Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.037281
Article

A Novel Internet of Medical Thing Cryptosystem Based on Jigsaw Transformation and Ikeda Chaotic Map

Sultan Almakdi[1], Mohammed S. Alshehri[1], Yousef Asiri[1], Mimonah Al Qathrady[2,*], Anas Ibrar[3] and Jawad Ahmad[4]

[1]Department of Computer Science, Najran University, Najran, 61441, Saudi Arabia
[2]Department of Information Systems, Najran University, Najran, 61441, Saudi Arabia
[3]Department of Electrical Engineering, Wah Engineering College, University of Wah, Wah Cantt, 47040, Pakistan
[4]School of Computing, Edinburgh Napier University, Edinburgh, EH10 5DT, UK
*Corresponding Author: Mimonah Al Qathrady. Email: mqalqathrady@nu.edu.sa
Received: 28 October 2022; Accepted: 28 December 2022

Abstract: Image encryption has attracted much interest as a robust security solution for preventing unauthorized access to critical image data. Medical picture encryption is a crucial step in many cloud-based and healthcare applications. In this study, a strong cryptosystem based on a 2D chaotic map and Jigsaw transformation is presented for the encryption of medical photos in private Internet of Medical Things (IoMT) and cloud storage. A disorganized three-dimensional map is the foundation of the proposed cipher. The dispersion of pixel values and the permutation of their places in this map are accomplished using a nonlinear encoding process. The suggested cryptosystem enhances the security of the delivered medical images by performing many operations. To validate the efficiency of the recommended cryptosystem, various medical image kinds are used, each with its unique characteristics. Several measures are used to evaluate the proposed cryptosystem, which all support its robust security. The simulation results confirm the supplied cryptosystem's secrecy. Furthermore, it provides strong robustness and suggested protection standards for cloud service applications, healthcare, and IoMT. It is seen that the proposed 3D chaotic cryptosystem obtains an average entropy of 7.9998, which is near its most excellent value of 8, and a typical NPCR value of 99.62%, which is also near its extreme value of 99.60%. Moreover, the recommended cryptosystem outperforms conventional security systems across the test assessment criteria.

Keywords: Jigsaw transformation; cryptosystem; image encryption; medical images; Ikeda map; chaotic system

1 Introduction

Digital grayscale or color images are necessary data-carrying instruments. Images are used in various of critical applications such as biometric identification, online commerce, telemedicine,

healthcare, military, and online banking. Concerns about the security of the storage and broadcast of medical images over public networks have grown in recent years. Organizations specializing in healthcare continue to publish mandatory requirements such as Picture Archiving and Communication Systems (PACS), Digital Imaging and Communications in Medicine (DICOM), and Health Insurance Portability and Accountability Act (HIPAA). Regarding medical image data storage, PACS is primarily meant to be used within the hospital network, which is typically secured by a firewall to keep out outsiders. Intruders, both accidental and evil, may have thousands of chances to tamper with private data if the conversation occurs on public networks. Public networks are rife with dangers to the security of medical image storage and transmission.

One of the leading security objectives is to ensure information confidentiality, considering the quickly expanding use of networks and multimedia capabilities. As they develop cutting-edge strategies to protect the privacy of image data both during storage and transmission, researchers continue to concentrate on image encryption. Image encryption differs from traditional text encryption because of images' low entropy, high spatial correlation, and tremendous storage capacity [1]. Numerous cryptographic techniques have been proposed in the literature for attaining the goals of confusion and distribution. Chaotic maps have been used in cryptography to achieve both goals because of their predictability and high sensitivity to initial conditions. A few uses for chaotic maps in image encryption include histogram equalization, pixel scrambling, the generation of pseudorandom numbers, and the development of substitution boxes (S-boxes). Using techniques like steganography or even cryptography, which hides the message's content from unauthorized readers, secret information is delivered. These techniques permit using text, audio, video, and picture for covert communication [2–5]. The image has grown in importance because of the development of the internet and digital multimedia capabilities.

1.1 Literature Review

Image data is far more significant and more spatially correlated than text data. Chaotic systems have been implemented in several image encryption techniques since they were first used, and their security capabilities were demonstrated. Non-linear, deterministic systems with properties that make them appropriate for image encryption are called chaotic maps. In other words, a chaotic system exhibits pseudorandom behavior and is susceptible to the beginning circumstances. This implies that a bit adjustment to the settings results in a different chaotic map output. Images sent or stored may be vulnerable to various security risks, including manipulation, eavesdropping, duplication, and noise. To make it easier to retrieve the original pixels during decryption, the scrambling technique must be reversible.

To achieve better encryption results, several methods integrate chaos theory with permutation algorithms. In [6], for instance, the authors suggest an encryption scheme with chaos that employs the Jigsaw procedure for the scrambling process. The method has three stages: pre-processing, encryption, and post-processing. In [7], an image-encryption technique with iterative cosine transform and the Jigsaw transform (JT) is described. To secure medical images, Hua et al. [8] first insert arbitrary data into the seed image and then use two steps of diffusion and pixel scrambling. The watermark is encrypted using the Jigsaw transform in a hybrid digital cryptosystem, which was presented in [9]. An input image was first permuted using a chaotic map, and then the watermark was embedded using the Discrete Cosine Transform (DCT). A selective chaos-based image encryption approach was proposed by Kanso et al. [10], which includes a scrambling phase using chaotic cat maps and a masking phase using the same block-based structure. Contrastingly, Wang et al. [11] proposed Langton's ant (LA), cellular automata, to permute the image, where an entwining logistic map specified the phases and

subsequent location of the ant. The researchers also concluded the process of image diffusion by employing a Piecewise Linear Chaotic Map (PWLCM). Chebyshev map and rotation equation was presented as pseudo-random bit generators in an image encryption scheme by Stoyanov et al. [12]. Aryal et al. [13] suggested a block-shuffling-based encryption model using block shuffling, positive-negative transformation, rotation, and color module permutation.

Furthermore, a histogram fluctuating technique was utilized as invertible data concealment. With an examination of the dynamic and the circuit of the chaotic map, Gao et al. [14] recommended an encryption approach based on multi-image fusion and fractional-order hyperchaotic systems. A method for image scrambling and diffusion was proposed by Wang et al. [15], which mixes 1D and 2D chaotic map systems to construct chaotic structures. The image is then scrambled using an L-shaped technique based on the block, observed by a diffusion period at the bit level. Both the scrambling and diffusion phases of Wang et al. dynamic encryption scheme [16] were presented. To achieve the dynamic behavior, the chaotic system's pseudo-random number is tweaked after each iteration. A nested sine map in several dimensions forms the chaotic system. A Henon map-based image encryption approach using elliptic curve cryptography and dynamic substitution box confusion was reported by Ibrahim et al. in [17]. The image encryption approach developed by Laiphrakpam et al. [18] uses an elliptic curve and chaotic structure. It features four distinct phases: a chaotic diffusion stage, an S-box-based substitution stage, a Logistic map-based diffusion stage, and a block permutation stage. Arnold transforms (AT) were reported to be enhanced by Liang et al. [19] via a double permutation encryption technique depending on AT that alters both the location of pixels and their grey values. This approach is faster than the standard AT and just as helpful.

Mehta et al. [20] suggested a robust scheme for fundus images based on chaos theory utilizing a grouping of permutation and substitution design, which has applications in medical image cryptography, such as the encryption of fundus images. Using robust adaptive control, Javan et al. [21] developed a solution based on hyper-chaotic systems' multi-mode synchronization to encrypt medical images. On the contrary, Moafimadani et al. [22] offered a technique based on chaotic maps to secure medical images from hacking. It employs a rapid shuffling procedure, observed by a diffusion that is both fast and flexible. Xue et al. introduced an image protection technique in [23] that uses the varying lengths of deoxyribonucleic acid chains. Row chain and column chain operations in DNA, dynamic coding in DNA, are all used to encrypt the image using this method. The approach was evaluated using three different types of medical images. Medical image encryption employing a genetic system variant and a coupled lattice map was published by Nematzadeh et al. in [24]. The cipher is enhanced by the connected lattice map, and the updated genetic algorithm speeds up convergence with a recent local search approach and a stop condition. An approach combining the Integer Wavelet Transform, DNA computing, and randomization was proposed by Ravichandran et al. [25]. The 1D logistic system coupled with pseudo-random numbers was used by Kumar et al. [26] in their presentation of a medical image encryption scheme. The authors examined how the logistic map's parameters and beginning values affect its reshuffling and replacement operations. Natural as well as medical images, including those of the human brain, magnetic resonance imaging (MRI), and lungs, were used to validate the procedure. To improve upon many preexisting biometric encryption schemes, Carey et al. [27] offered a system for encrypting medical images using the user's iris and fingerprint. These fingerprints and iris scans are hashed with the Indexing First One algorithm and then utilized as keys in an AES-CBC cipher with two rounds of encryption. The technique is also lossless, which is essential in a healthcare encryption system. For a strategy that is more stealthy, secure, and robust than prior approaches, Salama et al. [28] combined the Discrete Wavelet Transform's wavelet-induced multi-resolution decomposition capacity with the energy compaction of the Discrete

Cosine Transform. Banik et al. [29] presented a method for encrypting a series of medical photos using the elliptic curve analog ElGamal encryption scheme and the Mersenne Twister PRNG. This method decreases the time needed for encryption while also fixing ElGamal's bloatware issue. After applying an optimized Arnold map on grey images over a predetermined number of iterations, Ge [30] introduced an encryption technique dubbed ALC encryption that uses Chebyshev and Logistic map cross-diffusion. This updated Arnold map is generic for images of any dimension. A cross-diffusion of a double chaotic map is used to encrypt color images. Using the Rossler dynamical system and the Sine map, Sangavi et al. [31] suggested a Medical Image Encryption scheme that does the usage of the chaotic nature of the data. It was stated by Chai et al. [32] that a medical image encryption strategy was developed using a hybrid of the Latin square and a chaotic system. An encryption method for protecting individual identities in medical images was published by Elamir et al. [33]. Data is concealed in the least significant bits of image pixels using the Least Significant Bit method. Afterward, the image is compressed using a key devised using DNA encoding rules and chaotic systems. Shafai et al. [34] proposed a medical image encryption-based algorithm. Wang et al. [35] discussed ridge regression predictor-based high precision error prediction algorithm for data hiding. Ma et al. [36] prosed a code division multiplexing-based reversible data hiding scheme. Some other schemes were proposed by various researchers over time [37–41]. There are numerous encryption algorithms in the literature based on different domains. We have selected the combination of jigsaw transformation and chaotic map to get the highly random private keys.

1.2 Research Contribution

There exist many encryption structures for the security of image data in the literature. All the cryptosystems do not ensure the robustness of image data. There exists sensitive information in the images, such as the Internet of Medical Things (IoMT); which needs special protection. Numerous chaos-based encryption algorithms are vulnerable to some classical attacks. To make the encryption structure robust, we added the concept of plaintext-based key generation. The change of private key at each time of encryption makes the system perfect from a security point of view. Therefore, we have presented a cryptosystem to offer secrecy to cloud storage in IoMT. As compared to the other complex chaotic structures, the 2D chaotic map yields highly random and unpredictable numbers with low computation costs. Therefore we have selected the combination of a 2D Ikeda map and a jigsaw puzzle to achieve low computational cost. The key contributions of this work are as follows:

1. It offers excellent performance as compared to the traditional cryptosystems
2. To provide a robust communication system using a 2D chaotic map and Jigsaw transformation.
3. To offer security on the Internet of Medical Things (IoMT) by providing services in cloud storage.
4. To get maximum security with minimal computational complexity.
5. Its efficacy is examined in several forms of differential assaults, and positive results are found.

The numerical results are compared with the state of the art to assure the standard security achievement.

1.3 Paper Organization

The remaining manuscript is ordered as follows: Section 2 offerings some fundamental aspects of the encryption algorithm; Section 3 gives the structure of the anticipated cryptosystem; The simulation outcomes are shown in Second 4; The performance analyses are depicted in Section 5; A contrast with published work is performed in Section 6; Lastly, a conclusion is presented in the last section.

The illustration of an IoMT-based health cloud is shown in Fig. 1.

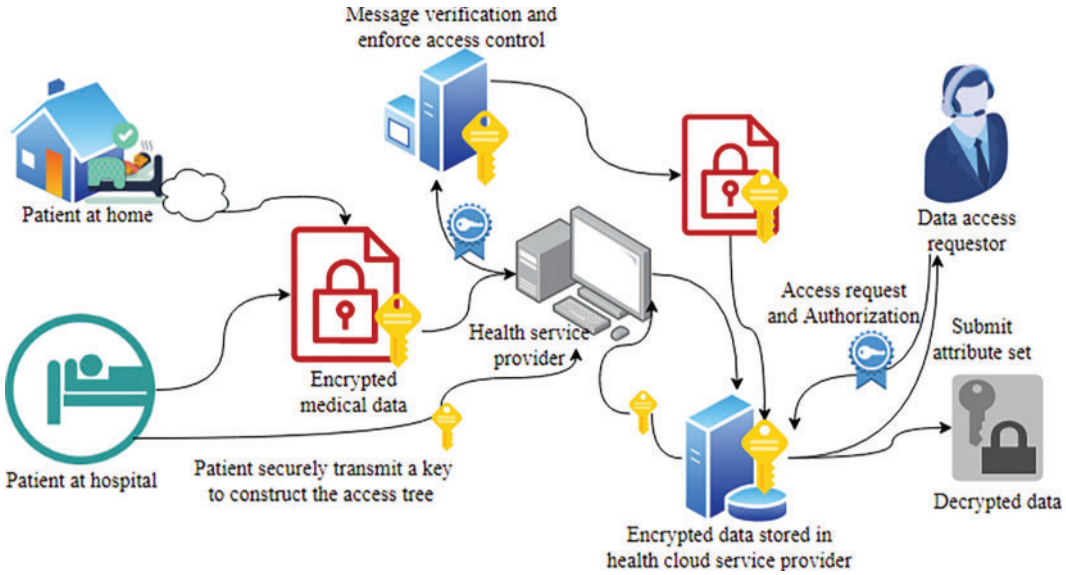


Figure 1: Secure data transmission at Health Cloud

2 Preliminaries

2.1 Jigsaw Transformation

A nonlinear operator $JT\{\}$ known as the Jigsaw transform randomly juxtaposes several portions of a complicated image. It has the benefit of utilizing the same method for both encrypting and decrypting the image.

Consider $P(r, s, i)$ be a digital image with N bands, r, s as its spatial coordinates and $i = i_1, ..., i_N$ signifying the index for the N bands. Initially, the image $P(r, s, i)$ is shattered into M non-overlying subdivisions of $p1 \times p2$ pixels for r and s in all bands. Then, by using some random permutation each block is relocated. The Jigsaw transform maintains the energy for both the directly $JT_M\{\}$ and the converse $JT_{-M}\{\}$ transforms since it is unitary. It, therefore, complies with the link implied by Eq. (1):

$$I(x, y, \tau) = JT_{-M}\{J_M\{I(x, y, \tau)\}\}. \tag{1}$$

A sample implementation of Jigsaw transformation on the Skull X-ray image is depicted in Fig. 2.

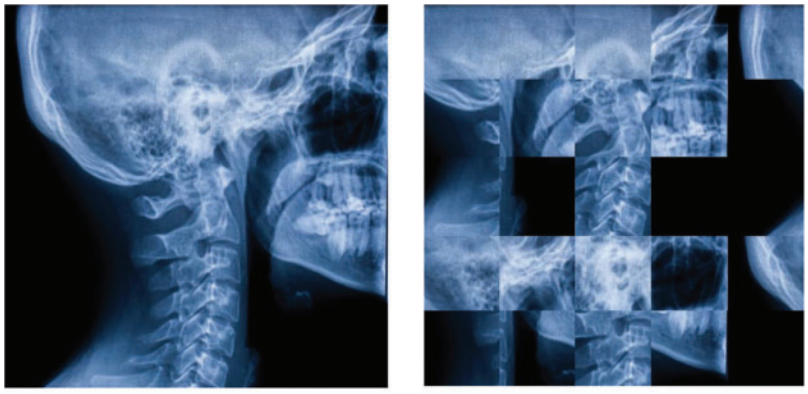
2.2 Ikeda Map

Kensuke Ikeda suggested the initial map as a model of light moving about a nonlinear optical cavity resonator. The 2D Ikeda map can be defined as:

$$\begin{cases} x_{n+1} = 1 + u(x_n \cos t_n - y_n \sin t_n), \\ y_{n+1} = u(x_n \sin t_n + y_n \cos t_n), \end{cases} \tag{2}$$

where u is a parameter and

$$t_n = 0.4 - \frac{6}{1 + x_n^2 + y_n^2}. \tag{3}$$

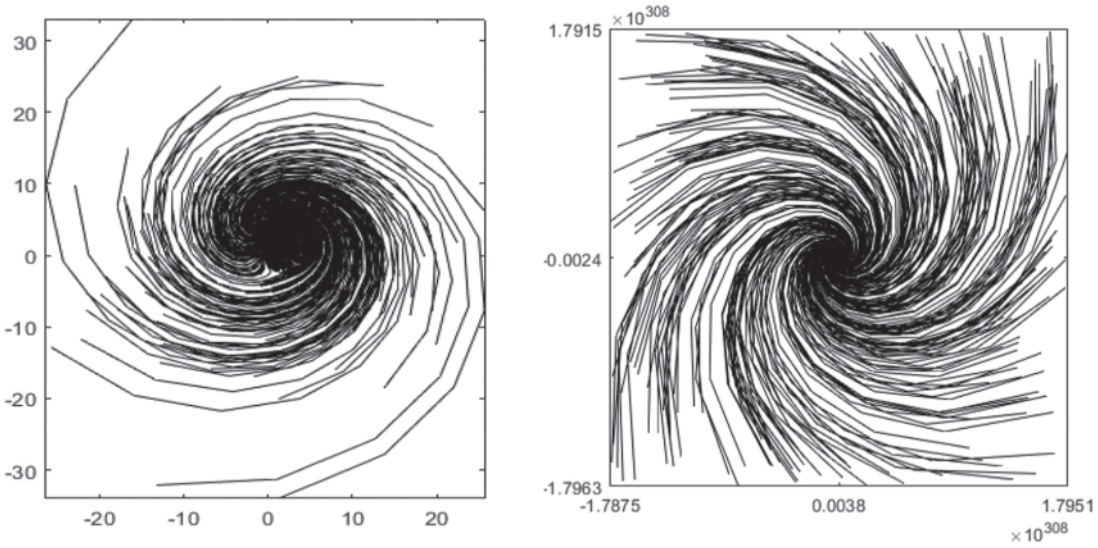


(a) (b)

Figure 2: A sample implementation of Jigsaw transformation on Skull X-ray image

The system shows chaotic behavior with $u \geq 0.6$.

The point trajectories for the Ikeda map with 10000 iterations by variating the parameter u are presented in Fig. 3.



(a) (b)

Figure 3: Point trajectories for (a) $u = 0.9$; (b) $u = 1.3$

3 Proposed Medical Image Cryptosystem

3.1 Private Key Generation

The maximum security in a cryptosystem is provided by the part of key generation. The unpredictability of the secret key of encryption algorithms makes it secure against all statistical and differential attacks. The simplest way to achieve randomness in the secret key is the dependency of key generation on the plaintext. The complete encryption with just a single pixel change in the plaintext

gives rise to a robust structure. Therefore, we have utilized a formula for the parameters and initial conditions generation of the Ikeda chaotic map. As chaotic systems are highly sensitive to their initial conditions and chaotic parameters, a slight modification in the initial values causes an entirely distinct sequence of numerous iterations. The parameters for the chaotic map can be generated by:

$$x(0) = \frac{\max \sum_{i=1}^{N} P_i}{M \times N}, \tag{4}$$

$$y(0) = \frac{\min \sum_{j=1}^{N} P_j}{M \times N}, \tag{5}$$

$$u = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} P_{ij}}{M \times N}, \tag{6}$$

where P_{ij} represents the pixels of the plain image, P_i shows rows of the image, P_j depicts the columns of the image and $M \times N$ signifies the dimensions of the plain image. Each plain image P produces unique values of $x(0)$, $y(0)$ and u.

3.2 Proposed Encryption Algorithm

The encryption structure involves the Ikeda map and Jigsaw transformation as primitives of the algorithm. The pseudo algorithm of the proposed algorithm is shown in Table 1. The working strides of the encryption scheme are as follows:

Step 1: Insert a plain medical image with dimensions $M \times N \times 3$ as input of the algorithm.

Step 2: Insert the original image in the key generation algorithm to construct the key parameters for the Ikeda chaotic map.

Step 3: The constructed initial conditions and parameter values are seeded in the Ikeda map and the chaotic sequences are stored for the encryption steps.

Step 4: The original image is initially permuted using the Jigsaw transformation with setting each block size 8×8.

Step 5: The permuted image is then diffused with the Ikeda map X trajectory by using the bitwise XOR operation.

Step 6: The matrix data gained from step 5 is then shuffled row-wise and column-wise by implementing the Y trajectory of the Ikeda map.

Step 7: The data attained from step 6 is again passed from the Jigsaw transformation to get the resultant matrix data.

Step 8: The final resultant is compiled as the enciphered image.

Table 1: The Pseudo algorithm for the suggested cryptosystem

Input: Original medical image P with dimensions $M \times N \times 3$.

Step 1: *Separate each layer of the image in R, G, B.*
Step 2: *Initial key generation*
for $i = 1$ to M **do**
for $j = 1$ to N **do**

(Continued)

Table 1: Continued

Input: Original medical image P with dimensions $M \times N \times 3$.

$x(0) = \max(sum(P_i/M \times N))$
$y(0) = \max\left(sum\left(P_j/M \times N\right)\right)$
$u = sum(P_{ij}/M \times N))$
end
end
Step 3: *Insert initial values obtained from step 2 into the Ikeda map and get the sequences* $\{X\}, \{Y\}$.
Step 4: *Implementation of Jigsaw Transformation*
for $i, j = M, N$ **do**
$C_1 = JT\{P\}$
end
Step 5: *Diffusion with a chaotic sequence*
$C_2 = C_1 \oplus X$
Step 6: *Shuffling of* C_2 *by using the chaotic sequence* Y.
Step 7: *Implementation of Jigsaw transformation on the final version obtained from step 6*.
Output: Encrypted medical image

The flowchart diagram of the proposed medical image cryptosystem is shown in Fig. 4.

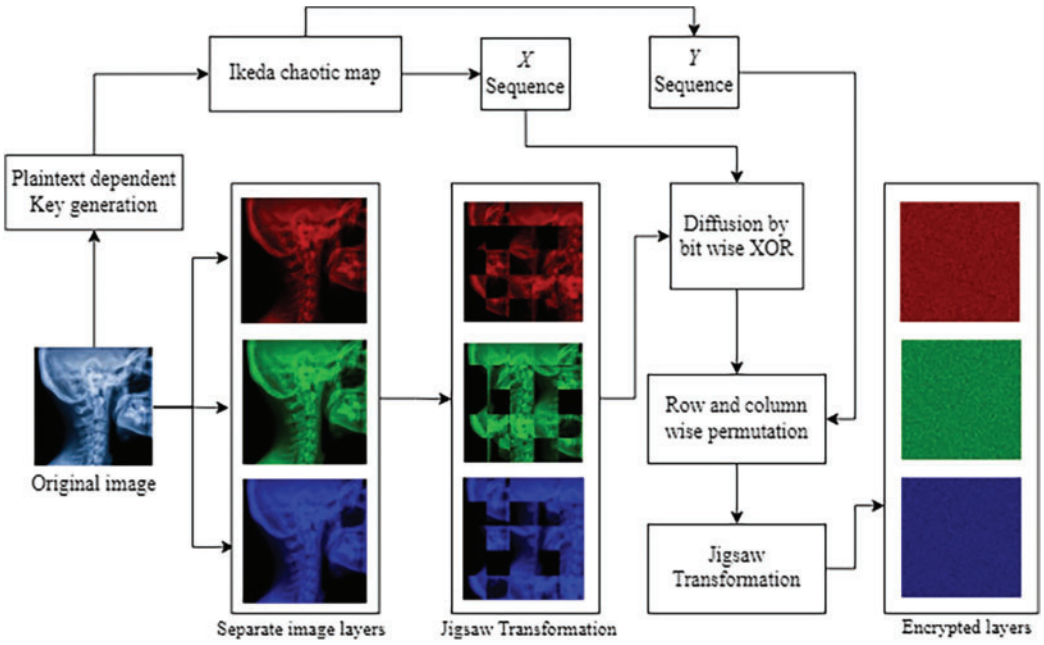


Figure 4: Flowchart of the proposed medical image cryptosystem

4 The Simulation Results

This section details the simulations that were carried out using Matlab 2020a on a 64-bit machine running Microsoft Windows 10 with an Intel(R) Core (TM) i3-3120M CPU running at 2.50 GHz and

8.00 GHZ RAM. The experimental images of the simulation outcomes incorporate abdominal Xray, Chest Xray, elbow Xray, hand Xray, knee Xray, and skull Xray with dimensions $512 \times 512 \times 3$ named "Image 1", "Image 2", "Image 3", "Image 4", "Image 5", and "Image 6" respectively. The experimental medical images are shown in Fig. 5.

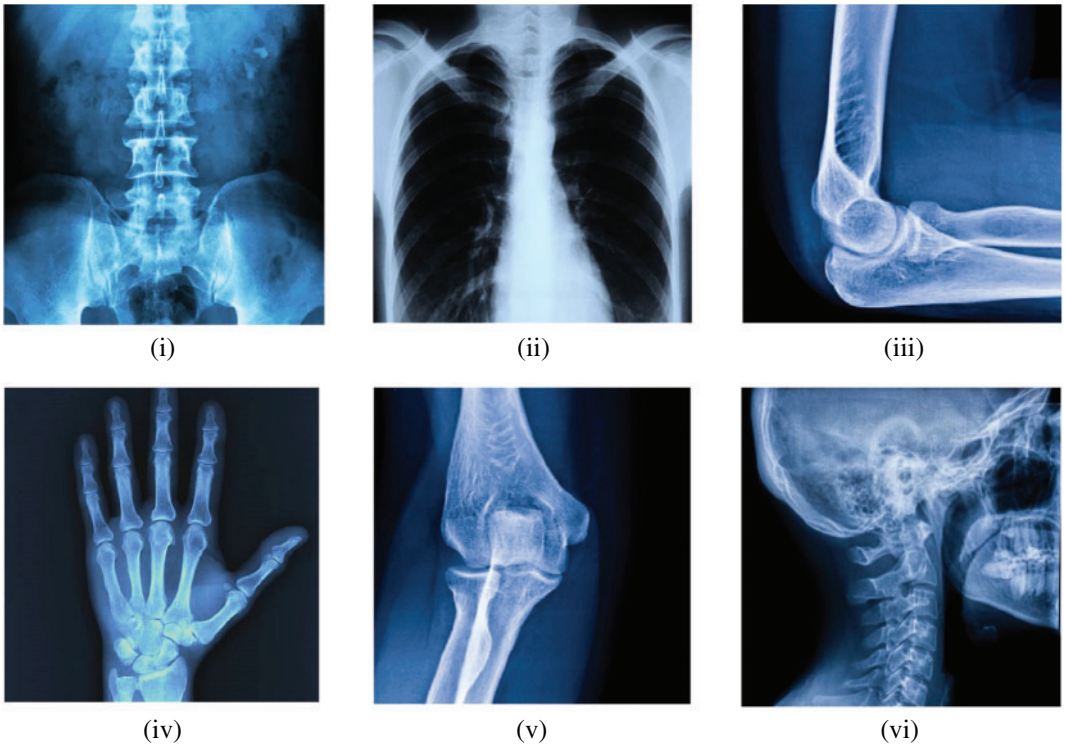


Figure 5: Experimental Xray images (i) Image 1; (ii) Image 2; (iii) Image 3; (iv) Image 4; (v) Image 5; (vi) Image 6

5 Security Performance Analyses

To check the efficiency of the proposed cryptosystem, we have performed some security analyses such as NIST, histogram, correlation coefficient, statistical histogram deviation, statistical irregular deviation, information entropy, differential attack, and key sensitivity analysis.

5.1 NIST

The National Institute of Standards and Technology (NIST) test is used for the encrypted data to examine the pseudo-randomness in the suggested method. The encrypted is tested using the NIST-800-22 technique, which contains 15 separate tests, in this study. All derived p-values must be higher than the predetermined significance level of 0.01 to qualify as a satisfactory pseudo-randomness sequence. Table 2 is a list of the NIST test results. As we can see, all the p-values are higher than 0.01, indicating that the hyperchaotic system passes all 15 of the NIST tests. As a result, the sequence employed in the suggested method behaves in a very unpredictable manner.

Table 2: NIST test results for "Image 1"

Test	*p*-value		
	Red	Green	Blue
Frequency	0.9254	0.7140	0.5119
Block frequency	0.9547	0.9632	0.8988
Runs	0.2919	0.2919	0.2919
Longest runs	0.0357	0.5214	0.8541
Universal	0.9191	0.9966	0.7712
Linear complexity	0.5521	0.6335	0.5824
Discrete Fourier transform (Spectral)	0.9634	0.6987	0.5631
Overlapping template matching	0.8740	0.5507	0.7553
Non-overlapping template matching	0.7001	0.8806	0.9964
Approximate entropy	0.9608	0.9914	0.2851
Serial	0.9987	0.7431	0.4799
Cumulative sums	0.8570	0.5874	0.4141
Binary matrix rank	0.9632	0.6634	0.8563
Random excursions	0.9014	0.9501	0.8956
Random excursions variant	0.6164	0.5004	0.6110

5.2 Histogram

The dispersal of pixels in the plain and enciphered images serves as the histogram's representation. It could reveal the spreading characteristics of the image pixel values by reflecting the frequency with which each grey level occurs. A standard image's histogram typically has an uneven distribution, but an encrypted image using a robust encryption method will have a histogram that is as uniform as feasible. The histogram of the original images and their respective encrypted images are displayed in Fig. 6. Fig. 6 shows the histograms of the plain images (a–d) and the cipher images (e–h).

Since the histograms of enciphered images vary from those of original images and the amount of every pixel value in the enciphered image is nearly equivalent, enciphered images cannot provide any statistical data about the plain image by examining their histograms. The suggested technique may, therefore, statistically evaluate assaults.

5.3 Correlation Coefficient

The correlation coefficient can be used to assess the unpredictability of ciphers produced by the offered cryptosystem. Each pair of contiguous pixels in the plain image have a robust association with one another. This association must be destroyed within the ciphered image by an effective cryptosystem. The diagonal, vertical, and horizontal correlations for the analyzed images are portrayed in Fig. 7.

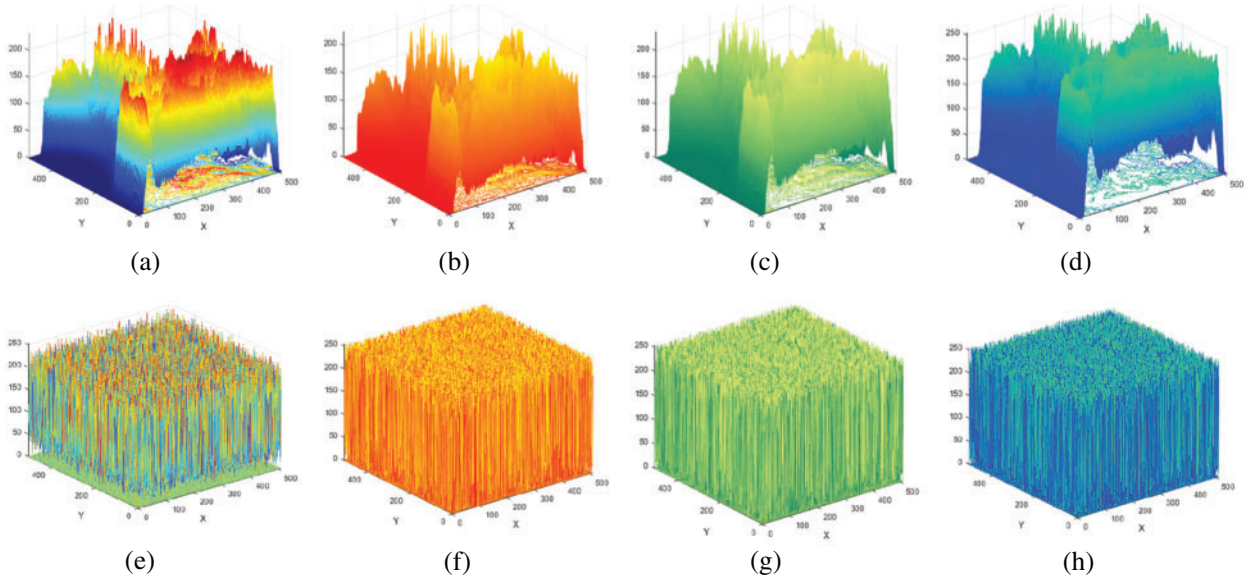


Figure 6: 3D histograms for Image 6 (a–d) Original layers; (e–h) Encrypted layers

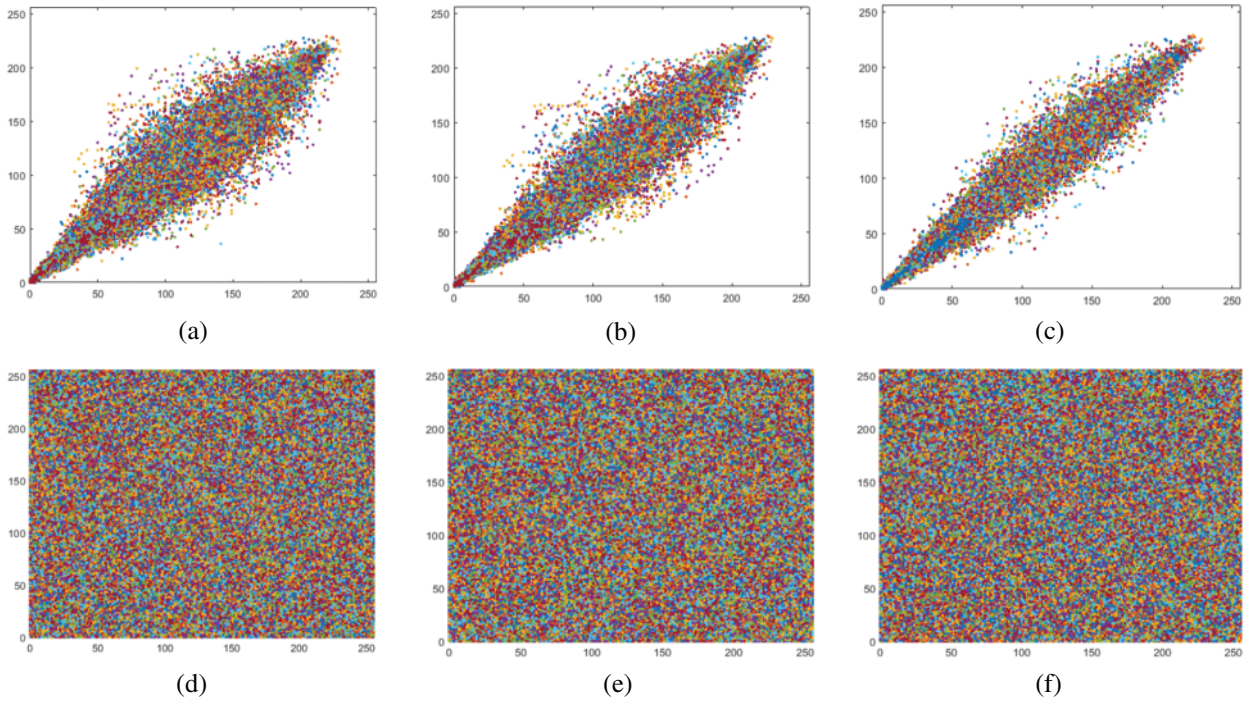


Figure 7: Correlation diagram for Image 1 (a–c) Original diagonal, horizontal, and vertical direction; (d–f) Encrypted diagonal, horizontal, and vertical direction, respectively

Using Eq. (7), the values of the correlation coefficients $r_{x,y}$ are obtained to measure pixel correlation. In Table 3, the correlation findings are displayed. By incorporating suitable correlation values, the recommended ciphering method provides a good level of security, as can be perceived from the

simulation results displayed in Table 3. As a result, the suggested cryptosystem's performance improves as the $r_{x,y}$ value drops.

$$r_{x,y} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{7}$$

$$\text{cov}\,(x, y) = E\left\{(x - E(x))(y - E(y))\right\}, \tag{8}$$

$$E\,(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{9}$$

$$D\,(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \tag{10}$$

where $r_{x,y}$ is the correlation value for contiguous pixels, and x and y are the gray-scale values of two nearby pixels in the plain image or enciphered image. The original image and its enciphered edition are used for the correlation evaluation. The correlation coefficient can be used in a variety of situations.

- The $r_{x,y}$ value is near to or equivalent to "± 1" to suggest a high scale of correlation among the two variables.
- The $r_{x,y}$ value is near or equivalent to "0", representing a significant discrepancy among the original image and its enciphered form.

Table 3: Correlation coefficient for plain and enciphered images

Image	Plain image			Ciphered image		
	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical
Image 1	0.9807	0.9869	0.9917	−0.0007	0.0011	0.0009
Image 2	0.9955	0.9966	0.9981	−0.0003	−0.0108	−0.0001
Image 3	0.9902	0.9952	0.9948	−0.0099	−0.0064	−0.0038
Image 4	0.9760	0.9840	0.9919	0.0051	−0.0081	−0.0147
Image 5	0.9920	0.9947	0.9978	−0.0039	−0.0001	−0.0022
Image 6	0.9878	0.9926	0.9949	−0.0071	−0.0092	0.0010

The results show a strong connection among contiguous pixels in the original experimental images, as expected. To put it another way, a low correlation coefficient value between the surrounding pixels of the evaluated cipher images shows that our suggested cryptosystem is quite efficient.

5.4 Statistical Histogram Deviation (D_H)

The histogram deviation, which represents the difference among the ciphered and plain images, may be used to assess ciphering quality. The value of the histogram deviation is calculated by (11).

$$D_H = \frac{\left(\frac{d_0 + d_{255}}{2} + \sum_{i=1}^{254} d_i\right)}{M \times N}, \tag{11}$$

where $M \times N$ denotes the size of the enciphered image. The absolute variance among the assessed histogram of plain and enciphered images is shown by d_i at the gray level i. The outcomes of statistical histogram deviation are displayed in Table 4 which are in the acceptable range.

5.5 *Statistical Irregular Deviation (D_I)*

The irregular deviation, which reflects the value of the indiscretion of the eccentricity coming from the enciphering procedure, may be used to evaluate the ciphering quality. The value of irregular deviation is determined by (12).

$$D_I = \frac{\sum_{i=0}^{255} H_D(i)}{M \times N}. \tag{12}$$

$H_D(i)$ is estimated by

$$H_D(i) = |H(i) - M_H|, \tag{13}$$

where $M \times N$ denotes the dimensions of the enciphered data matrix. M_H denotes the average of the histogram of a ciphered image, and $H(i)$ is the histogram of the enciphered data matrix.

The smallest value of statistical irregular deviation indicates the excellent quality of the cipher. The results of D_I are offered in Table 4 which depicts the best quality of the ciphered image.

Table 4: Statistical histogram and irregular deviation for experimental images

Image	Statistical histogram deviation (D_H)	Statistical irregular deviation (D_I)
Image 1	0.1274	8.25×10^{-4}
Image 2	0.1963	1.99×10^{-3}
Image 3	0.2511	0.91×10^{-4}
Image 4	0.3691	7.53×10^{-4}
Image 5	0.1579	8.41×10^{-5}
Image 6	0.2005	9.63×10^{-6}

5.6 *Entropy*

Shannon identified entropy as a crucial feature that expresses the uncertainty and irregularity of a data source 1949. Eq. (14) describes the entropy $H(s)$ of a message source s, where s denotes the source, N shows bits mandatory to signify the symbol s_i, and $P(s_i)$ denotes the probability of the symbol s_i. The entropy of a completely random source made up of 2^N symbols are N. As a result, the entropy of the encipher image having 256 grey levels should ideally be 8 for a safe cryptosystem.

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i) \log_2 P(s_i). \tag{14}$$

The results of global and local entropy for encrypted medical images are depicted in Table 5. The ciphered results of global entropy are near the ideal value of 8 and local entropy also lies within the acceptance rate which indicates a lower risk of attacks related to entropy.

Table 5: Entropy analysis for experimental images

Image	Global entropy			Local entropy		
	Red	Green	Blue	Red	Green	Blue
Image 1	7.9998	7.9991	7.9997	7.9012	7.9077	7.9002
Image 2	7.9996	7.9992	7.9996	7.9185	7.9014	7.9011
Image 3	7.9998	7.9997	7.9989	7.9896	7.9028	7.9034
Image 4	7.9988	7.9991	7.9999	7.9001	7.9007	7.9041
Image 5	7.9996	7.9993	7.9992	7.9021	7.9063	7.9000
Image 6	7.9991	7.9995	7.9998	7.9011	7.9002	7.9005

5.7 Differential Attack Analysis

The number of pixel change rates (NPCR), which refers to the proportion of various pixel numbers among two enciphered contents, is applied to quantify the unlikeness among two encrypted images. The number of averaged changing intensities among two enciphered images is counted using the Unified Average Changing Intensity (UACI). For 8-bit coded images, the idyllic NPCR and UACI values are 99.61 percent and 33.46 percent, correspondingly. The NPCR and UACI are specified as follows:

$$D(i,j) = \begin{cases} 0, & if \quad C_1(i,j) = C_2(i,j), \\ 1, & if \quad C_1(i,j) = C_2(i,j), \end{cases} \tag{15}$$

$$NPCR: N(C_1, C_2) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\%, \tag{16}$$

$$UACI: N(C_1, C_2) = \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{F \times T} \times 100\%, \tag{17}$$

where C_1 is the cipher image before and C_2 is the cipher image after significantly differing keys. NPCR and UACI values produced with slightly modified keys and the right cipher image are displayed in Table 6. To verify the variance of NPCR and UACI we have executed the analysis for different sizes of "Image 1".

Table 6 shows that the suggested algorithm's NPCR and UACI are also near standard values, at 99.6% and 33.5%, respectively.

Table 6: NPCR and UACI measures for some experimental medical images

	Size	NPCR			UACI		
		Red	Green	Blue	Red	Green	Blue
Image 1	128 × 128	99.44	99.67	99.63	33.54	33.07	32.89
	256 × 256	99.50	99.68	99.57	33.21	33.82	33.65
	512 × 512	99.30	99.57	99.64	33.35	33.58	33.24
	1024 × 1024	99.66	99.63	99.63	33.91	34.44	33.69

(Continued)

Table 6: Continued

	Size	NPCR			UACI		
		Red	Green	Blue	Red	Green	Blue
Image 2	512 × 512	99.67	99.70	99.69	34.01	34.33	34.11
Image 3	512 × 512	99.60	99.63	99.58	33.96	33.84	33.85
Image 4	512 × 512	99.66	99.64	99.65	33.45	33.48	33.97
Image 5	512 × 512	99.81	99.77	99.63	34.50	33.98	33.80
Image 6	512 × 512	99.61	99.75	99.07	33.57	33.62	33.71

5.8 PSNR and MSE Analysis

Mean-Square-Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) are used to evaluate the efficiency of the decryption process. Typically, the PSNR of an encrypted image will be lower. Grayscale values for pixels in the i^{th} row and j^{th} column of the $H \times W$ encryption and the plain image are denoted by $C(i,j)$ and $P(i,j)$, respectively. The mean squared error and peak signal-to-noise ratio of these two images is

$$MSE = \frac{1}{H \times W} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} |C(i,j) - P(i,j)|^2, \tag{18}$$

$$PSNR = 20 \log_{10} \left(\frac{255}{\text{sqrt(MSE)}} \right). \tag{19}$$

The low PSNR values in Table 7 demonstrate the difficulties in recovering the plain image from the cipher image without knowing the secret key.

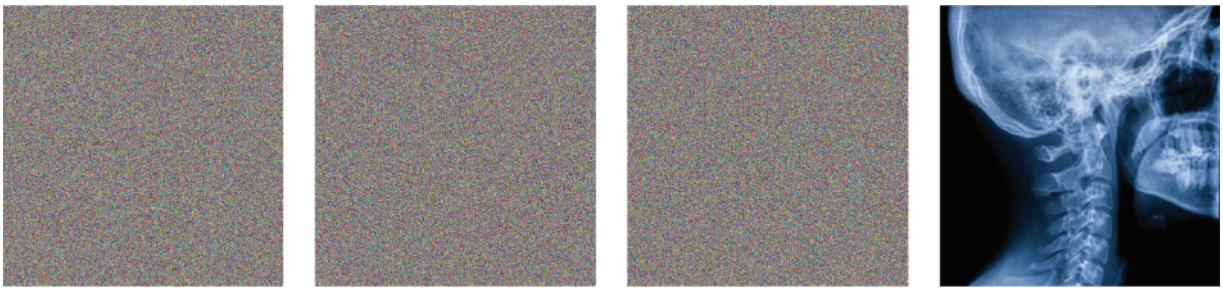
Table 7: Measurements of MSE and PSNR

Image	MSE	PSNR
Image 1	8.3491×10^3	9.7271
Image 2	1.3304×10^4	7.1369
Image 3	7.7159×10^3	8.9550
Image 4	8.1199×10^3	9.1109
Image 5	1.1824×10^4	7.0852
Image 6	8.0188×10^3	9.7109

5.9 Key Sensitivity and Space Analysis

Any data encryption structure's effectiveness and toughness be contingent on the private keys that are used, which are regarded as the main elements of the ciphering technique. The wide keyspace and high sensitivity of the encryption technique to key variations are the two most crucial characteristics of the secret keys. The keyspace is controlled by the key size. It is preferable to have a private key that is as big as possible so that it is challenging for an attacker to guess. The key sensitivity shows that even if the attacker can obtain the private key with just one bit of change, the plain image will continue to be unexpected. Therefore, even with little differences in the secret key, a trustworthy and robust image ciphering approach must be susceptible to modest changes in the decoding key. If an image encryption

method has a secret key that is larger than 2^{100}, brute-force attacks can be resisted. The overall size of the secret key, as was indicated in the proposed scheme, is 3×10^{100}, which can offer the required resistance. The secret key should also be extremely sensitive to changes in its values. The wrong keys were utilized to extract the plain image from the enciphered data to verify the sensitivity of the keys. The results shown in Fig. 8 depict the robustness of the algorithm. The recommended cryptosystem is believed to have good resilience based on all the provided.



(a) (b) (c) (d)

Figure 8: (a–c) Images retrieved through the wrong key; (d) Image retrieved by the correct key

5.10 Time Execution Analysis

The algorithm's performance concerning time reveals the reliability of the cryptosystem. Many algorithms offer high security with complex encryption structures but require a lot of time for execution which results in an increment in cost and time waste. Therefore, to examine the efficacy of the encryption algorithm, the time execution analysis plays a vital role in making it a reliable source of communication tool. The time execution analysis (in seconds) for the proposed cryptosystem is shown in Table 8. The results depict that the suggested cryptosystem offers higher security with reliable execution time.

Table 8: Time execution analysis for the proposed cryptosystem

Image	Encryption algorithm time (in s)			Total
	Key generation	Permutation	Diffusion	
Image 1	0.536	2.014	1.971	4.521
Image 2	0.452	2.362	1.604	4.418
Image 3	0.465	2.479	1.997	4.941
Image 4	0.601	1.998	2.001	4.600
Image 5	0.557	2.009	1.805	4.371
Image 6	0.498	2.207	1.759	4.464

6 Comparative Analysis

This section of the manuscript provides a brief comparison of the numerical statical analyses obtained from the proposed cryptosystem. The results of the correlation coefficient, entropy, statistical irregular deviation, statistical histogram deviation, NPCR, and UACI are compared with an already

existing medical encryption scheme. The numerical results of "Image 2" are utilized for comparison with References [34,42,43]. The comparative results are shown in Table 9. The comparison of correlation shows that our proposed cryptosystem meets the standard results as the results in References [34,42,43]. The values of irregular deviation and irregular histogram are also up to the mark. The NPCR and UACI of our proposed algorithm are better than the scheme in References [34,42,43]. The entropy of the cipher produced by our cryptosystem is near the standard value which is 8. Other the other hand, the entropy of the exiting scheme is less. Therefore, we can say that our proposed structure meets the analysis criteria as compared to the existing work, which indicates the robustness of the algorithm.

Table 9: The comparison of numerical results with the existing scheme

Analysis	Proposed	Reference [34]	Reference [42]	Reference [43]
Horizontal	−0.0108	−0.0077	0.0023	0.0681
Diagonal	−0.0003	−0.0064	−0.0008	0.0128
Vertical	−0.0001	0.0029	0.0007	0.0049
Irregular deviation	0.0019	0.0011	–	–
Histogram deviation	0.1963	0.2374	–	–
NPCR	99.68	99.6520	99.60	99.61
UACI	34.15	32.9235	33.59	33.35
Entropy	7.9994	7.9477	7.9995	7.9991

7 Conclusion

In this work, Jigsaw transformation and Ikeda chaotic map-based medical image cryptosystem were proposed. It depends on a combination of value diffusion and position permutation algorithms. The results of the experiments performed on various medical images show that the offered cryptosystem is both robust against differential assaults and highly sensitive to initial conditions. It offers a high level of protection with little computational overhead. The entropy results also show how practical the proposed cryptosystem is. The comparative study performed in Table 8 also depicts that the algorithm meets the existing standards. As a result, the proposed 2D chaotic cryptosystem can be suggested for essential and sensitive IoMT applications in healthcare and telemedicine. To enhance the security performance of medical picture broadcasts and develop a multi-level security system for these images, we will combine additional security methods including steganography and watermarking in our subsequent study. Further study could investigate testing the anticipated 2D chaotic map cryptosystem with the NIST benchmark, using the proposed hybrid security techniques on large databases of color medical images, and suggesting a robust medical image encryption method based on DNA encoding in addition to chaos encryption.

Acknowledgement: The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work under the Research Collaboration Funding program grant code (NU/RC/SERC/11/5).

Funding Statement: The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work under the Research Groups Funding program grant code (NU/RC/SERC/11/5).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Q. Zhou, K. W. Wong, X. Liao, T. Xiang and Y. Hu, "Parallel image encryption algorithm based on discretized chaotic map," *Chaos Solitons Fractals*, vol. 38, no. 4, pp. 1081–1092, 2008.

[2] H. Gao, Y. Zhang, S. Liang and D. Li, "A new chaotic algorithm for image encryption," *Chaos Solitons Fractals*, vol. 29, no. 2, pp. 393–399, 2006.

[3] L. Xiong, Z. Xu and Y. Q. Shi, "An integer wavelet transform based scheme for reversible data hiding in encrypted images," *Multidimensional Systems and Signal Processing*, vol. 29, no. 3, pp. 1191–1202, 2018.

[4] R. Punidha and M. Sivaram, "Integer wavelet transform based approach for high robustness of audio signal transmission," *International Journal of Pure and Applied Mathematics*, vol. 116, no. 23, pp. 295–304, 2017.

[5] R. Huang, K. H. Rhee and S. Uchida, "A parallel image encryption method based on compressive sensing," *Multimedia Tools Application*, vol. 72, no. 1, pp. 71–93, 2014.

[6] Z. Li, C. Peng, W. Tan and L. Li, "An effective chaos-based image encryption scheme using imitating jigsaw method," *Complexity*, vol. 2021, no. 11, pp. 1–18, 2021.

[7] O. Vilardy, J. L. M. Barba and C. O. Torres, "Image encryption and decryption systems using the jigsaw transform and the iterative finite field cosine transform," *Photonics*, vol. 6, no. 4, pp. 121, 2019.

[8] Z. Hua, S. Yi and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, no. 1, pp. 134–144, 2018.

[9] M. Arora and M. Khurana, "Secure image encryption technique based on jigsaw transform and chaotic scrambling using digital image watermarking," *Optical and Quantum Electronics*, vol. 52, no. 59, pp. 13, 2020.

[10] A. Kanso and M. Ghebleh, "An efficient and robust image encryption scheme for medical applications," *Communications in Nonlinear Science and Numerical Simulation*, vol. 24, no. 1–3, pp. 98–116, 2015.

[11] X. Wang and D. Xu, "A novel image encryption scheme using chaos and Langton's Ant cellular automaton," *Nonlinear Dynamics*, vol. 79, no. 4, pp. 2449–2456, 2015.

[12] B. Stoyanov and K. Kordov, "Image encryption using Chebyshev map and rotation equation," *Entropy*, vol. 17, no. 4, pp. 2117–2139, 2015.

[13] A. Aryal, S. Imaizumi, T. Horiuchi and H. Kiya, "Integrated model of image protection techniques," *Journal of Imaging*, vol. 4, no. 1, 2018.

[14] X. Gao, J. Yu, S. Banerjee, H. Yan and J. Mou, "A new image encryption scheme based on fractional-order hyperchaotic system and multiple image fusion," *International Journal of Scientific Reports*, vol. 11, 2021.

[15] X. Wang and Y. Chen, "A new chaotic image encryption algorithm based on L-shaped method of dynamic block," *Sensing and Imaging*, vol. 22, no. 1, pp. 503, 2021.

[16] X. Wang and M. Zhang, "An image encryption algorithm based on new chaos and diffusion values of a truth table," *Journal of Information Science*, vol. 579, no. 4, pp. 128–149, 2021.

[17] 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, 2021.

[18] D. Laiphrakpam and M. Khumanthem, "A robust image encryption scheme based on chaotic system and elliptic curve over finite field," *Multimedia Tools Applications*, vol. 77, no. 7, pp. 8629–8652, 2018.

[19] R. Liang, Y. Qin, C. Zhang, J. Lai, M. Liu *et al.,* "An improved Arnold image scrambling algorithm," in *IOP Conf. Series: Materials Science and Engineering*, Bristol, UK, IOP Publishing, vol. 677, 2019.

[20] G. Mehta, M. Dutta and P. Kim, "An efficient and lossless cryptosystem for security in tele-ophthalmology applications using chaotic theory," *International Journal of E-Health and Medical Communications*, vol. 7, pp. 28–47, 2016.

[21] A. A. K. Javan, M. Jafari, A. Shoeibi, A. Zare, M. Khodatars *et al.,* "Medical images encryption based on adaptive-robust multi-mode synchronization of chen hyper-chaotic systems," *Sensors*, vol. 21, no. 11, pp. 3925, 2021.

[22] S. S. Moafimadani, Y. Chen and C. Tang, "A new algorithm for medical color images encryption using chaotic systems," *Entropy*, vol. 21, no. 6, pp. 577, 2019.

[23] X. Xue, H. Jin, D. Zhou and C. Zhou, "Medical image protection algorithm based on deoxyribonucleic acid chain of dynamic length," *Frontiers in Genetics*, vol. 12, no. 266, pp. 1021, 2021.

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

[25] D. Ravichandran, S. A. Banu, B. Murthy, V. Balasubramanian, S. Fathima *et al.,* "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain," *Medical and Biological Engineering and Computing*, vol. 59, no. 589, pp. 589–605, 2021.

[26] M. Kumar and P. Gupta, "A new medical image encryption algorithm based on the 1D logistic map associated with pseudo-random numbers," *Multimedia Tools and Applications*, vol. 80, no. 12, pp. 18941–18967, 2021.

[27] A. Carey and J. Zhan, "A cancelable multi-modal biometric based encryption scheme for medical images," in *Proc. of the 2020 IEEE Int. Conf. on Big Data (Big Data)*, Atlanta, GA, USA, pp. 3711–3720, 2020.

[28] A. Salama, M. Mokhtar, M. Tayel, E. Eldesouky and A. Ali, "A triple-channel encrypted hybrid fusion technique to improve security of medical images," *Computers, Materials & Continua*, vol. 68, no. 1, pp. 431–446, 2021.

[29] A. Banik, Z. Shamsi and D. Laiphrakpam, "An encryption scheme for securing multiple medical images," *Journal of Information Security and Applications*, vol. 49, no. 4, pp. 102398, 2019.

[30] J. Ge, "ALCencryption: A secure and efficient algorithm for medical image encryption," *Computer Modeling in Engineering and Sciences*, vol. 125, no. 3, pp. 1083–1100, 2020.

[31] V. Sangavi and P. Thangavel, "An exotic multi-dimensional conceptualization for medical image encryption exerting Rossler system and Sine map," *Journal of Information Security and Applications*, vol. 55, no. 8, pp. 102626, 2020.

[32] X. Chai, J. Zhang, Z. Gan and Y. Zhang, "Medical image encryption algorithm based on Latin square and memristive chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 24, pp. 35419–35453, 2019.

[33] M. Elamir, W. Al-atabany and M. Mabrouk, "Hybrid image encryption scheme for secure E-health systems," *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 10, no. 1, pp. 1727, 2021.

[34] W. E. Shafai, F. Khallaf, E. S. M. El-Rabaie and F. E. A. E. Samie, "Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services," *Journal of Ambient Intelligence and Humanized Computing*, 2022.

[35] X. Wang, X. Wang, B. Ma, Q. Li and Y. Q. Shi, "High precision error prediction algorithm based on ridge regression predictor for reversible data hiding," *IEEE Signal Processing Letters*, vol. 28, pp. 1125–1129, 2021.

[36] B. Ma and Y. Q. Shi, "A reversible data hiding scheme based on code division multiplexing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1914–1927, 2016.

[37] W. Xingyuan, G. Suo, Y. Xiaolin, Z. Shuang and W. Mingxu, "A new image encryption algorithm with cantor diagonal scrambling based on the PUMCML system," *International Journal of Bifurcation and Chaos*, vol. 31, no. 1, pp. 2150003, 2021.

[38] X. Wang and S. Gao, "A chaotic image encryption algorithm based on a counting system and the semi-tensor product," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10301–10322, 2021.

[39] X. Wang, S. Gao, L. Yu, Y. Sun and H. Sun, "Chaotic image encryption algorithm based on bit-combination scrambling in decimal system and dynamic diffusion," *IEEE Access*, vol. 7, pp. 103662–103677, 2019.

[40] S. Gao, R. Wu, X. Wang, J. Wang, Q. Li *et al.,* "A 3D model encryption scheme based on a cascaded chaotic system," *Signal Processing*, vol. 202, no. 1, pp. 108745, 2022.

[41] R. Wu, S. Gao, X. Wang, S. Liu, Q. Li *et al.,* "AEA-NCS: An audio encryption algorithm based on a nested chaotic system," *Chaos Solitons & Fractals*, vol. 165, no. 1, pp. 112770, 2022.

[42] F. Masood, M. Driss, W. Boulila, J. Ahmad, S. U. Rehman *et al.,* "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations," *Wireless Personal Communications*, vol. 127, no. 2, pp. 1405–1432, 2022.

[43] R. Rhouma, S. Meherzi and S. Belghith, "Ocml-based colour image encryption," *Chaos Solitons & Fractals*, vol. 40, no. 1, pp. 309–318, 2009.