@uomustansiriyah.edu.iq

Abstract: Medical image encryption is essential for safeguarding the privacy and confidentiality of patients' medical information. Integrate the chaotic system with deep learning; subsequently, the above metadata embodies an innovative methodology to protect medical images from attacks. This paper presents four ways to encrypt an image: 1D (Logistic maps) and 3D (Lorenz maps) chaotic maps, one time with ResNet-18 and another with MobileNetV2 for each chaotic map. This approach assigns a unique key to each of its images by training a deep learning network to extract chaotic parameters from metadata (EXIF data), hence reducing the likelihood of key reutilization. The suggested approach is assessed using several medical imaging modalities, including CT scans, X-rays, MRI, and Fundus images. These datasets provide extensive structural and textural diversity, guaranteeing thorough confirmation of encryption strength. The statistical test results indicated that the proposed strategy offers a superior degree of security relative to the existing techniques, with the best results of a Number of Pixels Change Rate (NPCR) of 99.62%, a Unified Average Changing Intensity (UACI) of 39.4%, and an entropy of 8.

Keywords: Image encryption, Metadata, Deep learning, Chaotic maps, ResNet-18, MobileNetV2, AES, RSA.

1. Introduction

In this era of lightning-fast communication, digital photos are indispensable. Due to their widespread usage in sectors as diverse as healthcare, academia, and the military, digital image security is garnering much attention from academics and industry professionals [1]. New diseases such as black fungus, COVID-19, and others have recently afflicted many people. To track the intricacy of these diseases, doctors use medical image reports, including X-ray, ultrasonic, and MRI scans. Treatment of certain disorders depends on the use of several medical images.

In general, these medical pictures might include much personal information about the patient; some of them could be rather delicate and private [2]. The conveyance and preservation of these medical images on the cloud pose significant security issues due to the ease with which personal information may be leaked or tampered with [3]. Recently, it has been noted that intruders and unauthorized entities are extensively stealing medical records and selling them

to dealers on the black market on the dark web. This sensitive information is subsequently found to be used in fraudulent behavior and identity theft. According to the medical history of the United States, nearly 3000 breaches involving over 500 confidential medical records resulting from hacking have happened during the past ten years. For instance, reports show that a violation of 78 million American consumers' Anthem (medical insurance firm) medical data results in harm of $115 million as payment [4]

The challenges of image encryption are different from those of text information due to factors like huge data size, redundancy, and pixel correlation; as a result, traditional text encryption techniques such as DES, IDEA, and RSA are inadequate [5, 6]. Consequently, conventional cryptographic techniques cannot be directly applied to an image[6]. The image consumes more memory and bandwidth, complicating conventional encryption techniques and resulting in slower processing times. This, therefore, influences the computational cost and the speed of the encryption process, leading typical encryption algorithms to exhibit less sensitivity to starting key or

image values, hence providing little resistance to differential assaults on images [7]

In contrast to current approaches that use static or randomly generated keys, our approach utilizes real-time information, such as EXIF metadata, derived from medical images to produce encryption keys. This makes the keys dynamic, context-sensitive, and reliant on images. Distinct characteristics and benefits of our suggested methodology:

1. Metadata-Driven Key Generation: Our methodology derives metadata directly from the medical images. This allows dynamic, context-sensitive encryption, generating a distinct key for each image.
2. Deep Learning-Guided Chaos Parameter Generation: We use deep learning models to examine information and provide optimum parameters for chaotic maps. This introduces an element of uncertainty and amplifies essential sensitivity.
3. Hybrid Chaotic-DL Encryption Framework: The proposed framework integrates the advantages of chaotic systems (velocity and unpredictability) with deep learning (adaptive feature processing), resulting in a more sophisticated and safe encryption system.
4. Comprehensive Assessment Across Varied Modalities: Our approach is evaluated on many medical imaging modalities, including CT scans, X-rays, and fundus images. This illustrates resilience across modalities.
5. Enhanced Security Metrics: The approach attains elevated NPCR and UACI values, entropy nearing the optimal level, and minimal correlation coefficients, surpassing most contemporary state-of-the-art methodologies, as shown in our comparison tables.

A. Chaotic systems

These systems are frequently employed to produce arbitrary key streams by selecting suitable initial conditions and state variables, which are also referred to as "key parameters" or, in other words, "seeds." The susceptibility of chaotic systems to initial conditions, along with their inherent unpredictability and certainty, establishes a fundamental link between chaotic properties and encryption systems [8]. Utilizing the key streams that are generated, encrypted images can be generated. Completely distinct key streams may result from an insignificant alteration in the seed values, which can lead to a substantial disparity in the output image (encrypted image). Recently, chaos-based image

encryption has attracted the interest of numerous researchers due to its chaotic properties [8].

B. Deep learning

Deep learning consists of a subset of machine learning that aims to replicate the human brain and develop an artificial neural network. It collects data characteristics by training a deep artificial neural network to execute tasks such as classification, target identification, endorsement systems, and natural language processing [9]. Deep learning utilizes the training of deep artificial neural networks on a dataset to perform feature extraction, adeptly addressing machine learning difficulties such as retrieval, classification, identification, prediction, recommendation, and natural language processing. From the input layer all the way to the output layer, activation functions and multilayer nonlinear network topologies were created to make targeted data processing easier [10]Various fields currently utilize deep neural network models, including AlexNet, VGGNet, GoogleNet, ResNet, CNN, DBN, RNN, and GAN [9]. Due to the properties that define deep education, it has been utilized in numerous studies on image encryption.

C. EXIF Metadata

EXIF (Exchangeable Image File Format) information is a standardized format method for embedding further information into image files, predominantly in JPEG, TIFF, and some PNG formats. It includes information on the method and timing of the image capture. In accordance with ISO standard 12234-1, the camera image format was established by the Japan Electronic Industries Development Association (JEIDA). Numerous firms, including Canon, Sony, and Kodak, provide cameras that utilize the EXIF header of picture files [11, 12].

This study introduces an effective approach for the encryption and decryption of medical images using chaotic maps, deep learning, and metadata. The primary contribution of this study is as follows:

1. Integrate deep learning with chaotic maps to enhance the encryption of medical images.
2. Propose an innovative way to use metadata.
3. Assessing the suggested algorithm using various measures and contrasting the results.

The following outline delineates the structure of the paper: Section 2 presents many pertinent works. Section 3 delineates chaotic maps, deep learning, RSE, and ASE methods. Section 4 delineates the methodology. Section 5 presents the outcomes of the tests undertaken, together with their details. Section 6 illustrates the robustness against attacks, and Section 7 delineates the conclusion.

287

2. Related work

This section contains several studies that have addressed the subject of image encryption in various ways. We will briefly discuss a few of these studies.

Yuling Luo et al. (2019) proposed an image encryption technique based on the elliptic curve ElGamal (EC-ElGamal) cryptography and chaotic theory. The initial values of the LTM, TSM, and pandemonium game are generated using the SHA-512 cipher. This reduces the strong correlations between adjacent pixels in a plain image and resists the known-plaintext attack and chosen-plaintext attack. In addition, the final cypher is obtained by executing the diffusion based on the chaos game and DNA code, which can enhance the randomisation of the pixel distribution in advance. The NPCR and UACI scores reached 99.6292% and 33.5039%, respectively [13]

Saleh Ibrahim et al. (2020) presented a secure dynamic S-box construction algorithm that is efficient and derived from the Henon map. The proposed scheme is shown to be resistant to chosen-plaintext and chosen-ciphertext attacks by employing the dynamic S-box, which has been proposed to construct a depicted image encryption scheme. This scheme employs a unique combination of security features by employing two techniques: 1) the use of a random nonce and secure hash algorithm to calculate per-image Henon map initialisation, and 2) the use of elliptic curve encryption to safeguard the secret key. As a result, the retrieval of secret keys is as difficult as the elliptic curve discrete logarithm problem, even in the unlikely event that the transient S-box or keystream is recovered. The proposed algorithm's encryption velocities are nearly 60 MB/s, which suggests that it is highly computationally efficient. The UACI is nearly 33.46%, and the experimental value of the NPCR exceeds 99.60% [14]

Priyansi Parida et al. (2021) proposed a robust elliptic curve-based paradigm for image encryption and authentication applicable to both greyscale and colour images. The model employs the secure Elliptic Curve Diffie-Hellman (ECDH) key exchange to derive a shared session key in conjunction with the enhanced ElGamal encoding technique. 3D and 4D Arnold Cat maps are used to efficiently jumble and alter the values of standard image pixels. The model has a high average NPCR of 99.6% and an average UACI of 33.3% [15].

Subhajit Das et al. (2022) proposed an alternative DNA coding-based medical image encryption technique and a three-dimensional unified chaotic system. An effective keyword is produced from the input image to mitigate selected and recognised plaintext assaults. Subsequently, the encryption is executed via two intricate and perplexing phases using these keys. Chaotic systems are used to generate a pseudorandom sequence used for transforming pixels into DNA bases and for the scrambling and diffusion of plaintext images. Ultimately, straightforward reversible DNA base conversion rules are used to transform and interpret the DNA bases. The deciphered cypher image is very difficult to identify without the appropriate key value. The experiment's findings indicated that the NPCR and UACI values were 99.601% and 33.42%, respectively [1].

Ijaz Khalid et al. (2022) introduced an elliptic curve integrated encryption scheme (ECIES) aimed at securing RGB images. At the outset, the users exchange a secret parameter utilising Diffie-Hellman on the elliptic curve and subsequently process it through SHA-256. Subsequently, the suggested framework allocates the initial 128 bits to ensure data confidentiality, whereas the subsequent 128 bits are designated for authentication purposes. The confusion module is achieved through the application of the affine power affine transformation, which is then followed by the last four bytes of the symmetric key. Simultaneously, the diffusion module is achieved via highly nonlinear sequences produced through the elliptic curve. The quantitative findings indicate that the average values of UACI and NPCR are 33.4125% and 99.6935%, respectively [16]

Ali Akram Abdul-Kareem et al. (2023) suggested a medical image encryption paradigm using the Discrete Wavelet Transform domain, the Fast Fourier Transform domain, and the spatial domain to ensure secure transmission of medical images. The medical image undergoes a discrete wavelet treatment prior to the magic square rearranging the image subbands. Subsequently, the Arnold transform was used to obfuscate the image inside the FFT domain, and ultimately, the WAM map was utilised to produce a bit stream for diffusing the scrambled image. The final encrypted image is generated using secret keys extracted from the WAM 3D chaotic system. Notwithstanding the intricacy of the frequency domain encryption process, the offered technique offers advantages of fast installation, improved security, and elevated encryption efficiency. The experimental values recorded for the NPCR and UACI were 99.63% and 33.58%, respectively. [17].

Ali Abou El Qassime et al. (2024) proposed an innovative hyper-chaotic logistic map that is utilised for the first time in the encryption of biological images. This system is characterised by a notable Lyapunov dimension (DL = 2.1886) and exhibits rapid synchronisation. It demonstrates exceptional

durability in the face of numerous types of attacks, especially those that are statistical, differential, ciphertext, noisy, and brute-force in nature. A correlation coefficient between -1.8319×10^{-4} and 6.6977×10^{-4} is noted, along with a substantial key space that surpasses 2^{298}. This established encryption duration ensures the quickest encryption time, approximately 0.3 seconds for 512×512 images. It was proposed that employing adaptive feedback control mode synchronisation could facilitate the rapid synchronisation of this map. The experiments yielded results indicating that UACI was 33.5438% and NPCR was 99.62% [18]

Tutu Raja Ningthoukhongjam et al. (2024) introduced an image encryption method using public key encryption, integrating the attributes of elliptic curve encryption (ECC) and Blum-Goldwasser encryption (BGC). The experimental values recorded for the NPCR and UACI were 99.6901% and 33.5260%, respectively. The total time required for the proposed method is 0.142 seconds[19].

The previous research has several deficiencies, such as a lack of real-time, high computational complexity, and limited datasets. Grayscale medical images are the sole focus of most studies, which do not conduct comparative analyses or benchmark their methods against existing techniques. Furthermore, the compression used to encrypt large image sets may affect restoration. Developing encryption methods that are more efficient and secure necessitates addressing these voids.

In our research, we focus on enhancing medical image encryption and decryption by utilizing deep learning and chaotic maps with metadata that is less complex and in different ways.

3. Methodology

This study used several techniques, which will be presented below.

3.1 Chaotic systems

Chaos is a pseudo-random and unpredictable motion characterized by its high sensitivity to initial values and parameters in a deterministic dynamical system. Based on their temporal evolution, chaotic systems can be sorted into two categories: discrete chaotic mappings and continuous chaotic systems [20].

Logistic Map: is a 1D discrete chaotic map, a system with an iterative dynamical equation and a discrete time evolution of the state, Eq.(1) [20], [21]

$$X_i = rX_{i-1}(1 - X_{i-1}) \tag{1}$$

Where the component that confines the system's growth is represented by $(1 - X_{i-1})$, and the state element at time step i is represented by $X_{i-1} \in (0, 1)$. Let r be a control parameter ranging from [0, 4] when the parameter r is within the range of (3.57, 4).

Lorenz Map: is a 3D continuous chaotic map, a dynamic system demonstrating intricate and unexpected behavior. Typically, these systems are described by a system of ordinary or partial differential equations that control the time-dependent development of state variables, Eq.(2)[20], [22]

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = \rho x - y - xz \, , \\ \frac{dz}{dt} = xy - \beta z \end{cases} \tag{2}$$

Where x, y, and z denote state variables, whereas σ, ρ, and β represent control parameters known as the Prandtl number, Rayleigh number, and direction ratio, respectively.

3.2 Deep learning

Deep neural networks are efficient for many machine learning tasks. They delineate parameterised functions from inputs to outputs via the combination of several levels of essential components, including affine transformations and basic nonlinear functions [23].

ResNet-18: (Residual Network-18) is a deep convolutional neural network (CNN) designed to mitigate the vanishing gradient issue with the use of residual connections, facilitating the effective training of deep networks [24]. The features of this network: employ residual connections (skip connections) to enhance gradient propagation, comprise fundamental residual blocks, each with two 3×3 convolutional layers, and are more efficient than deeper ResNet variants while maintaining commendable accuracy.

Architecture:
- The number of layers is 18.
- The input size is 224×224×3.
- Output size is variable.
- Residual Blocks: 8 (each containing two convolutional layers).

MobileNetV2 is a lightweight CNN specifically engineered for mobile and embedded applications. It enhances efficiency by utilizing inverted residual blocks and linear constraints [25]. The features of this network: employ inverted residuals and linear bottlenecks to enhance efficiency, depthwise separable convolutions to decrease computing

expenses, optimized for mobile and edge devices with reduced parameters, and ReLU6 activation to enhance accuracy on low-bit hardware.
Architecture:

- Number of Layers: 53 convolutional layers.
- Input Dimensions: 224×224×3.
- Output Size: Variable.
- Model Size: Approximately 3.4 million parameters.

3.3 RSA algorithm

The RSA algorithm, developed by Rivest et al. in 1978, is an asymmetric cryptosystem using two keys: a public key for encryption and a private key for decryption, in distinction to symmetric cryptosystems that use a single key[26]Steps for RSA Key Generation[27]:

1- Choose two substantial prime numbers, p and q.
2- Calculate N and Euler's totient function.
$$N = p \times q, \; \varphi(N) = (p - 1) \times (q - 1)$$
3- Determine an encryption key e that satisfies the following conditions:
$$1 < e < \varphi(N), \; \gcd(e, \varphi(N)) = 1$$
4- Calculate the decryption key d.
$$e \cdot d \equiv 1 \,(\mathrm{mod}\,\varphi(N))$$

Encryption and Decryption:

- Encryption transforms plaintext M (less than N) into ciphertext C using the public key (e, N).
$$C = M^e \mathrm{mod} N$$
- Decryption: Retrieves the plaintext via the private key (d, N). $M = C^d \,\mathrm{mod}\, N$

3.4 AES algorithm

AES (Advanced Encryption Standard) was endorsed by NIST in 2001 as FIPS-197, superseding DES, which was withdrawn in 2005. It accommodates key lengths of 192, 256, or 128-bit and 128-bit data blocks. The AES algorithm has 10, 12, or 14 rounds of processing, corresponding to 128, 192, or 256-bit keys [27]. AES manipulates data inside a 4×4 byte matrix referred to as the state. Encryption starts with an AddRoundKey phase, followed by nine principal rounds, each executing four transformations[26]:

1. SubBytes: Substitutes each byte via the Rijndael S-box.
2. ShiftRows: Cyclically shifts rows according to their location.
3. MixColumns: Performs polynomial multiplication of columns using a predetermined matrix.

4. AddRoundKey: Executes a bitwise XOR operation with the round key.

The definitive round excludes the MixColumns phase. Decryption reverses these alterations with inverse functions (Inverse SubBytes, Inverse ShiftRows, Inverse MixColumns).

Each AES round guarantees safe and efficient encryption, establishing AES as one of the most used encryption algorithms.

4. Proposed method

Four techniques are used to encrypt medical images from different entities to cover this study. Clarified as it comes:

- Logistic Map with ResNet-18.
- Logistic Map with ResNet-18.
- Lorenz Map with MobileNetV2.
- Lorenz Map with MobileNetV2.

Fig. 1 represents the whole framework of the suggested methodology, while the comprehensive procedures for the suggested encryption technique are as stated below:

1. Upload the medical image.
2. Extract metadata from the image's EXIF information, including date and time.
3. If metadata is unavailable, manually input the date and time.
4. Transform metadata into an image form compatible with the deep neural network.
5. Train a neural network to correlate metadata with parameters of chaotic systems.
6. Generate chaotic parameters from the trained model.
7. Using the chaotic parameters as inputs for the chaotic Map and inserting initial parameters as fixed numbers.
8. Generate three chaotic sequences(xkey, ykey, zkey).
9. Sort the row and column indices using the xkey and ykey:

- xindex: The row indices are sorted according to the xkey.
- yindex: The column indices are sorted according to the ykey.

10. Rearrange rows and columns(permutation):

- First, shuffle the rows using yindex.
- Then, shuffle the columns using xindex.

11. Perform the XOR operation between the pixel of the scrambled image and zkey (diffusion).
12. The encrypted image is the output.
13. Encryption keys using a hybrid AES and RSA encryption scheme:
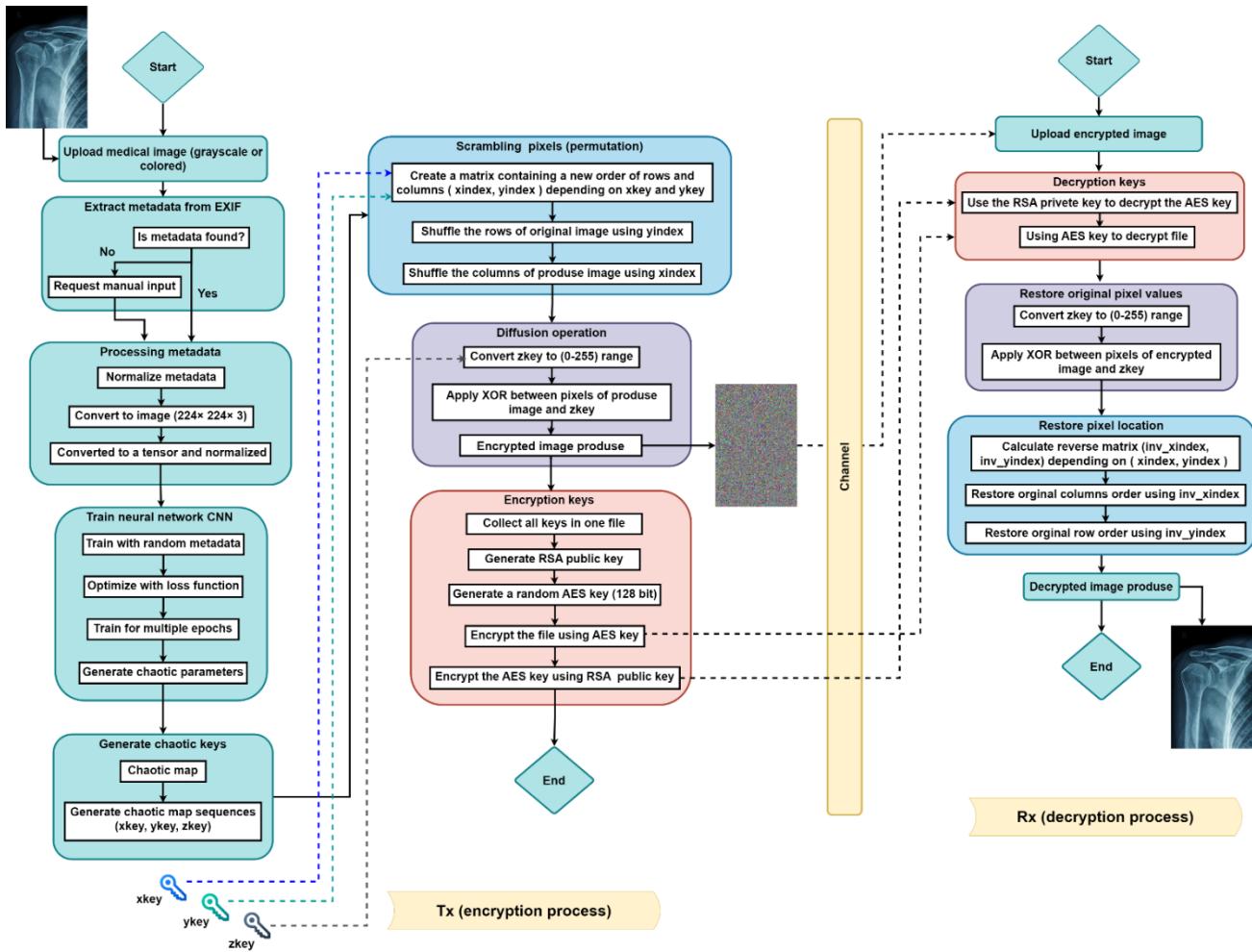
Figure. 1 The general outline for the suggested method

- Collect all keys (xindex, yindex, zkey) in one file.
- Produce RSA public key (e, N).
- Produce a random AES key with a length of 128 bits.
- Using the AES key, encrypt the file that contains the keys.
- Cipher the AES key by using the public key generated by RSA.

The suggested decryption technique is the opposite of encryption. The receivers decrypt a ciphered image by employing the keys (xindex, yindex, zkey) in the following steps:

1. Receive encrypted image.
2. Decryption keys:
- Utilizing the private key of the RSA(d, N) algorithm to decipher the AES key.
- The use of the AES key in order to decipher the file.
3. Restore the pixel values of the original image by performing the XOR operation between the pixel of the encrypted image and the zkey.

4. Calculate inv_xindex and inv_yindex from xindex and yindex.
5. Restore pixel location:
- First, reinstate the order of columns with inv_xindex use.
- Then, reinstate the order of the row with inv_yindex use.
6. The decrypted image is the output.

5. Results

The results obtained are presented in this section for the four ways to encrypt medical images of various sizes, whether grayscale or color (8 bits). This work utilizes experimental data from open-access medical images sourced from the NIH[28], the DRIVE image collection[29], Chest X-ray images (Pneumonia)[30], and Brain Tumor MRI

This dataset [31]includes modalities such as CT scans, X-rays, MRI, and Fundus images. Table 2 displays medical images with their encryption outcomes, including their names and dimensions. These results are evaluated based on encryption

Table 1. Comparison of key space

proposed method	Ref. [19]	Ref. [13]	Ref. [14]	Ref. [15]	Ref. [16]
2^{133120}	2^{1024}	2^{564}	2^{208}	2^{512}	2^{128}

Table 2. Comparisons of time consumption with other methods [unit: sec]

Ref.	Image size	Encryption time	Decryption time
Proposed	256×256 512×512	0.7914 1.8107	0.8669 1.9592
[17]	512×512	10.22	-
[18]	256×256 512×512	0.103657 0.303619	0.098381 0.274332
[13]	256×256 512×512	1.17084 4.73389	-

standards such as entropy, Number of pixels change rate (NPCR), Unified average changing intensity (UACI), Correlations of Adjacent Pixels, Peak signal-to-noise Ratio (PSNR), and histogram.

5.1 Entropy analysis

Entropy is the statistical analysis of randomness or uncertainty within images [32]of the encrypted image ranges from 0 to 8, as the maximum pixel value, expressed in 8-bit binary, is 255. Test results nearing 8 indicate the efficacy of the encryption system and the significant unpredictability of the image [17]. Entropy can be determined using the mathematical [33]Eq. (3).

$$E(q) = -\sum_{i=0}^{255} p(q_i) \log_2 p(q_i) \qquad (3)$$

Where $p(q_i)$ is the probability of (q_i), Table 4 demonstrates the outcomes of using the entropy analysis. In our studies, encrypted images regularly attained entropy levels of 8, which is the optimal value. This signifies a very uniform distribution of pixel values, rendering statistical assaults mostly useless. The increased entropy arises from the implementation of metadata-driven dynamic key creation. Each image has unique information, leading deep learning models to provide separate chaotic parameters for every encryption instance, hence enhancing uncertainty and pixel variation.

5.2 NPCR measure

NPCR is an index often used to assess the variations between images before and after encryption, serving as a metric for evaluating image encryption techniques, whose maximum value is 100%. NPCR is a method devised to evaluate the sensitivity of an encryption algorithmic process concerning an image [20]. It forms in the following manner, Eq. (4):

$$\text{NPCR} = \sum_{i,j} \frac{d(i,j)}{S} \times 100\% \qquad (4)$$

Let S represent all of the pixel counts in the original image, and let d denote a binary array formed as follows Eq. (5):

$$d = \begin{cases} 1 & if\ C_1(i,j) \neq C_2(i,j) \\ 0 & if\ C_1(i,j) = C_2(i,j) \end{cases} \qquad (5)$$

Where C_1 signifies the input image, whereas C_2 denotes the encrypted image, Table 4 demonstrates that the NPCR attained by the suggested system is roughly equivalent to the optimal values, indicating that the algorithm exhibits enhanced resilience against various assaults.

5.3 UACI measure

The average variance between the image before and after the encryption procedure is measured by UACI. This greater value suggests that there is an important difference between the images. The typical range for UACI in an ideal encryption scheme is between 30% and 35%; however, this range is contingent upon the image and algorithm employed [20], [34] Eq. (6).

$$UACI = \frac{1}{P}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{M} \right] \times 100\% \qquad (6)$$

Where P is the number of pixels, M is the maximum permissible pixel value in the images, and C1 and C2 are the input and encrypted images, respectively. Table 4 exhibits the outcomes of using the UACI measure. The suggested approach achieves a great performance in UACI. Consequently, it will provide robust protection against "known plaintext attacks" and "chosen plaintext attacks".

5.4 Correlation coefficient

The linear correlation assesses the relationship among successive pixels in vertical, horizontal, and diagonal arrangements [35]. Optimal encryption

requires little correlation. Denotes the mathematical correlation Eq. (7) [36]

$$r = \frac{Covariance(x,y)}{S_x \times S_y} \qquad (7)$$

Where S_x and S_y represent the standard deviations at pixel positions x and y, values of r approaching 0 indicate the absence of a relationship between neighboring pixels. Table 5 presents the results of using correlation measures. We have juxtaposed our results with contemporary studies. Table 6 summarizes the various comparative criteria, allowing us to infer that our findings demonstrate greater performance.

5.5 Histogram analysis

The histogram shows the distribution of pixel values in the image. An optimal approach requires a smooth histogram with evenly distributed pixel values to prevent the loss of image information. [20]

Table 2 displays the histograms of Samples 1, 2, 3, and 4 for both encrypted and original images. The histogram of these images indicates that the suggested technique offers robust security and is resilient against static assaults because of its uniform distribution for the histogram of the encrypted image.

5.6 MSE measure

The mean square error (MSE) is calculated to assess the discrepancies between the original and decrypted images. The decrypted image quality and the efficacy of the encryption algorithm are indicated by minor variations in MSE, which should be as low as possible. It is determined that the MSE is as Eq. (8) [17] :

$$MSE = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left[f(x,y)_r - f(x,y)_p \right]^2 \qquad (8)$$

Where the input image is represented by $f(x,y)_p$, while the encrypted or decrypted image is represented by $f(x,y)_r$. X and Y are pixel coordinates, while M and N are the dimensions of the images [17], [37]. Tables 4 and 5 present the results of using the MSE measure.

5.7 PSNR measure

The PSNR is regarded as a very appropriate criterion for evaluating encryption quality since it quantifies the degree of distortion in an image after encryption; fundamentally, it measures the similarity

between the original image and its encrypted version[38]. A PSNR value below 10 is considered acceptable for efficient encryption; however, the PSNR between the original image and the post-decryption image approaches infinity. It is computed using the following Eq. (9) [37].

$$PSNR = 20\, log_{10}(\frac{K-1}{\sqrt{MSE}}) \qquad (9)$$

Let K be the maximum value an image may get, often K=2^8. The PSNR values for various grey and color medical images are presented in Table 3. The results indicate that our proposed algorithm is highly effective in the encryption of medical images.

5.8 Key space

An effective image-encryption method must exhibit robust key sensitivity, and its key space ought to be sufficiently expansive to render brute force assaults unfeasible [39]. The proposed method uses three keys (xindex, yindex, zkey). Xindex and yindex lengths depend on the image's width (W) and height (H), respectively, while zkey depends on the image size. Then, the key size will be calculated as follows, Eq. (10):

$$\text{Key size(bits)} = (L_{xin} + L_{yin} + L_z) \times 8 \qquad (10)$$

Where L_{xin}, L_{yin} and L_z are the length of xindex, yindex and zkey, respectively and 8 is the bit-depth. To calculate the key space [40]we used the following equation (11):
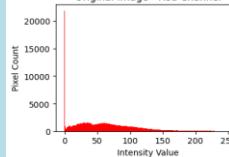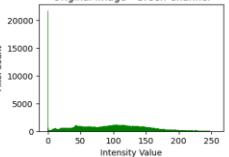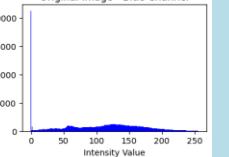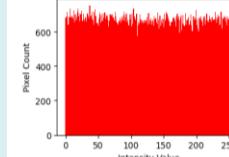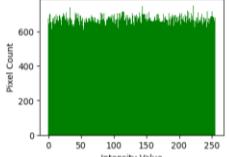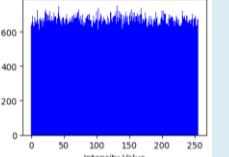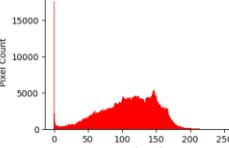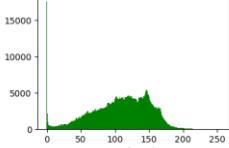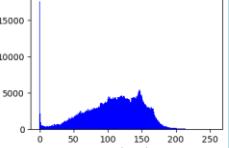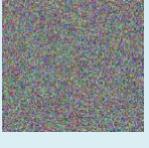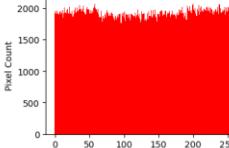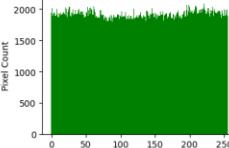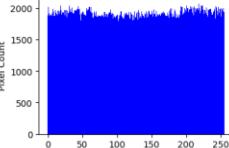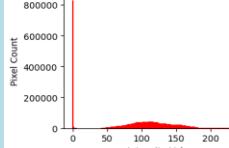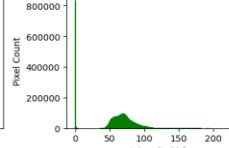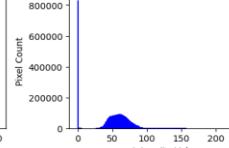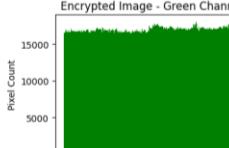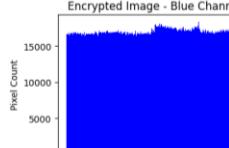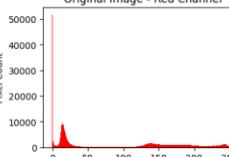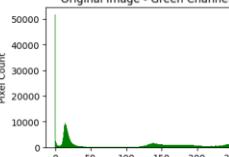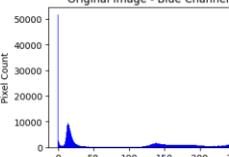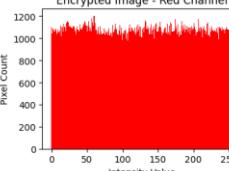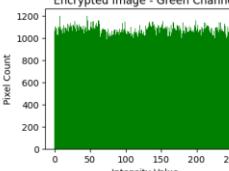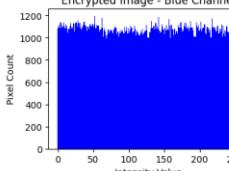
$$\text{Key space} = 2^{\text{Key size}} \qquad (11)$$

For example, when the image size (128×128) is used as input to a logistic map with ResNet-18, the key space is approximately 2^{133120}, much larger than 2^{128}. So, the key space changes with image size and how it is used. Additionally, to determine the effective key entropy, we used to analyse the statistical randomness of the key sequences using the NIST SP 800-22 test suite[41], which is esteemed for validating cryptographic randomness, and the result of this test was 7.9864 bits, approaching the theoretical limit of 8 bits. This signifies a substantial level of unpredictability and uniform distribution among key values, suggesting that the keys are resilient to statistical and brute-force attacks.

5.9 Key sensitivity analysis

The transmitter generates the encryption keys (xkey, ykey, zkey) and transmits them securely to the

Table 3. The original and encrypted images with histogram

| Image name\size	Image	Histogram		
Sample 1 (original image) 339×509		Original Image - Red Channel	Original Image - Green Channel	Original Image - Blue Channel
Sample 1 (encrypted image)		Encrypted Image - Red Channel	Encrypted Image - Green Channel	Encrypted Image - Blue Channel
Sample 2 (original image) 702×701		Original Image - Red Channel	Original Image - Green Channel	Original Image - Blue Channel
Sample 2 (encrypted image)		Encrypted Image - Red Channel	Encrypted Image - Green Channel	Encrypted Image - Blue Channel
Sample 3 (original image) 2124×2056		Original Image - Red Channel	Original Image - Green Channel	Original Image - Blue Channel
Sample 3 (encrypted image)		Encrypted Image - Red Channel	Encrypted Image - Green Channel	Encrypted Image - Blue Channel
Sample 4 (original image) 581×476		Original Image - Red Channel	Original Image - Green Channel	Original Image - Blue Channel
Sample 4 (encrypted image)		Encrypted Image - Red Channel	Encrypted Image - Green Channel	Encrypted Image - Blue Channel
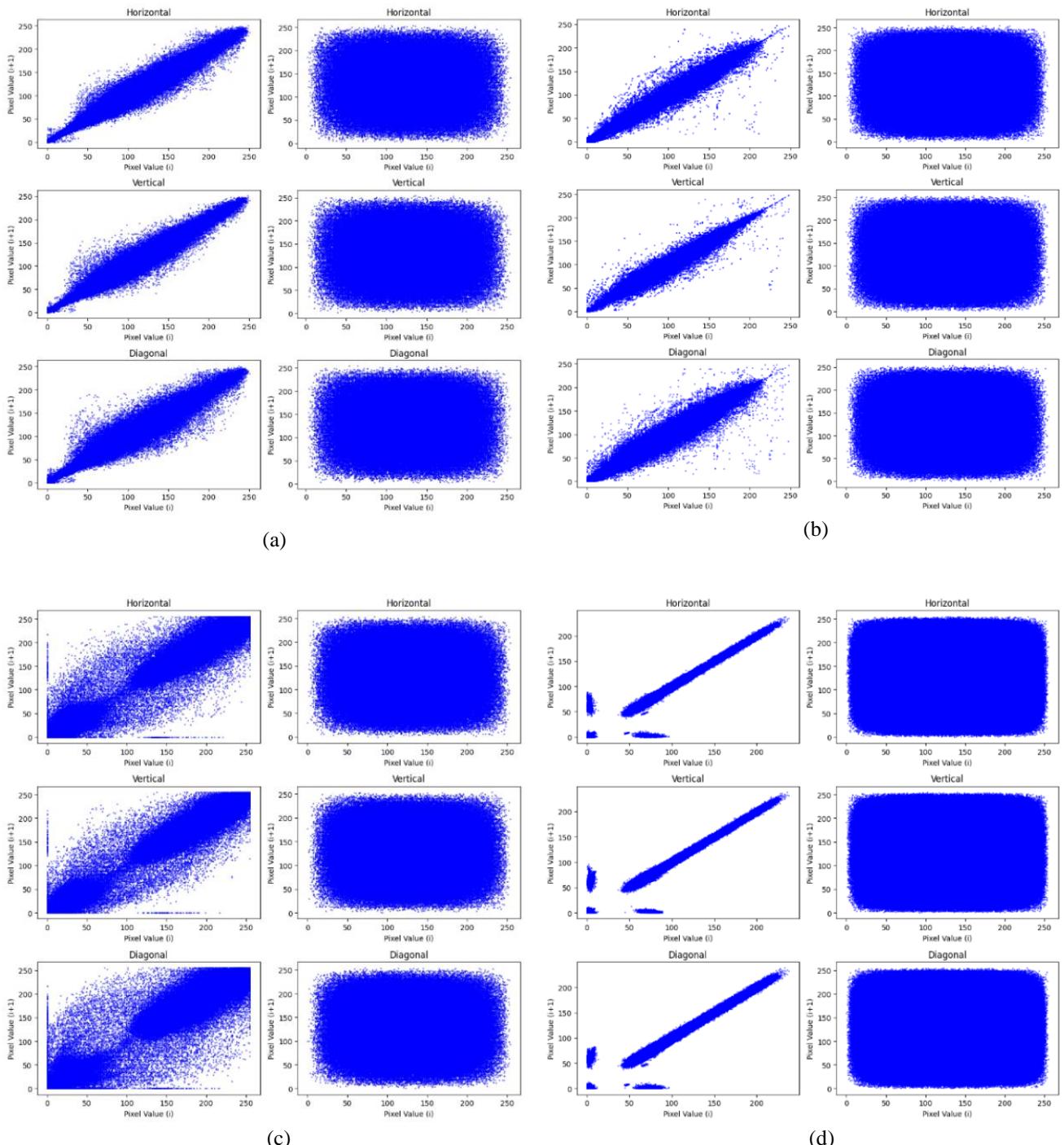
Figure. 2 Correlation analysis in all directions, 1st line correlation of original image, 2nd line correlation of encrypted image: (a) correlation sample 1, (b) correlation sample 2, (c) correlation sample 3, and (d) correlation sample 4

recipient using AES or RSA. Consequently, the decryption is independent of the regeneration of keys from chaotic parameters or information.
Consequently, conventional key sensitivity analysis is inapplicable. Small changes in chaotic parameters or metadata have no influence on decryption accuracy, as the precise keys are transmitted immediately. This method enhances system stability,

prevents decryption failures caused by rounding mistakes or metadata discrepancies, and streamlines the receiver's architecture by eliminating the need for key regeneration.

5.10   Execution time analysis

Both excellent security performance and rapid speed are necessary for an effective encryption

Table 4. PSNR and MSE between the original and decrypted image
(for all four ways to encrypted image proposed)

Images	PSNR	MSE
Sample 1	∞	0
Sample 2	∞	0
Sample 3	∞	0
Sample 4	∞	0

Table 5. The measure results for (UACI, NPCR, MSE, PSNR, Entropy encrypted image)

Measure	Images	Logistic +Resnet	Logistic +Mobilenet	Loranz +Resnet	Loranz +Mobilenet	Logistic	Loranz
UACI	Sample 1	33.5588	33.6085	33.5856	33.5939	33.509	33.5725
	Sample 2	28.8845	28.7269	28.8157	28.8133	28.8341	28.8310
	Sample 3	33.9182	33.7264	33.7579	33.7599	33.8657	33.7528
	Sample 4	39.4001	39.3327	39.3110	39.3113	36.3152	39.3571
NPCR	Sample 1	99.615	99.6138	99.6096	99.609	99.5963	99.6034
	Sample 2	99.6149	99.6113	99.6155	99.6095	99.6116	99.6154
	Sample 3	99.6162	99.6035	99.6067	99.6080	99.6125	99.6100
	Sample 4	99.6024	99.6115	99.6061	99.6027	99.4507	99.6110
MSE	Sample 1	10954.3304	10974.5847	11049.4144	10976.8830	10939.1760	10992.7339
	Sample 2	7870.0591	7943.2164	7895.3863	7883.1200	7889.1150	7892.1013
	Sample 3	11190.0849	11101.6739	11113.4993	11116.4142	11168.9102	11111.2496
	Sample 4	14816.6820	14727.6796	14735.2049	14739.7167	13421.6902	14769.2028
PSNR	Sample 1	7.72	7.71	7.72	7.71	7.74	7.72
	Sample 2	9.15	9.18	9.16	9.16	9.16	9.16
	Sample 3	7.64	7.68	7.67	7.67	7.65	7.67
	Sample 4	6.42	6.45	6.45	6.45	6.85	6.44
Entropy-encrypted image	Sample 1	7.9995	7.9996	7.9997	7.9996	7.9991	7.9997
	Sample 2	7.9998	7.9998	7.9999	7.9999	7.9998	7.9999
	Sample 3	7.9999	7.9999	8.0000	8.0000	7.9999	8.0000
	Sample 4	7.9997	7.9995	7.9998	7.9998	7.0619	7.9998

Table 6. Correlation coefficients for encrypted images

Measure	Images	Logistic +Resnet	Logistic +Mobilenet	Loranz +Resnet	Loranz +Mobilenet	Logistic	Loranz
Horizontal Corr. Coef.	Sample 1	0.0002	0.0013	0.002	-0.0027	0.1442	0.0026
	Sample 2	0.0009	0.0022	-0.0011	-0.0001	0.0026	-0.0001
	Sample 3	-0.0019	0.0075	-0.0011	-0.0003	0.0060	-0.0003
	Sample 4	0.0010	-0.0003	0.0001	-0.0013	0.8428	0.0008
Vertical Corr. Coef.	Sample 1	-0.0015	-0.0038	0.0015	-0.0015	-0.0008	-0.0020
	Sample 2	-0.0021	0.0031	-0.0018	-0.0008	0.0005	0.0003
	Sample 3	-0.0001	-0.0004	0.0002	0.0003	-0.0006	0.0013
	Sample 4	-0.0001	0.0003	-0.0025	-0.0002	0.2421	0.0001
Diagonal Corr. Coef.	Sample 1	-0.0036	-0.0015	0.0009	0.0022	-0.0005	-0.0018
	Sample 2	-0.0008	0.0022	-0.0011	-0.001	-0.0026	-0.0001
	Sample 3	-0.0007	-0.0001	-0.0009	0.0006	0.0002	-0.0001
	Sample 4	-0.0024	-0.0010	0.0006	0.0004	0.2399	0.0013

solution. To evaluate the efficacy of the suggested strategy, we conducted a speed study utilising Python 3.12.4 on a PC Windows 11 Pro 64-bit operating system with 11th Gen Intel® Core ™ i7-11800H @ 2.30GHz (16 CPUs), ~2.3GHz, and 16.384 GB of RAM. Table 2 presents the average execution time of the proposed encryption technique for images of varying sizes. The experimental findings shown in Table 2 demonstrate the linear complexity of the suggested encryption technique.

The proposed method's execution time is slightly longer than [18], [13], [17] Consequently, the suggested approach may ensure system performance while also achieving quicker encryption speeds.

6. Robustness against attacks

We now delineate the subsequent prevalent danger situations and elucidate how our methodology handles each one.

- Brute-force attack: Our method produces encryption keys using a high-dimensional chaotic system shaped by metadata and deep learning results. The key space is projected to surpass 2^{128}, making brute-force attacks impractical.
- Known-plaintext attack: The use of metadata-dependent keys results in the same plaintext generating distinct ciphertexts under varying situations. The irreusability of keys renders known-plaintext assaults useless.
- Chosen-plaintext attack: We emulate an assailant encrypting meticulously designed graphics. Our system generates very sensitive reactions owing to its chaotic configuration. The avalanche effect guarantees that little alterations in input produce significant changes in the ciphertext.
- Noise attacks: Our suggested encryption approach is quite resistant to noise assaults, as shown by the perceptual quality assessments in Table 4. The robustness of our algorithms is clearly shown by their continuously low PSNR values (below 10), and strong MSE.
- Differential attacks: Evidenced by UACI values larger than 36.3% and NPCR values greater than 99.62%, our encryption approach is resilient against differential attacks.

Table 3. Show the histogram of both the original and encrypted images in all channels.

Fig. 2 Show correlation analysis in all directions for the original and encrypted images.

Tables 4, 5, and 6 show the results of testing the proposed method (4 ways) using images of different sizes and colors.

Table 7. Comparisons based on several criteria

Images	Methods	UACI	NPCR	MSE	PSNR	Entropy-encrypted image	Horizontal Corr. Coef.	Vertical Corr. Coef.	Diagonal Corr. Coef.
	Ref.[18]	33.4388	99.62	13060	6.9713	7.9998	0.0006	-0.00018	0.00044
	Logistic +Resnet	35.9933	99.6019	12562.7240	7.14	7.9986	-0.0071	-0.0033	0.0032
	Logistic +Mobilenet	35.8011	99.6225	12452.4592	7.18	7.9988	-0.0006	0.0009	-0.0075
	Loranz +Resnet	35.8503	99.5940	12467.9548	7.17	7.9989	-0.0006	0.0049	-0.0002
	Loranz +Mobilenet	35.8221	99.6079	12461.0620	7.18	7.9989	0.0073	0.0019	-0.0006
	Ref.[1]	33.4062	99.603	-	-	7.9943	0.0068	-0.0136	0.0045
	Logistic +Resnet	30.2331	99.6133	8856.9724	8.66	7.9980	0.0032	-0.0051	-0.0011
	Logistic +Mobilenet	30.4678	99.5765	8953.8537	8.61	7.9982	-0.0040	0.0091	-0.0021
	Loranz +Resnet	30.4423	99.6209	8944.4058	8.62	7.9982	-0.0032	-0.0049	0.0019
	Loranz +Mobilenet	30.4453	99.5907	8935.1867	8.62	7.9983	-0.0048	0.0002	-0.0027
	Ref.[17]	33.39	99.61	-	-	7.9994	-0.0145	0.0070	-0.0184
	Logistic +Resnet	35.5081	99.6246	12224.8234	7.26	7.9987	-0.0025	-0.0056	-0.0030
	Logistic +Mobilenet	35.3381	99.5940	12174.1880	7.28	7.9988	0.0036	0.0004	0.0038
	Loranz +Resnet	35.3718	99.6183	12173.6363	7.28	7.9987	-0.0013	-0.0012	-0.0012
	Loranz +Mobilenet	35.4324	99.6420	12202.3892	7.27	7.9989	-0.0041	0.0042	-0.0002
	Ref.[18]	33.5044	99.61	8935.8	8.6195	7.9997	0.0006	-0.00018	0.00044
	Logistic +Resnet	30.6419	99.6178	9055.7139	8.56	7.9996	-0.0024	0.0020	0.0009
	Logistic +Mobilenet	30.4229	99.6159	8927.7541	8.62	7.9997	0.0011	0.0004	0.0021
	Loranz +Resnet	30.4630	99.6011	8954.3779	8.61	7.9998	-0.0002	0.0010	0.0006
	Loranz +Mobilenet	30.4603	99.6142	8955.1980	8.61	7.9998	-0.0019	-0.0001	0.0004

Table 7. Compare the results of implementing UACI, NPCR, MSE, PSNR, entropy, and correlation coefficient distributions in the Horizontal, vertical, and diagonal directions with the results of other techniques.

Four techniques were evaluated to determine the resilience of the proposed encryption scheme. The objective was to assess the impact of various chaotic systems and deep learning models on encryption efficacy. After examining the testing findings in Tables 4, 5, and 6, it was determined that the setup using the Logistic Map with ResNet-18 attained the highest overall performance. This indicates that the integration of a lightweight chaotic system with a deep residual network is ideal for producing resilient encryption keys.

In comparison with current methodologies, it indicates that they depend on static key configurations or immutable chaotic systems devoid of image-dependent randomisation, rendering them susceptible to key reutilization and chosen-plaintext attacks. Our approach uniquely combines metadata-driven dynamic key generation with deep learning-enhanced chaos parameter optimisation, guaranteeing image-specific encryption and enhancing key unpredictability. Results indicate that metadata-guided models provide enhanced NPCR, UACI, and other metrics, confirming the efficacy of this hybrid approach.

7. Conclusion

This research introduced an innovative approach to encrypting medical images by combining deep learning with chaotic systems. The proposed technique employs metadata-driven key generation, whereby a trained deep neural network retrieves important chaotic parameters from image information. This guarantees that every image produces a distinct encryption key, so as to avert key reuse and augment resilience against known-plaintext and statistical attacks.

Theoretically, the amalgamation of chaos theory, characterized by its sensitivity to initial conditions and unpredictability, with deep learning allows dynamic, context-sensitive key generation. This approach enhances entropy and guarantees uncorrelated cypher images, even for visually similar inputs, in contrast to fixed-key systems. The method utilises the extensive key space generated by double-precision parameters and neural models, rendering brute-force assaults computationally impractical.

Among all assessed configurations, the Logistic Map with ResNet-18 had the superior performance, indicating it as the most appropriate model for safe medical image encryption within this framework. Empirical findings corroborate the theoretical assertions, with NPCR above 99.62%, UACI surpassing 36.3%, PSNR below 10, and elevated MSE values, indicating robust confusion and diffusion characteristics. The technology has a theoretical key space of 2^{133120} for 128×128 images with scalability for increased resolutions.

This study introduces novel avenues for integrating machine learning with chaos-based encryption in secure medical imaging, and possibly in other formats such as audio and video data. Additional theoretical investigation is recommended to officially characterise the security assurances provided by neural-chaotic key generation.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The first author executed conceptualization, methodology, software development, formal analysis, resource management, data curation, and the creation of the original draft. The second and third writers were accountable for monitoring and project management.

Acknowledgments

References

[1] S. Das and M. K. Sanyal, "Medical image encryption using 3D unified chaotic system and dynamic DNA coding", *Research Square*, 2022, doi: 10.21203/rs.3.rs-2244229/v1.

[2] S. Dash, S. Padhy, B. Parija, T. Rojashree, and K. A. K. Patro, "A Simple and Fast Medical Image encryption System Using Chaos-Based Shifting Techniques", *International Journal of Information Security and Privacy*, Vol. 16, No. 1, 2022, doi: 10.4018/IJISP.303669.

[3] Z. Liu, J. Li, Y. Ai, Y. Zheng, and J. Liu, "A robust encryption watermarking algorithm for medical images based on ridgelet-DCT and THM double chaos", *Journal of Cloud Computing*, Vol. 11, No. 1, 2022, doi: 10.1186/s13677-022-00331-4.

[4] T. S. Ali and R. Ali, "A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map", *IEEE Access*, Vol. 8, pp. 71974-

71992, 2020, doi: 10.1109/ACCESS.2020.2987615.

[5] S. T. Allawi and Y. H. Alagrash, "A New Image Encryption Method Combining the DNA Coding and 4D Chaotic Maps", *International Journal of Intelligent Engineering and Systems*, Vol. 18, No. 1, pp. 860-873, 2025, doi: 10.22266/ijies2025.0229.61.

[6] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, B. V. Elsevier, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", *Procedia Computer Science*, pp. 617-624, 2016, doi: 10.1016/j.procs.2016.02.108.

[7] A.-G. T. Al-Tamimi, B. Abduh, and M. Aljafary, "Security and Performance Analysis of Chaos-based Image Encryption Schemes", 2022.

[8] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, "Noise-Resistant Image Encryption Scheme for Medical Images in the Chaos and Wavelet Domain", *IEEE Access*, Vol. 9, pp. 59108-59130, 2021, doi: 10.1109/ACCESS.2021.3071535.

[9] Q. Zhang, Y. Yan, Y. Lin, and Y. Li, "Image Security Retrieval Based on Chaotic Algorithm and Deep Learning", *IEEE Access*, Vol. 10, pp. 67210-67218, 2022, doi: 10.1109/ACCESS.2022.3185421.

[10] M. Abadi et al, "Deep learning with differential privacy", In: *Proc. of the ACM Conference on Computer and Communications Security, Association for Computing Machinery*, 2016, pp. 308-318. doi: 10.1145/2976749.2978318.

[11] H. Wijayanto, S. Sinar, N. Surakarta, Y. Prayudi, and I. Riadi, "Encryption EXIF Metadata for Protection Photographic Image of Copyright Piracy", Hendro Wijayanto et al, *IJRCCT*, Vol. 5, No. 5, 2016.

[12] K. Malik Mohamad and M. Mat Deris, "Visualization of JPEG Metadata", 2009.

[13] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems", *IEEE Access*, Vol. 7, pp. 38507-38522, 2019, doi: 10.1109/ACCESS.2019.2906052.

[14] S. Ibrahim and A. Alharbi, "Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography", *IEEE Access*, Vol. 8, pp. 194289-194302, 2020, doi: 10.1109/ACCESS.2020.3032403.

[15] P. Parida, C. Pradhan, X. Z. Gao, D. S. Roy, and R. K. Barik, "Image Encryption and Authentication with Elliptic Curve Cryptography and Multidimensional Chaotic Maps", *IEEE Access*, Vol. 9, pp. 76191-76204, 2021, doi: 10.1109/ACCESS.2021.3072075.

[16] I. Khalid, T. Shah, S. M. Eldin, D. Shah, M. Asif, and I. Saddique, "An Integrated Image Encryption Scheme Based on Elliptic Curve", *IEEE Access*, Vol. 11, pp. 5483-5501, 2023, doi: 10.1109/ACCESS.2022.3230096.

[17] A. A. Abdul-Kareem and W. A. M. Al-Jawher, "A Hybrid Domain Medical Image Encryption Scheme Using URUK and WAM Chaotic Maps with Wavelet - Fourier Transforms", *Journal of Cyber Security and Mobility*, Vol. 12, No. 4, pp. 435-464, 2023, doi: 10.13052/jcsm2245-1439.1241.

[18] A. A. El Qassime, H. Nhaila, and L. Bahatti, "Enhancing the Security and Efficiency of Biomedical Image Encryption through a Novel Hyper-Chaotic Logistic Map", *International Journal of Intelligent Engineering and Systems*, Vol. 17, No. 5, pp. 334-349, 2024, doi: 10.22266/ijies2024.1031.27.

[19] T. R. Ningthoukhongjam, S. Devi Heisnam, and M. Singh Khumanthem, "Medical Image Encryption Through Chaotic Asymmetric Cryptosystem", *IEEE Access*, Vol. 12, pp. 73879-73888, 2024, doi: 10.1109/ACCESS.2024.3404088.

[20] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges", 2023, MDPI. doi: 10.3390/math11112585.

[21] J. Leonel Rocha and A. K. Taha, "Allee's Effect Bifurcation in Generalized Logistic Maps", *International Journal of Bifurcation and Chaos*, Vol. 29, No. 3, 2019, doi: 10.1142/S0218127419500391.

[22] "04 - Simple Mathematical Models".

[23] M. Abadi et al, "Deep learning with differential privacy," In: *Proc. of the ACM Conference on Computer and Communications Security, Association for Computing Machinery*, pp. 308-318 2016. doi: 10.1145/2976749.2978318.

[24] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition", In: *Proc. of IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, pp. 770-778, 2016.

[25] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L.-C. Chen, "MobileNetV2: Inverted residuals and linear bottlenecks", In: *Proc. of IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, pp. 4510-4520 2018.

[26] R. Sood and H. Kaur, "A Literature Review on RSA, DES and AES Encryption Algorithms", *Emerging Trends in Engineering and Management, Soft Computing Research Society*,

pp. 57-63 2023. doi: 10.56155/978-81-955020-3-5-07.

[27] D. M. Alsaffar, A. S. Almutiri, B. Alqahtani, R. M. Alamri, H. F. Alqahtani, N. N. Alqahtani, G. M. Alshammari, and A. A. Ali, "Image Encryption Based on AES and RSA Algorithms", In: *Proc. of 2020 Int. Conf. on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, pp. 1-5, 2020. doi: 10.1109/ICCAIS48893.2020.9096809.

[28] X. Wang, Y. Peng, L. Lu, Z. Lu, M. Bagheri, and R. M. Summers, "ChestX-ray8: Hospital-scale chest X-ray database and benchmarks on weakly-supervised classification and localization of common thorax diseases", In: *Proc. of IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, Honolulu, HI, USA, pp. 2097-2106, 2017.

[29] J. Staal, M. D. Abràmoff, M. Niemeijer, M. A. Viergever, and B. Van Ginneken, "Ridge-based vessel segmentation in color images of the retina", *IEEE Trans Med Imaging*, Vol. 23, No. 4, pp. 501-509, 2004, doi: 10.1109/TMI.2004.825627.

[30] P. Mooney, "Chest X-Ray Images (Pneumonia)". Accessed: 2025. [Online]. Available: https://www.kaggle.com/datasets/paultimothy mooney/chest-xray-pneumonia

[31] M. Nickparvar, "Brain Tumor MRI Dataset". Accessed: 2025. [Online]. Available: https://www.kaggle.com/datasets/masoudnickp arvar/brain-tumor-mri-dataset

[32] B. V Nair, V. V S, S. S. Muni, and A. Durdu, "Deep Learning and Chaos: A combined Approach To Image Encryption and Decryption", *arXiv Preprint, arXiv:2406.16792*, 2024.

[33] N. Iqbal, S. Abbas, M. A. Khan, T. Alyas, A. Fatima, and A. Ahmad, "An RGB Image Cipher Using Chaotic Systems, 15-Puzzle Problem and DNA Computing", *IEEE Access*, Vol. 7, pp. 174051-174071, 2019, doi: 10.1109/ACCESS.2019.2956389.

[34] S. T. Allawi and D. R. Alshibani, "Color image encryption using LFSR, DNA, and 3D chaotic maps", *Int. J. Electr. Comput. Eng. Syst.*, Vol. 13, No. 10, pp. 885-893, 2022.

[35] M. Lawnik, L. Moysis, and C. Volos, "Chaos-Based Cryptography: Text Encryption Using Image Algorithms", *Electronics (Switzerland)*, Vol. 11, No. 19, 2022, doi: 10.3390/electronics11193156.

[36] R. A. Mohammed, M. A. A. Khodher, and A. Alabaichi, "Image Encryption in IOT Using Hyper-chaotic System", *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 6, pp. 101-112, 2023, doi: 10.22266/ijies2023.1231.09.

[37] I. A. Taqi and M. G. Abdul-Haleem, "An Efficient Cryptosystem for Image Using 1D and 2D Logistic Chaotic Maps", *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 4, pp. 125-136, 2023, doi: 10.22266/ijies2023.0831.11.

[38] A. A. El Qassime, H. Nhaila, and L. Bahatti, "Enhancing the Security and Efficiency of Biomedical Image Encryption through a Novel Hyper-Chaotic Logistic Map", *International Journal of Intelligent Engineering and Systems,* Vol. 17, No. 5, pp. 334-349, 2024, doi: 10.22266/ijies2024.1031.27.

[39] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", *Chaos Solitons Fractals*, Vol. 21, No. 3, pp. 749-761, 2004, doi: 10.1016/j.chaos.2003.12.022.

[40] E. Barker, "Recommendation for key management", *Gaithersburg*, *MD*, 2020, doi: 10.6028/NIST.SP.800-57pt1r5.

[41] L. E. Bassham et al, "A statistical test suite for random and pseudorandom number generators for cryptographic applications", *Gaithersburg, MD*, 2010, doi: 10.6028/NIST.SP.800-22r1a.