# Lightweight Medical Image Encrypting and Decrypting Algorithm Based on the 3D Intertwining Logistic Map

Hadjer Bourekouche[1],*, Samia Belkacem[2] and Noureddine Messaoudi[1]

[1]*LIST Laboratory, Department Engineering of Electrical Systems, Faculty of Technology, University M'Hamed Bougara of Boumerdes, 35000 Boumerdes, Algeria.*

[2]*LIMOSE Laboratory, Department Engineering of Electrical Systems, Faculty of Technology University M'Hamed Bougara of Boumerdes, 35000 Boumerdes, Algeria.*

## Abstract

The quantity of medical image data accessible for analysis is increasing because of advancements in telehealth services. Therefore, effective cryptographic solutions must be developed to prevent data manipulation by unauthorized users in insecure networks. This paper focuses on developing a lightweight symmetric cryptosystem algorithm with decreasing memory and power consumption at high speed for standard and medical images based on 3D intertwining logistic map-cosine (ILM-cosine), which is a powerful chaotic system in contemporary cryptography. The motivation of this paper is to reduce the memory space required for storing program data while minimizing execution time for lower implementation complexity in telehealth applications. Our proposed scheme consists of five main steps: ILM-cosine map key generation with histogram normalization, row rotation, column rotation, and exclusive-OR (XOR) logic operation. Various normal and medical images were used as samples for the simulation. The results showed that cipher images have good visual quality, high information entropy, large key space, and low computational complexity.

## Keywords

Telehealth, cryptosystem, memory, ILM cosine, chaotic map, key space.

## 1. Introduction

In medical systems, patient data are increasingly stored in cloud-based Internet-of-Health (IoHS) systems. Therefore, these devices can be accessed remotely at various facilities/locations. The data, which included sensitive and highly confidential images, were treated as crucial information. Hence, important criteria, including confidentiality, validity, and integrity, are required for the transmission and storage of medical data using the IoHS.

Medical imaging is a valuable tool for providing patients with excellent care, because it can be used for both diagnosis and therapy. Medical imaging methods are categorized into structural and functional imaging categories, according to the type of information they offer about the organ being studied. Magnetic resonance imaging (MRI), computed tomography (CT), ultrasound, positron emission tomography (PET), single-photon emission computed tomography (SPECT), magnetic resonance angiography (MRA), contrast-enhanced MRI (CT-MRI), functional MRI (fMRI), magnetic resonance spectroscopy (MRS), and electrocardiography (ECG) were performed.

To provide information security services, a cryptosystem implements cryptographic techniques and supporting infrastructure. A cipher system is another term used in cryptosystems. A basic cryptosystem is composed of several parts, including plaintext, an encryption algorithm, an encryption key, a decryption algorithm, and ciphertext. A multitude of security objectives are provided by medical image cryptography to guarantee data privacy, nonalteration, and other concerns. The following are some of the objectives of cryptography: Only an authorized person is allowed to change the information that has been transmitted. No one between the sender and receiver can change the message sent.

The primary elements of the medical image encryption lifecycle in healthcare are as follows: The first stage is data collection, which is used to submit patient physiological data and share medical information. In the next step, the data must be filtered, classified, and subjected to any changes required for use in a relevant study. These data are often compressed using a lossless compression strategy with less processing and a greater compression ratio to minimize the volume of medical data and enhance transmission performance. However, the data gathered may have included sensitive information. Consequently, it is critical to create handling, storage, and disposal requirements that include security during the data lifecycle[1]. At this stage, the data are vulnerable to a range of assaults, such as distributed/denial-of-service attacks, content-based attacks, and attacks on new networks. Consequently, by retaining access-level security

*6th International Hybrid Conference On Informatics And Applied Mathematics, December 6-7, 2023 Guelma, Algeria*

*Corresponding author.
h.bourekouche@univ-boumerdes.dz (H. Bourekouche); s.belkacem@univ-boumerdes.dz (S. Belkacem); n.messaoudi@univ-boumerdes.dz (N. Messaoudi)
0000-0003-3516-290X (H. Bourekouche); 0000-0003-0912-3392 (S. Belkacem); 0000-0002-3406-4120 (N. Messaoudi)

and access control with symmetric encryption, the data will remain segregated and strictly guarded. In chaos-based image encryption, a chaotic system [2] is used to generate random chaotic sequences that can be used as secret keys for the permutation and diffusion phases. Permutation is an alteration of the bit order according to an algorithm. During the confusion stage, each pixel must normally be shifted at least once. Following data collection, transformation, and storage in secure storage systems, a data processing analysis is performed to provide relevant knowledge that may be used for decryption in a manner similar to encryption.

When implementing encryption algorithms for telehealth applications, lower implementation complexity should be guaranteed, which is the motivation of our work, where we aim to reduce the memory space required for storing program data while minimizing the execution time. Hence, we develop a fast chaos-based encryption technique that can encrypt medical images in five steps: generation of a random number by using the intertwining 3D logistic-cosine map, normalization, pixel rotation through which row and column rotation is performed, and the XOR-based encryption technique. The proposed scheme can encrypt a $256 \times 256$ medical image in less than 0.4 seconds and can be used in stringent medical applications.

The remainder of this paper is organized as follows. Section 2 introduces the theoretical background of the chaos map used for key- generation. Section 3 reviews the related work. Section 4 describes the medical- image encryption technique. Section 5 presents the simulation results and security analysis. Section 6 discusses and compares our results with those of recent schemes. Finally, Section 7 concludes the study.

## 2. Related Works

Digital images are multimedia data that contain confidential information in the medical field. The challenge lies in creating an effective, secure cryptosystem that can safeguard shared private images. Thus, several researchers have designed chaos-based symmetric cryptosystem algorithms for both standard and medical- image encryption. These methods frequently make use of chaos maps, including the Lorenz and Chen system, Arnold, logistic maps, and cat maps. To assess the state of the art, we selected published research performed mainly from 2018 to 2023.

### 2.1. Schemes based on chaotic maps

The hybrid chaotic model proposed by John and Kumar[3] uses a 2D Lorentz chaotic model coupled with a logistic chaotic model for the encryption/decryption of medical Digital Imaging and Communications DICOM CT images[4]. Prior to encryption, a median filter was used to scramble the rows and columns of the image, and a bitwise XOR operation was performed to generate the encrypted image [4].

Ahmed et al.[5] present an innovative image encryption approach for medical imaging. This method uses a four-dimensional (4D) hyperchaotic map[5] to construct four substitution boxes (S-boxes). The key benefit of this new approach is its sensitivity to threats, which makes it extremely secure. The encryption process begins with a three-dimensional (3D) Chen map shuffling of a plain image. This was followed by dividing the image into four subimages. The final stage entails replacing the pixel values in each subimage with values from one of the four S-boxes. In the first stage, the four subimages are merged, followed by fusion of the combined image using a one-dimensional (1D) logistic map[5].

Sarosh et al.[6] proposed a quick chaos-based encryption method for medical images. To confuse and disperse medical images. The method uses a logistic map, Chebyshev map, and piecewise linear chaotic map (PWLCM). The image was first circularly shifted, and then, bit-plane slicing was performed. A plane is created by performing an XOR operation on the most significant bit (MSB) and seventh ISB plane MSB plane. The final image was jumbled using a pseudorandom number (PRN) produced by the logistic map. The plan is adaptive and computes image parameters, such as the sum or mean, to establish the initial conditions of the PWLCM chaotic map. The scrambled image was XORed using the key image produced by the PWLCM. A Chebyshev map is iterated, and a PRN sequence is formed to permute the image pixels and produce the final encrypted image[6].

Jain et al.'s [7] novel chaotic image encryption method for medical images guarantees increased chaos and randomness of the encrypted data, protecting it from crypt-analysis and other statistical attacks. Arnold's cat map and the 2D logistic sine-coupling map (2DLSCM) are combined into one algorithm. The iterative transformation algorithm, known as Arnold's cat map, randomly distributes the pixels of the input image. The number of iterations, which is sometimes referred to as the period, determines the final image. After a certain number of iterations, the original image is completely reconstructed. Compared to other 2D chaotic maps, 2DLSCM guarantees greater complexity and ergodicity.

A Hermite chaotic neural- network-based medical- image encryption algorithm was proposed by Han et al.[8]. First, chaotic sequences of the logistic map are used in the medical- image encryption algorithm. Second, a Hermite chaotic neural network is trained using this chaotic sequence. Two key streams created by the trained Hermite chaotic neural network are subsequently used to encrypt medical images [9].

### 2.2. Schemes based on chaos and DNA

The authors of [10] provided a cryptosystem with a unique encoding scheme and a lossless compression method. Chaos-based DNA cryptography has been used to enhance the security of medical images. A lossless discrete Haar wavelet transform was employed to reduce the transmission efficiency in terms of both space and time. The binary image created from the compressed image is then separated into four smaller images. By employing a 4D Lornez chaotic map to construct chaotic sequences, the subimage pixels are scrambled. The DNA coding instructions were used to create four distinct DNA structures. The XOR technique is used to combine DNA structures, and after DNA decoding, a cipher image is acquired. Based on cryptanalysis, the proposed cryptographic system is secure against differential, exhaustive, and statistical attacks. The proposed cryptosystem can be used for telemedicine and e-health applications.

Abdelfatah et al.[11] proposed a medical image encryption technique based on adaptive deoxyribonucleic acid (DNA) and a novel multi chaotic map (HGL) created by combining Henon, Gaussian, and logistic maps. Using adaptive DNA, each image is encrypted with a different DNA rule than the other images, making the proposed algorithm effective against attackers' perceptions.

Amdouni et al.[12] discussed the use of chaos and DNA as encryption methods for digital medical images. The Rossler and Lorenz systems were used to generate a random key stream. The key and input original images were then encoded using DNA encoding principles. The scheme was evaluated using National Institute of Standards and Technology (NIST) suite tests. The Zedboard Development Kit implements the hardware design of the proposed scheme.

### 2.3. Schemes based on chaos and cellular automata

Choi et al.[13] proposed a secure and dependable color medical image encryption algorithm based on a nonlinear cellular automaton (NCA) and a generalized 3D chaotic cat map[13]. NCA, a group cellular automaton created by fusing two nonlinear CAs and a maximum length CA (MLCA), which possesses nonlinearity and expands the key space, is an efficient pseudorandom number generator (PRNG)[13]. Pixel values of a basic image may be unfeasible. In addition, they employed a generalized 3D chaotic cat map for effective color medical image encryption shuffling. The R, G, and B channels of the pixels in a color image can be moved using this map. The proposed technique conducts a full experimental test through in-depth analysis to demonstrate the high security and dependability of the new color medical image encryption system.

### 2.4. Schemes based on chaos and the genetic algorithm

Nematzadeh et al.[14] presented a hybrid technique based on a coupled lattice map and modified genetic algorithm for the encryption of medical images. The first population of the modified genetic algorithm was created using a coupled lattice map. Consequently, the cipher images were of higher quality, and this approach was also more resistant to attacks. The significantly shorter execution time of the proposed method compared to that of prior evolutionary algorithm-based image encryption techniques is another significant accomplishment. This was because of the method chosen to design the GA.

## 3. Basic requirement and definitions

The principles of logistic maps (LMs), intertwining logistic maps (ILMs), and ILM-cosine, which were used to produce keys for the proposed picture encryption scheme, are annotated in this section.

### 3.1. Logistic Map

The one-dimensional logistic function provided by equation 1 is a discrete recursive relation of degree two. The popularity of these maps can be attributed to their ease of use.

$$x_{i+1} = rx_i(1 - x_i) \tag{1}$$

$x_i$ varies in (0, 1], and $r$ exhibits chaotic behavior in [3.57, 4].

### 3.2. 3-Dimensional logistic map

A 3D logistic map with superior chaotic properties compared with a 1D logistic map has recently been investigated. The following equation 2 serves as the definition.

$$\begin{cases} x_{i+1} = \gamma(1 - x_i) + \beta(y_i^2 x_i) + \alpha z_i^3 \\ y_{i+1} = \gamma(1 - y_i) + \beta(z_i^2 y_i) + \alpha x_i^3 \\ z_{i+1} = \gamma(1 - z_i) + \beta(x_i^2 z_i) + \alpha y_i^3 \end{cases} \tag{2}$$

This system of equations exhibits chaotic behavior in $3.53 < \gamma < 3.81, 0 < \beta < 0.022, 0 < \alpha < 0.015$ [15].

### 3.3. Intertwining logistic map (ILM)

In 2014, Wang and Xu [16] proposed an intertwining relation between different LM sequences[17], which indicates that the ILM has more dynamic behavior than the LM[17]. The equations for the ILM sequence are as follows[17]:

$$\begin{cases} x_{i+1} = (\eta\sigma y_i(1-x_i)+z_i) \mod 1 \\ y_{i+1} = (\eta\vartheta y_i + z_i(1+x_{i+1}^2)) \mod 1 \\ z_{i+1} = (\eta(y_i+1+x_i+1+\kappa)\sin z_i) \mod 1 \end{cases} \tag{3}$$

This system of equations exhibits chaotic behavior for $\eta$ in the range of [0, 4), $\eta > 33.5$, $\vartheta > 37.9$, and $\kappa > 35.7$.

### 3.4. Intertwining Logistic Map-Cosine (ILM-Cosine)

The ILM-cosine expressed by equation 4 is the result of combining the ILM with a cosine function with the aim of improving the ILM output nonlinearity. This system of equations exhibits chaotic behavior when $\eta$ is in the range of [0, 4), $\sigma > 33.5$, $\vartheta > 37.9$ , and $\kappa > 35.7$.

$$\begin{cases} x_{i+1} = \cos\left((\eta\sigma y_i(1-x_i)+z_i) \mod 1 + \vartheta\right) \\ y_{i+1} = \cos\left((\eta\vartheta y_i + z_i(1+x_{i+1}^2)) \mod 1 + \vartheta\right) \\ z_{i+1} = \cos\left((\eta(y_i+1+x_i+1+\kappa)\sin z_i) \mod 1 \right. \\ \left. +\vartheta\right) \end{cases} \tag{4}$$

## 4. Proposed cryptosystem

The widespread use of medical image encryption based on chaotic maps has increased in recent years, due to the notable nonlinear features of chaos that make it an appropriate candidate for medical cryptographic applications. In this section, we present a detailed medical image encryption technique. The proposed image encryption scheme based on the ILM-cosine is shown in Figure 1. To create a cryptosystem strong enough to encrypt medical images, the following five crucial procedures are needed:

### 4.1. Key generation

In this step, we use equation 4 to generate a pseudo-random bit sequence based on the 3D ILM-cosine chaos sequences. The initial conditions and parameter values are considered keys to the cryptosystem.

$x(1) = 0.2350, y(1) = 0.3500, z(1) = 0.7350, \eta = 3.7700, \sigma = 33.6, \vartheta = 39.69, \kappa = 36.58$.

### 4.2. Histogram normalization

The generated values and histogram generation of the 3D ILM-cosine chaotic sequence $x$, $y$, and $z$ obtained using equation 4 are depicted in Figure 2a. The resulting chaotic sequence histogram has a nonuniform distribution, which may affect the security of the system. Consequently, we use a normalizing (equalization) technique for $x$, $y$, and $z$ using equation 5 to further strengthen the security of the resulting histograms by a sufficiently large number because the map only generates floating-point values between 1 and -1.

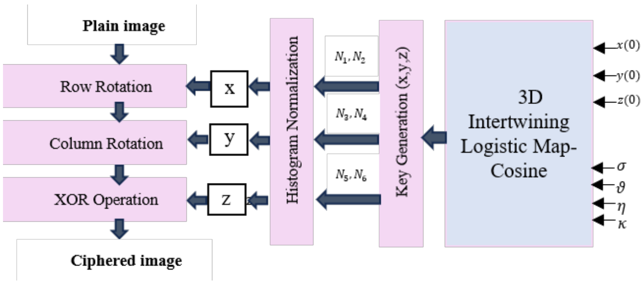


**Figure 1:** Encryption steps based on 3D Intertwining LM-Cosine.

$$\begin{cases} x = int(x \times N_1) \mod N \\ y = int(y \times N_3) \mod M \\ z = int(z \times N_5) \mod 256 \end{cases} \tag{5}$$

where $N_1$, $N_3$ and $N_5$ are large random numbers that are chosen to be equal to or greater than 100,000 for simplicity, while M and N are chosen to be equal to the image dimension (256 × 256). It is clear from Figure 2b that after applying the above constraints, we obtain an equalized histogram for $x$, $y$, and $z$.

### 4.3. Row rotation

The steps used to rotate a gray image of $M \times N$ dimensions are as follows:

- Applying an offset value $N_2$,
- Choosing$M$ elements of the chaos sequence$x$ starting from the offset value $N_2$,
- The chaos value, $x$, obtained using equation5 is used to rotate the row.

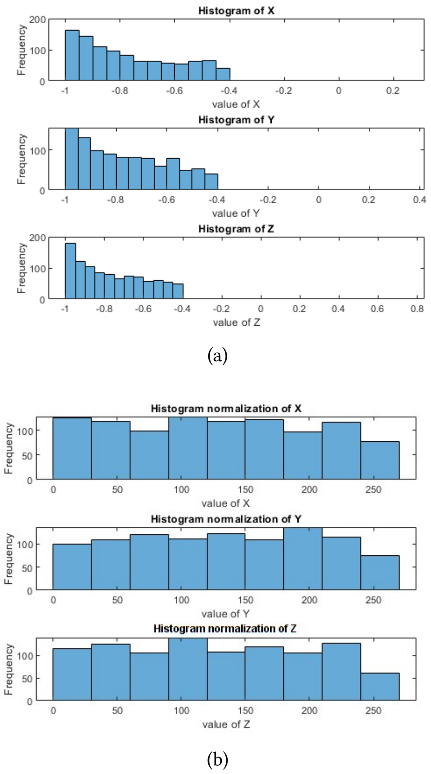
### 4.4. Column rotation

The steps used to rotate the column are similar to those of row rotation and can be applied as follows:

- Applying an offset value $N_4$,
- Choose $N$ elements of the chaos sequence $y$ starting from the offset value $N_4$.

### 4.5. XOR operation

The sequence acquired from the row and column rotations is finally subjected to an XOR operation to produce new pixel values that are distinct from the original values. The XOR operation is performed using the following steps.



(a)

(b)

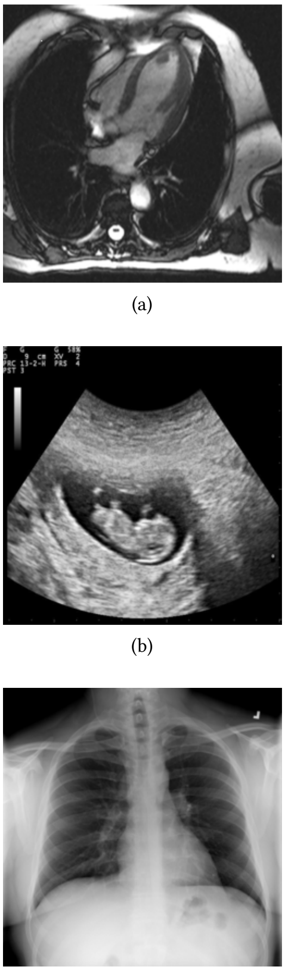
**Figure 2:** Histograms of generated sequences $x$,$y$, and $z$:(a) original histograms;(b) normalized histograms.

- Converting the $M \times N$ image to a new $1 \times MN$ image,
- XOR the chaos sequence $z$ starting from $N_6$.

## 5. Simulation results and analysis

In this section, various tests often used to analyze the statistical metrics and security of cryptosystems are employed to evaluate the performance of the proposed scheme. The tests for the performance analysis of the proposed scheme were conducted on a Core (TM) i3-4030U CPU @ 1.90 GHz with 4 GB of RAM.

**Databases used** In analyzing the proposed solution, all of the standard test images were obtained from the USC-SIPIimage database. The medical images used for the analysis arewere retrieved from The Intramural Research Program of the NClinical Center and the National Library of Medicine. The collection in Figure 3 comprises X-ray images (chest X-ray images), sonography images (abdominal sonography images), and MRI images (heart MRI images). These images are .png images with $256 \times 256$-pixel resolution.



(a)

(b)

(c)

**Figure 3:** Medical images used for the analysis:(a) Heart MRI Scan Image (M1); (b) Abdomen sonography image (M2); (c) Chest X-ray Image (M3).

### 5.1. Histogram analysis

An image histogram is used to visually depict the distribution of pixel intensity within an image[18]. The histogram of the encrypted M3 image produced by our scheme is evenly distributed and completely different from that of the plain image, as shown in Figure 4. Hence, the proposed approach is more robust to statistical attacks.

### 5.2. Shannon's entropy analysis

The distribution of pixels in cipher images must be completely uniform [19] to ensure safety against any assault. Consequently, the entropy of an n-bit image is n when the

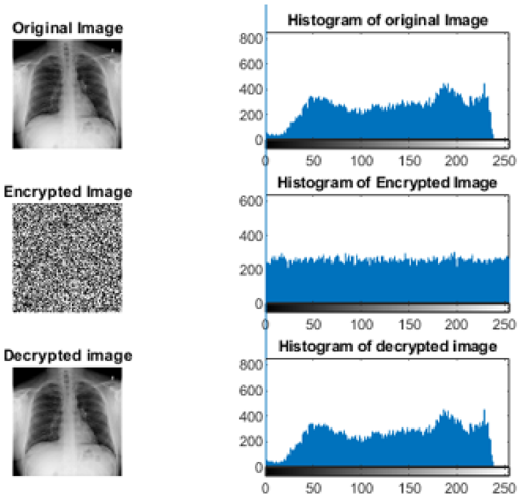


**Figure 4:** Histogram plot results of plain, encrypted, and decrypted M3 images.

**Table 1**
Shannon entropy results.

| Images | Original | Encrypted | Decrypted |
|---|---|---|---|
| M1 | 6.670125 | 7.997410 | 6.670125 |
| M2 | 6.018538 | 7.996868 | 6.018538 |
| M3 | 7.669655 | 7.997229 | 7.669655 |
| Lena | 7.446718 | 7.996744 | 7.446718 |

pixel distribution is perfectly uniform. After calculating the entropy values using equation 6, it can be observed from Table1 that our scheme is closer to 8, with a mean entropy value of 7.9966, which ensures that the pixel distribution of the cipher images is uniform and provides maximum security.

$$H(x) = \sum_{i=0}^{2^n-1} p(x_i) \log_2 p(x_i) \tag{6}$$

$p(x_i)$ is the probability of a specific symbol $x$, and $n$ is the number of bits[7].

## 5.3. Differential analysis

By carefully examining the connections between plain and ciphered images, a differential attack can be used to recover the input image from the encrypted image without the secret key. This is measured using the “Unified Average Changing Intensity (UACI)”, “Number of Pixels Changing Rate (NPCR)”, and “Peak Signal-to-Noise Ratio (PSNR)”[20] given by equations 7-9. The NPCR, UACI, and PSNR of two cipher images, $I1$, which is encrypted from the original plain image, and $I2$, which is encrypted from the same image with a single-pixel value change [7].

**Table 2**
NPCR, UACI, and PSNR values.

| Images | NPCR | UACI | PSNR(dB) |
|---|---|---|---|
| M1 | 0.996047 | 0.339776 | 40.610644 |
| M2 | 0.996551 | 0.369822 | 38.662443 |
| M3 | 0.996398 | 0.321238 | 41.844615 |
| Lena | 0.996124 | 0.339796 | 44.498529 |

$$NPCR = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{A(i,j)}{W \times H} \times 100 \tag{7}$$

where:

$$A(i,j) = \begin{cases} 0\; if I1(i,j) = I2(i,j) \\ 1\; otherwise \end{cases}$$

$$UACI = \sum_{i=1}^{M}\sum_{j=1}^{N} \left(\frac{|I1(i,j) - I2(i,j)|}{W \times H \times L}\right) \times 100 \tag{8}$$

$$PSNR = 20log_{10}\frac{255}{\sqrt{MSE}} \tag{9}$$

where: $MSE = \frac{1}{W\times H\times L}\sum_{i=1}^{W}\sum_{j=1}^{H}\sum_{k=1}^{L}[I(i,j,k) - K(i,j,k)]^2$

$W$ and $H$ are the width and height of the image, respectively, and $L$ is the maximum possible pixel value in the image[7]. $MSE$ is the mean squared error. $i$, $j$, and $k$ are the pixel positions, and $I$ and $K$ are the pixel values of the original and encrypted images, respectively.

As shown in Table2, with a mean score close to 99% for the NPCR and 33% for the UACI, our strategy yielded good results in the differential analysis. Thus, we can conclude that the proposed method effectively protects against differential attacks.

## 5.4. Contrast analysis

Contrast is a textural feature that characterizes the clarity and regional differences in an image. Consequently, it can be used to determine and compute the average distribution of pixels in an image, as expressed in equation 10.

$$H(x) = \sum_{i,j} |i-j|^2 G(i,j) \tag{10}$$

$G$ is referred to as the "gray-level co-occurrence matrix (GLCM)", and $G(i,j)$ is the number of grayscale values in the matrix. Table 3, shows that the proposed encryption method guarantees the best possible image contrast for the generated cipher images.

**Table 3**
Contrast analysis results.

| Images | Plain image | Encrypted image |
|---|---|---|
| M1 | 253.83 | 10917.88 |
| M2 | 308.53 | 10953.55 |
| M3 | 36.78 | 10918.00 |
| Lena | 269.74 | 10902.15 |

**Table 4**
Run time (in seconds) and memory used (in MB) for the encryption and decryption algorithm.

| Images | Run time | Memory usage |
|---|---|---|
| M1 | 0.552356 | 0.864256 |
| M2 | 0.554510 | 0.159744 |
| M3 | 0.560326 | 1.626112 |
| Lena | 0.572440 | 0.872448 |

## 5.5. Performance analysis

Owing to the vast amount of image data that must be processed, performance analysis is crucial for image encryption and decryption techniques. It assists in identifying potential areas for improvement and optimization, such as reducing useless tasks or memory utilization. To assess the effectiveness of the proposed algorithm, we examined its memory requirements and end-to-end runtime. MATLAB R2023 is the simulation tool and language used.

### 5.5.1. Run-Time analysis

To assess the effectiveness of the proposed algorithm for encrypting and decrypting images, we calculated the execution times for various images. Table4shows that the proposed scheme is considerably faster than the other methods and can encrypt $256 \times 256$ images in an average time of approximately 0.55 seconds.

### 5.5.2. Memory analysis

Memory analysis was used to estimate the memory required by the proposed technique for encrypting and decrypting images. We calculate the end-to-end memory usage for different images in Figure 4. Since the memory usage of the proposed algorithm depends on the image size and the software/Hardwar performance, our proposed scheme has low memory usage regardless of the PC performance and the simulation tool used.

## 5.6. Key space

The key space is the total number of keys that can be used in a cryptographic system. 3D chaos is a more key space than 1D and 2D chaos; as a result, 3D chaos provides greater security than others[21]. In this work, seven initial conditions $x(1)$,$y(1)$,$z(1)$,$\eta$,$\sigma$, $\vartheta$, $\kappa$. of the chaotic map are used as secret keys for encryption with precision $10^{-15}$. The following six random numbers are used as keys:$N_1$, $N_2$, $N_3$,$N_4$, $N_5$, and $N_6$ . These are used as keys with a precision of $10^5$. The total key space size is $(10^{15})^7 \times (10^5)^6 = 10^{135}$, which is large enough to resist exhaustive attack.

# 6. Comparison and discussion

In the past section, numerous tests were performed on the images to assess the security and statistical capabilities of the proposed image-encryption algorithm. Here, we compare our scheme with different medical algorithms in Ref[7], Ref[22], and Ref[23], as tabulated in Table5.

Resistance to statistical attacks: The histograms of the plain image and encrypted image generated by our scheme share no similarity. The encrypted image has a more uniform histogram. Additionally, it is clear by comparing the contrast values with those of other encryption techniques that our encryption scheme performs almost as well as other algorithms. Hence, the proposed technique was more resistant to statistical assaults.

Resistance to ciphertext only attacks: The entropy of images with 8-bit pixel values should be close to 8. With a mean entropy value of 7.9970, our encryption scheme is more entropy-rich than the aforementioned methods. Thus, the proposed technique is more resistant to ciphertext-only assaults.

Resistance to differential attacks: When subjected to differential analysis, our scheme yielded good results, with a mean score comparable to those of the other schemes. Thus, we can conclude that the proposed scheme is resistant to differential assaults.

Computational processing analysis: The proposed scheme uses the least amount of memory and encrypts a $256 \times 256$ image in 0.55 seconds, which is the fastest of the other systems.

Consequently, based on several tests, our technique was proven to achieve a reasonable balance between performance and security.

**Table 5**
Comparison to other schemes.

| Metrics | Ideal value | Image used | Proposed | Ref [23] | Ref[7] | Ref[22] |
|---|---|---|---|---|---|---|
| Entropy | Equal to 8 | Heart MRI Scan image | 7.9974 | 7.9970 | 7.9974 | - |
| | | Abdomen Sonography image | 7.9968 | 7.9973 | 7.9974 | - |
| | | Lena image | 7.9967 | - | 7.9832 | 7.9974 |
| NPCR | Equal to 99.609375% | Heart MRI Scan image | 99.6047 | 99.6262 | 99.5884 | - |
| | | Abdomen Sonography image | 99.6551 | 99.5881 | 99.4280 | - |
| | | Lena image | 99.6124 | - | 99.6000 | 99.60 |
| UACI | Equal to 33.463541% | Heart MRI Scan image | 33.9776 | 33.3514 | 33.4026 | - |
| | | Abdomen Sonography image | 36.9822 | 33.321 | 33.3485 | - |
| | | Lena image | 33.9796 | - | 33.3530 | 33.49 |
| PSNR | High as much as it can be | Heart MRI Scan image | 40.6106 | - | - | - |
| | | Abdomen Sonography image | 38.6624 | - | - | - |
| | | Lena image | 44.4985 | - | - | - |
| Run-Time (Mean) | Small as much as it can be | - | 0.5599 | 1.5800 | 6.8433 | - |
| Memory usage (Mean) | Low as much as it can be | - | 0.88064 | 0.4933 | 0.0767 | - |
| Contrast analysis | High | Heart MRI Scan image | 10917.88 | 10,917.07 | 10,957.36 | - |
| | | Abdomen Sonography image | 10953.55 | 10,913.82 | 10,993.71 | - |
| Key space | Large as much as it can be | - | $10^{135}$ | - | - | $2^{532}$ |

## 7. Conclusion

The widespread use of medical image encryption based on chaotic maps has increased in recent years owing to the notable nonlinear features of chaos, which make it an appropriate candidate for medical cryptographic applications. In this study, we propose a fast and secure cryptosystem algorithm that employs a chaotic intertwining 3D logistic-cosine map to generate a key image that is used to perform XOR diffusion of the image. It has the advantages of high speed and comparable performance to the state-of-the-art schemes. Objective parameters such as entropy and histogram analysis, the NPCR, and the UACI reveal the strength of cryptosystems in resisting statistical, differential, and ciphertext attacks. However, our scheme currently supports only square and grayscale images. This approach may be extended in the future to encrypt colored and nonsquare images.

## References

[1] H. Khaloufi, K. Abouelmehdi, A. Beni-hssane, M. Saadi, Security model for big healthcare data lifecycle, Procedia Computer Science 141 (2018) 294–301.

[2] M. Kaur, V. Kumar, Efficient image encryption method based on improved lorenz chaotic system, Electronics Letters 54 (2018) 562–564.

[3] S. John, S. Kumar, 2d lorentz chaotic model coupled with logistic chaotic model for medical image encryption: Towards ensuring security for teleradiology, Procedia Computer Science 218 (2023) 918–926.

[4] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, I. Hussain, A novel hybrid secure image encryption based on julia set of fractals and 3d lorenz chaotic map, Entropy 22 (2020) 274.

[5] S. M. Ahmed, H. MA Elkamchouchi, A. Elfahar, W. El-Shafai, A. G. Mohamed, A hybrid medical image cryptosystem based on 4d-hyperchaotic s-boxes and logistic maps, Multimedia Tools and Applications (2023) 1–29.

[6] P. Sarosh, S. A. Parah, G. M. Bhat, Fast image encryption framework for medical images, in: 2021 2nd International conference on intelligent engineering and management (ICIEM), IEEE, 2021, pp. 149–154.

[7] K. Jain, A. Aji, P. Krishnan, Medical image encryption scheme using multiple chaotic maps, Pattern Recognition Letters 152 (2021) 356–364.

[8] B. Han, Y. Jia, G. Huang, L. Cai, A medical image encryption algorithm based on hermite chaotic neural network, in: 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), volume 1, IEEE, 2020, pp. 2644–2648.

[9] P. V. B. Bayari, G. Bhatnagar, C. Chattopadhyay, A comprehensive study on the security of medical information using encryption, Medical Information Processing and Security: Techniques and Applications (2022) 229.

[10] P. T. Akkasaligar, S. Biradar, Medical image compression and encryption using chaos based dna cryptography, in: 2020 IEEE Bangalore humanitarian technology conference (B-HTC), IEEE, 2020, pp. 1–5.

[11] R. I. Abdelfatah, H. M. Saqr, M. E. Nasr, An efficient medical image encryption scheme for (wban) based on adaptive dna and modern multi chaotic map, Multimedia Tools and Applications 82 (2023) 22213–22227.

[12] R. Amdouni, M. Gafsi, M. A. Hajjaji, A. Mtibaa, Combining dna encoding and chaos for medical image encryption, in: 2022 IEEE 21st international Ccnference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), IEEE, 2022, pp. 277–282.

[13] U. S. Choi, S. J. Cho, S. W. Kang, Color medical image encryption using 3d chaotic cat map and nca, in: 2019 10th IFIP international conference on new technologies, mobility and security (NTMS), IEEE, 2019, pp. 1–5.

[14] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, V. N. Coelho, Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices, Optics and Lasers in Engineering 110 (2018) 24–32.

[15] G. Narayanan, R. Narayanan, N. Haneef, N. B. Chittaragi, S. G. Koolagudi, A novel approach to video steganography using a 3d chaotic map, in: TENCON 2019-2019 IEEE Region 10 Conference (TENCON), IEEE, 2019, pp. 955–959.

[16] X. Wang, D. Xu, Image encryption using genetic operators and intertwining logistic map, Nonlinear Dynamics 78 (2014) 2975–2984.

[17] M. Dua, D. Makhija, P. Y. L. Manasa, P. Mishra, 3d chaotic map-cosine transformation based approach to video encryption and decryption, Open Computer Science 12 (2022) 37–56.

[18] H. Movafegh Ghadirli, A. Nodehi, R. Enayatifar, Color image dna encryption using mrna properties and non-adjacent coupled map lattices, Multimedia Tools and Applications 80 (2021) 8445–8469.

[19] H. Li, L. Deng, Z. Gu, A robust image encryption algorithm based on a 32-bit chaotic system, IEEE Access 8 (2020) 30127–30151.

[20] K. H. Moussa, A. I. El Naggary, H. G. Mohamed, Non-linear hopped chaos parameters-based image encryption algorithm using histogram equalization,

Entropy 23 (2021) 535.

[21] M. B. Hossain, M. T. Rahman, A. S. Rahman, S. Islam, A new approach of image encryption using 3d chaotic map to enhance security of multimedia component, in: 2014 International Conference on Informatics, Electronics & Vision (ICIEV), IEEE, 2014, pp. 1–6.

[22] Y. Luo, J. Yu, W. Lai, L. Liu, A novel chaotic image encryption algorithm based on improved baker map and logistic map, Multimedia Tools and Applications 78 (2019) 22023–22043.

[23] S. Sudevan, K. Jain, A lightweight medical image encryption scheme using chaotic maps and image scrambling, in: 2023 11th International Symposium on Digital Forensics and Security (ISDFS), IEEE, 2023, pp. 1–6.