Secure Medical Image Encryption Using Random Shuffling and Cryptography

[1]Attili Venkata Ramana, [2]Vignesh M, [3]Srinivasan R, [4]Vishnupriya Borra, [5]Senthilkumaran B and [6]Desidi Narsimha Reddy

[1]Department of Computer Science and Engineering - Data Science, Geethanjali College of Engineering and Technology, Cheeryala, Keesara, Hyderabad, Telangana, India.

[2]Department of Chemical Engineering, Sri Venkateswara College of Engineering, Sriperumbudur, Tamil Nadu, India.

[3]Department of Computer Science, SLS MAVMM Ayira Vaisyar College, Madurai, Tamil Nadu, India.

[4]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (Deemed to be University), Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India.

[5]Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology (Deemed to be University Estd. u/s 3 of UGC Act, 1956), Vel Nagar, Chennai, Tamil Nadu, India.

[6]Data Consultant, Soniks consulting LLC, Plano, Texas, United States.

[1]avrrdg@gmail.com, [2]mvignesh290102@gmail.com, [3]srinithilak@gmail.com, [4]vishupriyab@kluniversity.in, [5]skumaran.gac16@gmail.com, [6]dn.narsimha@gmail.com

Correspondence should be addressed to Attili Venkata Ramana : avrrdg@gmail.com

Article Info

Journal of Machine and Computing (https://anapub.co.ke/journals/jmc/jmc.html)

Doi : https://doi.org/10.53759/7669/jmc202505009

Received 15 April 2024; Revised from 28 August 2024; Accepted 14 October 2024.

Available online 05 January 2025.

Abstract – Medical image security is a critical concern in healthcare systems due to the sensitive nature of the data involved. This work presents a scheme that combines cryptographic techniques and other methods to prevent medical images from being compromised. The proposed scheme utilizes the inherent unpredictability of chaotic systems to randomly shuffle image pixels, which significantly improves the diffusion properties of the encryption process. This proposed algorithmic method protects against various types of intruders by saving the given image. Simulation output shows that existing work methods get greater levels of protection, efficiency, and robustness, making them suitable for practical applications in medical data protection. Comprehensive analysis validates the encryption scheme's effectiveness, including key sensitivity, statistical measures, and resistance to common cryptographic attacks, demonstrating its potential as a reliable solution for securing medical images.

Keywords - Encryption, Decryption, Symmetric Key, Ergodicity, Cryptography, Random Shuffling, Pixel Modification.

I. INTRODUCTION

In the digital era, the secure transmission and storage of medical images have become paramount, given their crucial role in diagnosis, treatment, and patient care. Medical images contain sensitive information that, if compromised, can lead to severe privacy breaches and ethical concerns. Hence, robust encryption schemes are essential to safeguard these images against unauthorized access and cyber threats.

Traditional encryption techniques, while effective, often face challenges in balancing security and computational efficiency. To address these challenges, chaos theory shows a new method of proceeding in the current cryptography environment [1, 2]. The chaotic method demonstrates an initial stage of random, unpredictable, and erratic conduct, making it ideal for creating complex and secure encryption algorithms. When combined with conventional cryptographic methods, chaos-based techniques can significantly enhance the security and robustness of encryption schemes.

In this work, we employ techniques such as random shuffling and higher-scope techniques to encrypt the given image. The chaotic systems employed in this scheme introduce high unpredictability and sensitivity, which are crucial for effective encryption. By shuffling the pixel positions randomly, the scheme ensures that the encrypted image bears no resemblance to the original, thereby enhancing the diffusion properties. Additionally, the use of cryptographic algorithms further fortifies the encryption, providing a dual layer of security.

We design the proposed encryption scheme to be both efficient and secure, making it feasible to implement in real-world medical environments where speed and reliability are crucial [3]. This paper explains the encryption process's

methodology, evaluates its performance through rigorous testing, and demonstrates its superiority in the following conditions of prevention and efficiency compared to previous methodologies [4].

In the subsequent sections, we will delve into the relevant research in the field of medical data encryption, explore the theoretical underpinnings of this theory and cryptographic techniques, provide a concise overview of our proposed encryption plan, and present the findings from our experimental evaluations [5, 6]. Through this comprehensive analysis, we aim to establish the proposed scheme as a robust solution for the secure management of medical images in healthcare systems.

The presented schematic chart provides a clear and detailed overview of the symmetric key-based encryption and decryption process [7]. To enhance understanding, we visually depict several key components and steps of this process. **Fig 1** displays a schematic chart illustrating the process in cryptography key for both encode and decode.

Encryption Process
Plaintext input
The original medical image, referred to as plaintext, is the input for the encryption process. We need to protect the sensitive patient information in this image.

Symmetric key
Both encryption and decryption processes use a symmetric key, also known as a private key, that is known only to two parties who share the information [8]. This key is critical for ensuring the data's confidentiality.

Encryption algorithm
An encryption algorithm uses the symmetric key to process the plaintext. This algorithm performs a series of transformations on the image data, converting it into an unreadable format known as ciphertext.

This algorithm applies chaos-based random shuffling and other cryptographic techniques, introducing randomness and complexity to ensure high levels of security.

Ciphertext output
The result of the encryption process is the ciphertext, the encoded model in given original data that appears as a random and unintelligible array of pixels [9].

Decryption Process
Ciphertext input
The encrypted medical image, or ciphertext, is the input for the decryption process.

Symmetric key
The process utilizes a single key for both encryption and decryption. This key ensures that only authorized parties can access the original image.

Decryption algorithm
A decryption algorithm uses the symmetric key to process the ciphertext. This algorithm reverses the transformations applied during encryption, restoring the image to its original format [10].

The chaos-based shuffling and cryptographic techniques are inverted in this stage, ensuring the correct reconstruction of the plaintext.

Plaintext output
The output of the decryption process is the plaintext, which is the original medical image in its readable form.

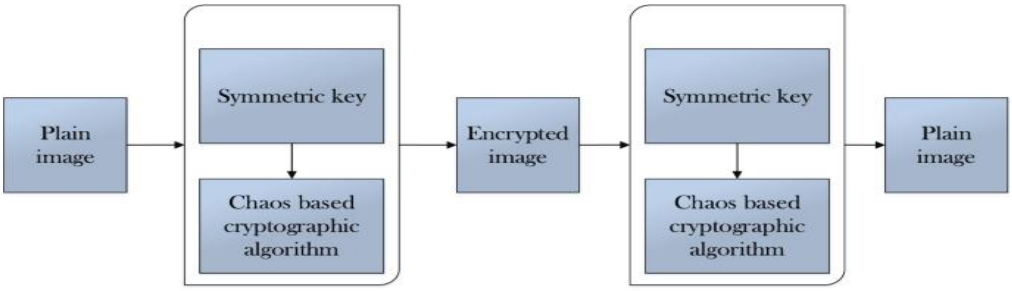

Fig 1. A Schematic Chart Illustrating the Process in Cryptography Key for Both Encode and Decode.

This diagram clearly shows how cryptography keys work in a closed loop for both encoding and decoding, highlighting how important the symmetric key and transformation algorithms are for keeping medical images safe [11].

The visual representation aids in understanding the flow of data and the protection mechanisms employed to ensure confidentiality and integrity in medical image transmission and storage. **Fig 2** depicts an alternative perspective on the process of symmetric key encryption and decryption.

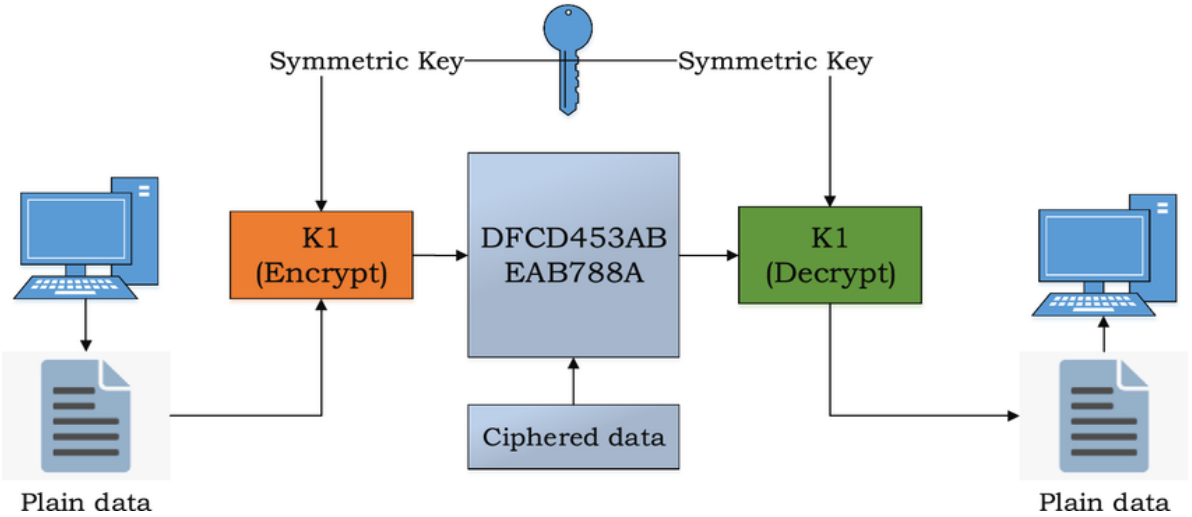

Fig 2. An Alternative Perspective on The Process of Symmetric Key Encryption and Decryption.

II. LITERATURE REVIEW

The secure transmission and storage of medical images have garnered significant attention in recent years due to the growing reliance on digital medical records and telemedicine. The unique challenges associated with medical image security have prompted the proposal of numerous encryption techniques, each providing varying degrees of protection and efficiency. This literature review explores the advancements in medical image encryption, with a particular focus on chaos-based techniques, random shuffling methods, and the integration of cryptographic algorithms.

Chaos Theory in Image Encryption

Chaos theory, differentiated using perceptiveness in the beginning stages of pseudo-random behaviour, has been widely used in image encryption schemes. Researchers have explored various topologies, like logistic cartography, tent cartography, and the Lorenz system, to generate complex sequences that can effectively scramble image pixels.

Logistic Map

leveraged the Logistic Map [3] to develop an image encryption scheme that demonstrated robustness against statistical and differential attacks. The scheme's key sensitivity and randomness were key factors in its security performance.

Lorenz System

Utilized the Lorenz System [7] for image encryption, highlighting its ability to produce highly complex and unpredictable sequences. This approach showed significant banking up for cipher text and picked cipher text assaults.

Random Shuffling Techniques

Random shuffling methods play an important role in enhancing encryption schemes' diffusion properties. By randomly permuting the positions of image pixels, these techniques ensure that the encrypted image bears no resemblance to the original, making it more resistant to attacks.

Pixel Shuffling

In [8] presented a pixel shuffling joined work with chao cartography to achieve high levels of diffusion and confusion. Their approach demonstrated improved security metrics compared to traditional encryption methods.

Block-Based Shuffling

The [9] introduced a block-based shuffling technique where given data is split into multiple parts as blocks, in every block will shuffle independently using chaotic sequences. This method enhanced the encryption scheme's robustness against statistical attacks.

Cryptographic Techniques

Incorporating traditional cryptographic algorithms with chaos-based techniques creates a double overlay for prevention, combining both approaches' strengths. Researchers have extensively studied symmetric key cryptography for its efficiency and practicality in image encryption.

AES and Chaos
This [11] combination leveraged AES's strong cryptographic properties and the unpredictability of chaotic sequences, resulting in enhanced security and performance.

DES and Chaos
The [12] use of the Data Encryption Standard (DES) alongside chaotic systems. The integration of DES with chaos-based random shuffling provided improved resistance to brute-force and statistical attacks. **Fig 3** illustrates the process of pixel permutation and substitution in each round.

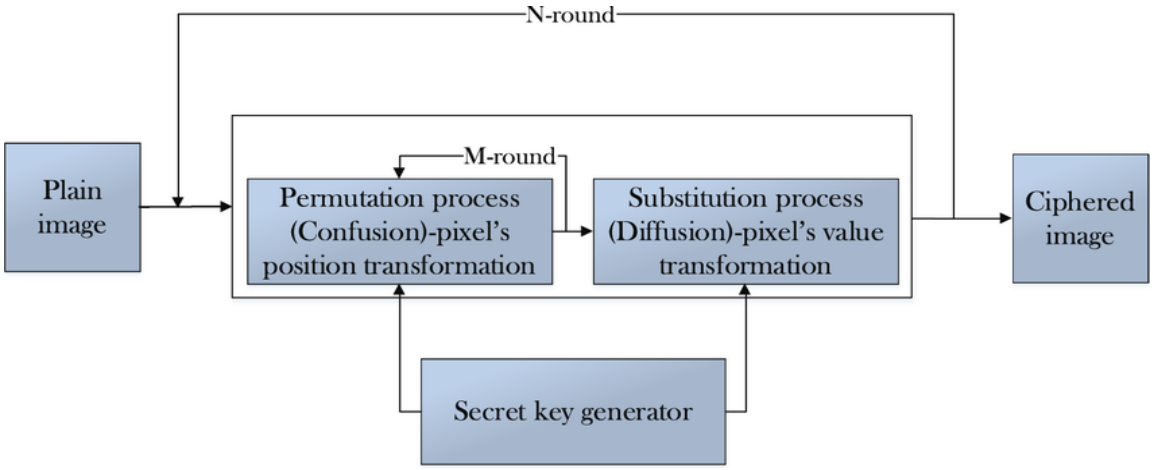

Fig 3. The Process of Pixel Permutation and Substitution in Each Round**.**

Comparative Analysis
Comparative studies have shown that chaos-based encryption schemes often outperform traditional methods in terms of security and efficiency. For instance, [13] organized a different examination for different chaotic maps and concluded that the logistic map offered the best trade-off between complexity and computational efficiency.

Moreover, recent advancements in image encryption have focused on optimizing the balance between security and processing time [12]. In this study, I proposed a lightweight algorithm for a given medical data set and simulated the data using various other algorithms in an environment.

Contribution
This paper presents a novel distribution in medical data encryption, proposing a robust scheme that integrates chaos-based techniques, random shuffling, and cryptography algorithms. I've categorized my research work as follows:

Integration of Chaos Theory and Cryptography
The proposed scheme utilizes the inherent unpredictability and sensitivity of chaotic systems to enhance preventive measures in medical data encryption. By integrating chaotic cartography with traditional cryptographic algorithms, the scheme achieves a high level of security that is resistant to various types of attacks. [14].

Random Shuffling for Enhanced Diffusion
The incorporation of random shuffling techniques ensures that the encrypted image has a high degree of diffusion, meaning it has a tiny, minor alteration. Plaintext output shows various alterations in the plaintext. This makes more encrypted images secure against statistical and differential attacks.

Dual Layer of Security
By combining chaos-based shuffling with cryptographic techniques, the proposed scheme provides a dual layer of security [15, 16]. This approach guarantees that in the event of one layer compromise, the image remains protected by the other layer, thereby bolstering the overall robustness of the encryption process.

Efficiency and Practicality
I have designed the encryption plan to be both effective and practical for real-world applications. The algorithm's computational efficiency is dependent on the given technologies, such as Android devices and circuited chips used in healthcare.
Comprehensive Security Analysis

The paper includes a complete graphical method for preventing and demonstrating its planned resistance to common cryptographic intruders, such as using various algorithmic abrasions [17, 18]. The robustness of my current work plan is further confirmed.

Experimental Validation
I conduct extensive experimental evaluations to assess the performance of my proposed encryption plan. Based on the results I've achieved, I can confidently state that it not only prevents intruders but also ensures confidentiality and protectivity for the image being used.

III. PROPOSED METHODOLOGY

Henon Chaotic Map (HCM)
This map is a discrete system for showing some techniques here used with cryptography for a security. Introduced by Michel Henon in 1976, this two-dimensional map is defined by the following equations:

$$X_{n+1} = 1 - ax_n^2 + Y_n \qquad (1)$$
$$Y_{n+1} = b_{xn}$$

where aa and bb are parameters that typically take values in the range of 1.4 and 0.3, respectively, but can be varied to explore different dynamical behaviours.

Characteristics of the Henon Map
Sensibility in starting stage
The Henon map, like other chao systems, is highly suitable for starting predicaments. Minor changes in earlier values like x0 and y0 will increase indifferent curves and slopes, a hallmark of chaotic behaviour.

Attractor
The Henon map, like other chao systems, is highly suitable for starting predicaments. Minor changes in earlier values, such as x0 and y0, will increase indifferent curves and slopes, a hallmark of chaotic behaviour [19].

Ergodicity
The Henon map exhibits ergodic behavior, meaning that over time, the system explores the entire phase space in a statistically uniform manner. This property is useful for encryption because it ensures that the image data is thoroughly mixed.

The given image is implemented using a chaos technique.

Initialization
Choose parameters aa and bb, and initial conditions (x0,y0)(x0,y0).

Generate Chaotic Sequence
Repeat Henon map to acquire a sequence numbers. For each iteration, compute: equation

Pixel Shuffling
Use the generated sequence to determine the new positions in the single point data. For instance, mapping a correct sequence values for given data's coordinate system and rearrange the pixels accordingly.

Pixel Modification
Use the sequence to modify the pixel values, such as by XORing the pixel values with the generated chaotic values.

Decryption
To decrypt the image, reverse the process using the same Henon map parameters and initial conditions. **Fig 4**.

Brownian Motion
This Technique was invented by botanist Robert Brown in 1827 for a liquid particle moves faster and finds the result of the movement in liquid [20]. It serves as a fundamental concept in various scientific fields, including physics, finance, and mathematics. **Fig 4** shows 2-d Brownian motion map for 6000 iterations with coordinates as a = 1.5 and b = 0.6.

Characteristics of Brownian Motion
Step 1: Randomness
Brownian motion is characterized by its randomness and unpredictability. Each particle moves in a random direction at each time step, resulting in a stochastic or random walk.

Step 2: Continuous Path
The path of a particle undergoing Brownian motion is continuous but highly irregular, with no smooth segments. The trajectory appears as a jagged, fractal-like curve.

Step 3: No Memory
Brownian motion has the Markov property, meaning its upcoming position in this particle is conduct only on its present position but not in previous work.

Step 4: Scale Invariance
Statistical properties of Brownian motion are scale-invariant, meaning that the process looks the same at different time scales [21]. This fractal-like property is important in various applications.

$$X = r \sin a \cos b$$
$$Y = r \sin a \sin b$$
$$Z = r \cos a \quad (2)$$

Therefore $0 \leq r \leq +\infty$, $0 \leq b \leq 2\pi$, and $0 \leq a \leq \pi$

Simulation of BM
Brownian motion (BM) is simulated using computational methods. Here's a basic outline of how it can be implemented:

Step 1: Initialization
Set the initial position B(0)=0.
Choose the time step Δt and the number of steps N.

Step 2: Generate Increments
For each time step i, generate a random increment ΔBi with a natural dispersion including mean 0 and variability Δt: ΔBi~N(0,Δt)

Step 3: Update Position
Update the position of the particle for each time step: B(ti+1)=B(ti)+ΔBi

Step 4: Repeat
Repeat the process for NN steps to generate the trajectory of the particle
.

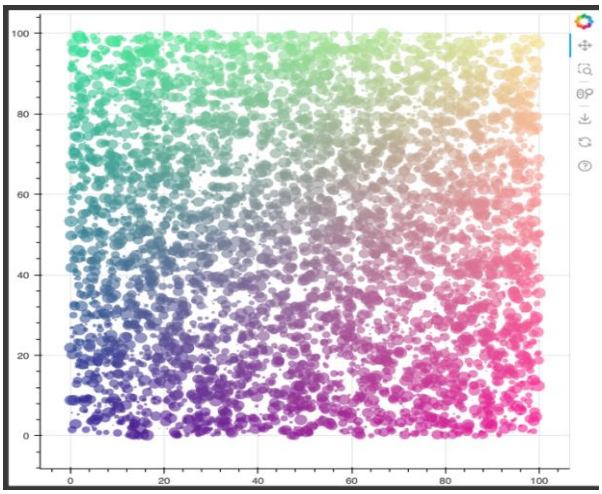

Fig 4. 2-D Brownian Motion Map for 6000 Iterations with Coordinates as a = 1.5 and b = 0.6.

Chaotic Chen System (CSS)
It's a 3D architecture, continuous-time dynamical network known for its chaotic behaviour. Introduced by Guanrong Chen in 1999, it is a modification of the Lorenz network and it was widely referred in this explanation and its applications, including secure communication and encryption [22]. **Fig 5** shows the chen system along X, Y, Z with a,b,c directions.
Characteristics of the Chen System
The Chen network was explained in a given three coupled, nonlinear distributional formula:

$$\begin{aligned} \frac{dx}{dt} &= a(y-x) \\ \frac{dy}{dt} &= (c-a)x - xz + cy \\ \frac{dz}{dt} &= xy - bz \end{aligned} \tag{3}$$

Therefore, X Y Z are condition variable, and A B C are framework variables. Typically, the framework exhibits its behaviour for the variable number a=35, b=3, and c=35.

This network's fractional order can be described as below:

$$\begin{aligned} \frac{d^{\,q}x}{dt^{\,q}} &= (y-x) \\ \frac{d^{\,q}y}{dt^{\,q}} &= (c-a)x - xz + cy \\ \frac{d^{\,q}z}{dt^{\,q}} &= xy - bz \end{aligned} \tag{4}$$

Initialization
Choose parameters a b c in initial conditions

Generate Chaotic Sequence
Solve the Chen system differential equations to generate a sequence of chaotic values. For this, numerical methods like the Runge-Kutta method can be used.

Pixel Shuffling
Map the chaotic sequence to the image's coordinate system to shuffle the pixels randomly.

Pixel Modification
Use the chaotic sequence to modify the pixel values, such as by XORing the pixel values with the chaotic values

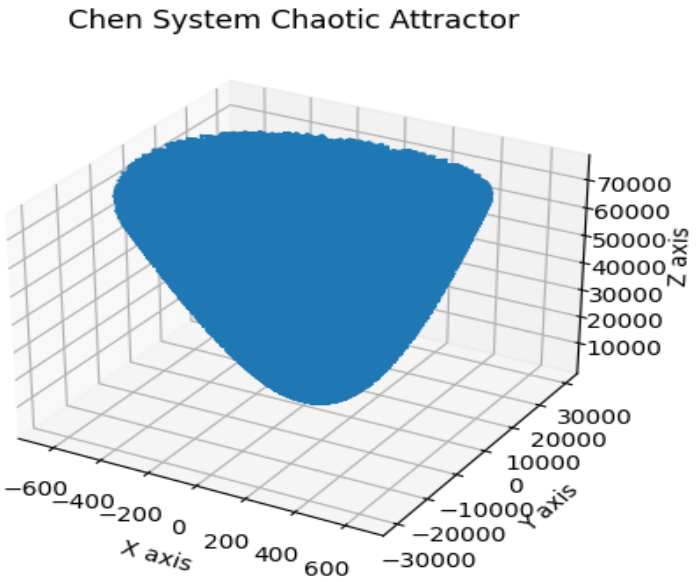

Fig 5. Chen System along X, Y, Z with a,b,c Directions.

The Proposed Algorithm
Fig 6 displays the graph by suggesting medical picture encrypt system. The architecture explains about a encryption and decryption of given images with the basic steps

Initialization
Choose values a b c are used in Chen network, and set an initial conditions (x0,y0,z0). 1.2 Set the parameters for the cryptographic algorithm (e.g., AES key).
Generate Chaotic Sequence

Following this chen network to produce a chaotic. sequence:

$$\begin{aligned} X' &= a(y - x) \\ Y' &= (c - a)x - xz + cy \\ Z' &= xy - bz \end{aligned} \tag{5}$$

Random Shuffling

Normalize the chaotic order x y z to its range in the image pixel indices.

Output the Encrypted Image

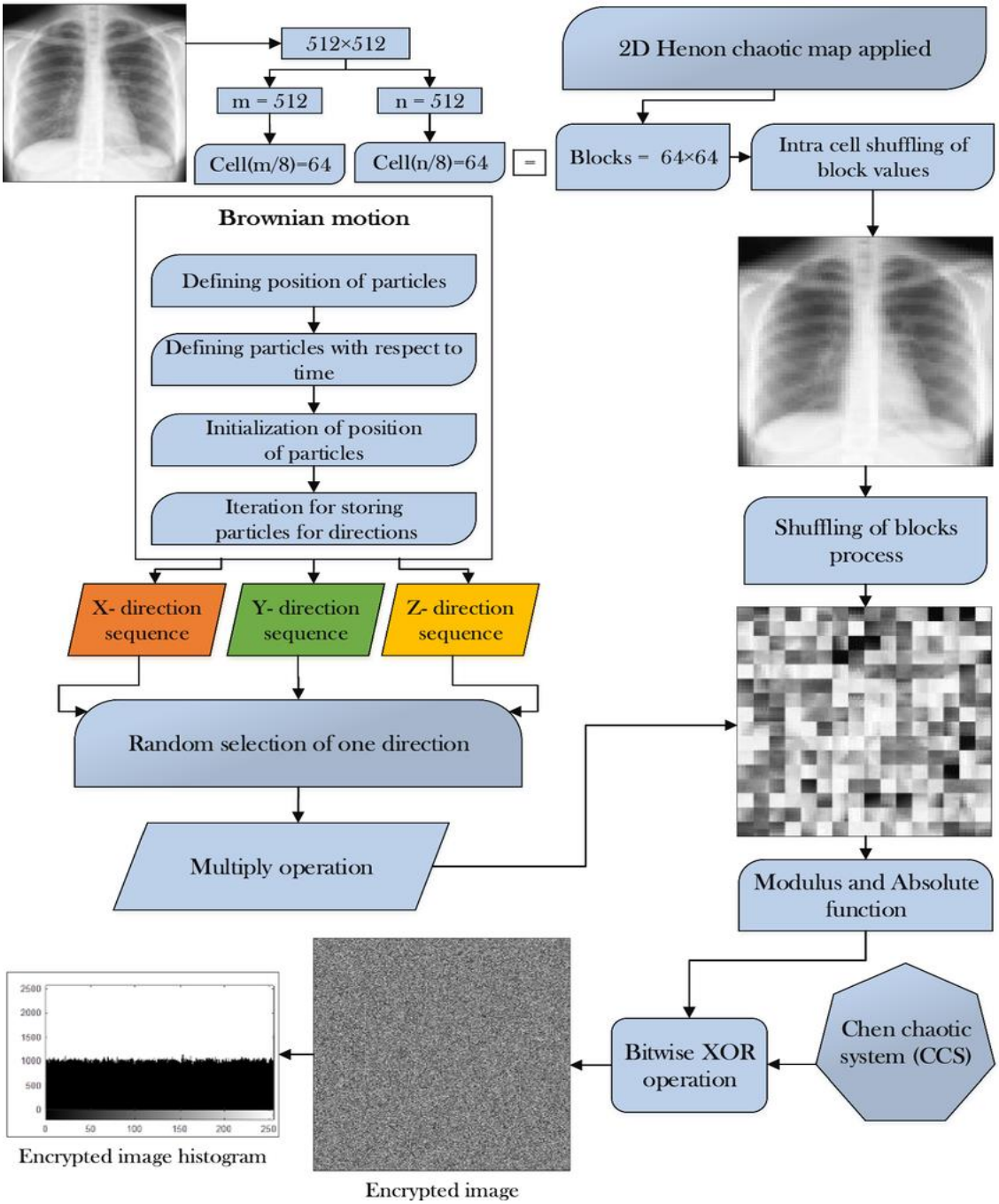

Fig 6. The Proposed Medical Cryptosystem's Flow.

Decryption Algorithm

Initialization

Use the same parameters a b c in starting stage (X0 Y0 Z0) used during encryption.

Cryptographic Decryption

Use the cryptographic algorithm (e.g., AES) to decrypt the received encrypted pixel array.

Pixel Inverse Modification

XOR the decrypted pixel values with the same chaotic values used during encryption. **Fig 7** shows the starting rotation in given models No. of Blocks = 4096 and **Fig 8** shows the next round displacement of blocks in inner side.

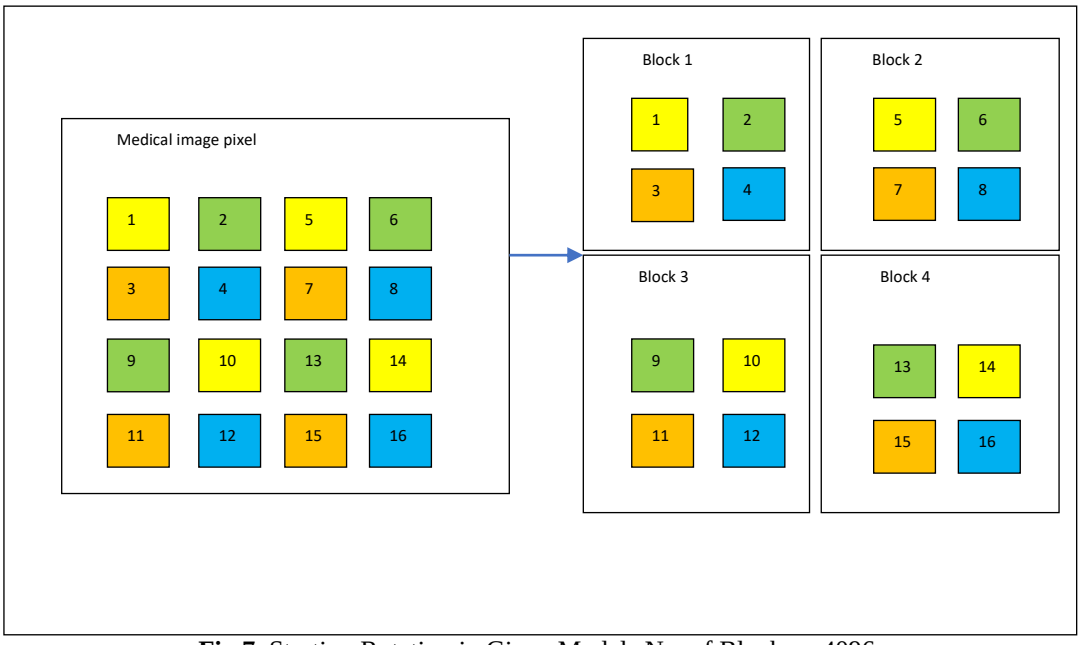

Fig 7. Starting Rotation in Given Models No. of Blocks = 4096.

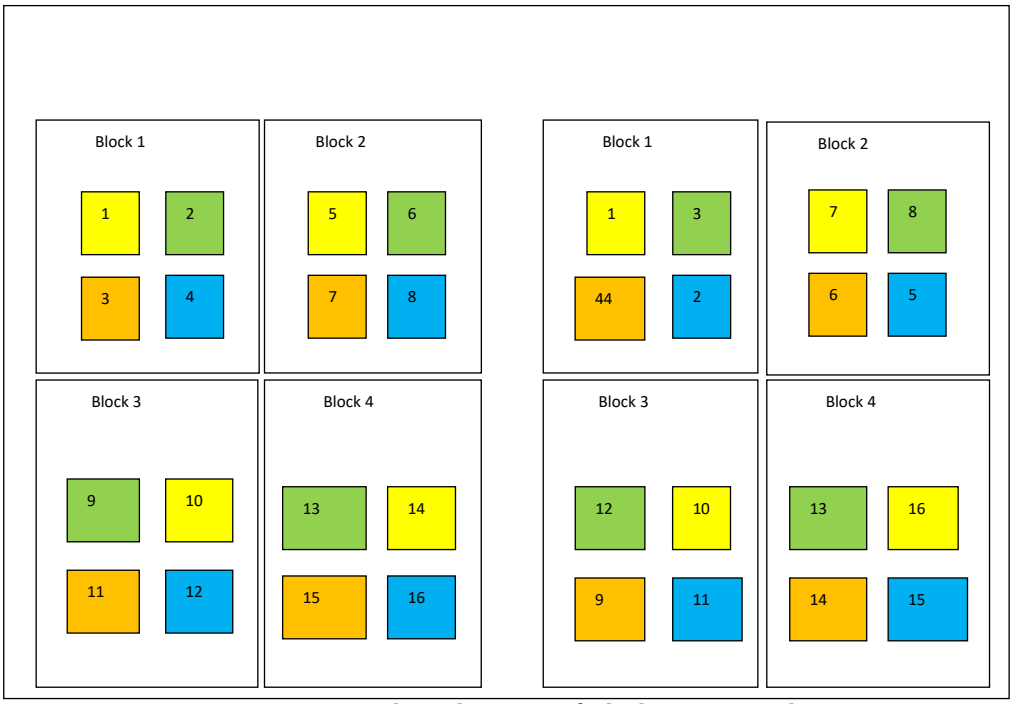

Fig 8. Next Round Displacement of Blocks in Inner Side.

Inverse Shuffling

Generate the same permutation of pixel indices using the Chen system chaotic sequence. Inversely rearrange the dot positions of the data according to the original pixel positions [23].

Output the Decrypted Image

Reshape the decrypted pixel array back into the original image dimensions. Save or display the decrypted image. **Fig 9** shows third phase displacement of blocks shuffle in inside.

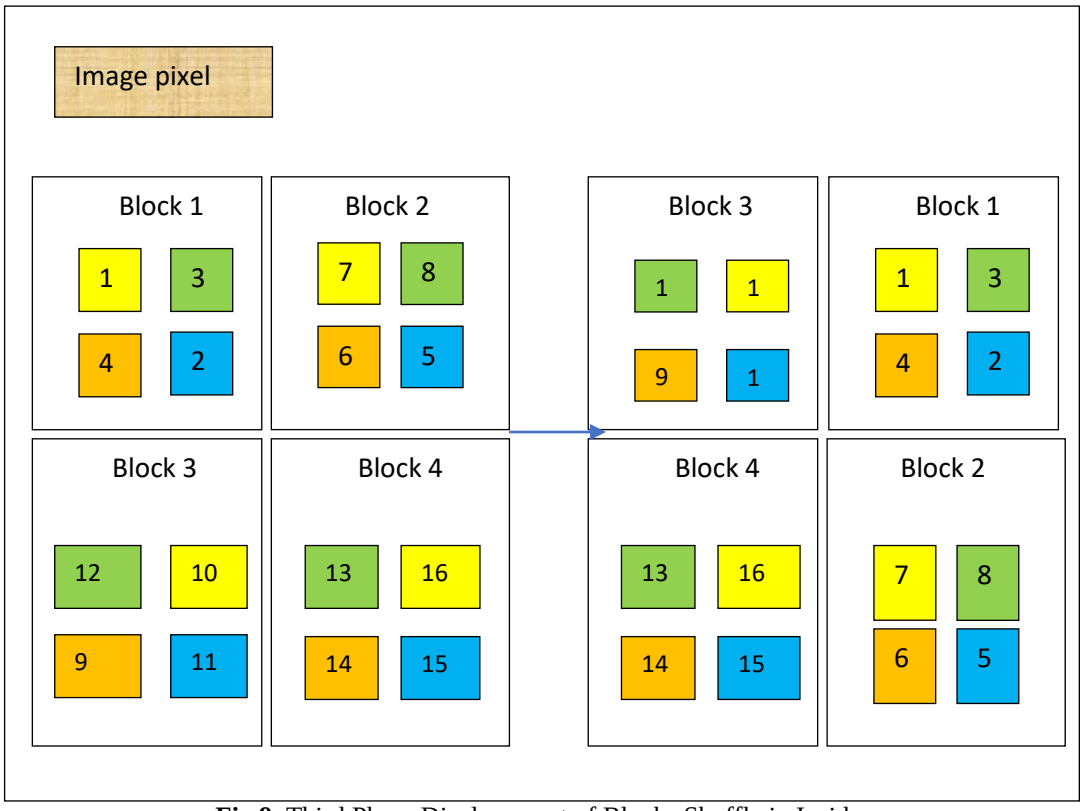

Fig 9. Third Phase Displacement of Blocks Shuffle in Inside.

IV. EXPERIMENTAL ANALYSIS AND RESULTS

Results and Analysis

The encrypted images were visually inspected and compared with the original images [24, 25]. The encrypted images were noise-like and lacked discernible patterns, ensuring that the encoded data did not reveal any information about the original data. **Fig 10** shows X-Ray of the chest original artwork, rearranging block values, and rearranging individual blocks.

Fig 10. X-Ray of The Chest Original Artwork, Rearranging Block Values, and Rearranging Individual Blocks.

Analysing Histogram

The original, encoded data became blurry.

The blurred encoded data was uniformly distributed, indicating favorable diffusion and preventing statistical attacks. **Fig 11** shows cerebral imaging initial image, permutation of block values, permutation of blocks.

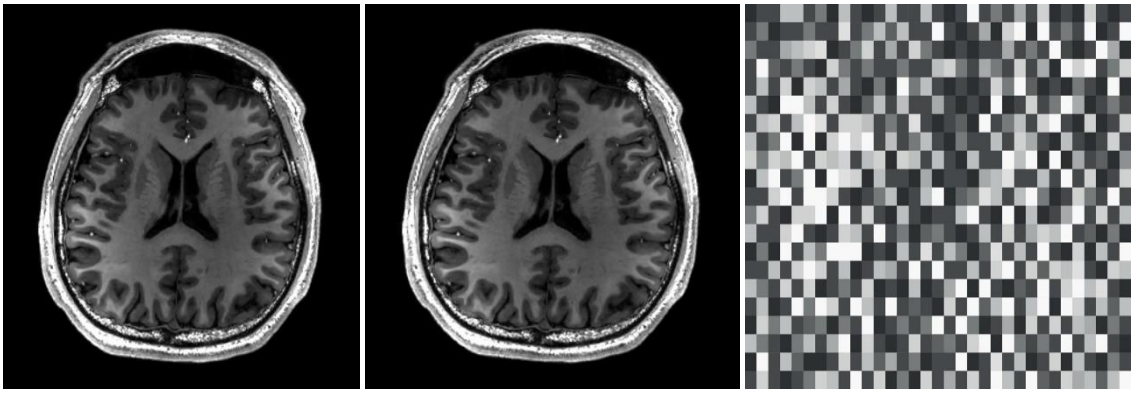

Fig 11. Cerebral Imaging Initial Image, Permutation of Block Values, Permutation of Blocks.

Correlation Coefficient

The adjacent in pixel's are three direction X Y Z axis and got result for both the unmodified data and also in encryption method [26]. **Fig 12** shows magnetic resonance picture initial image, permutation of pixel values within blocks, permutation of blocks themselves, **Fig 13** shows encryption image of the chest in three direction X Y Z, **Fig 14** depicts cerebral imaging image encrypted along the X-axis image encrypted through the Y-axis picture and Z-axis picture, **Fig 15** depicts magnetic resonance picture encrypted through X-axis, Y-axis, Z-axis picture, **Fig 16** illustrates the image of chest, brain and MR image in a histogram view and **Fig 17** illustrates graphical representation of chest data. **Fig 18** shows the graphical representation of brain data. **Fig 19** shows Graphical Representation of MR Data. **Fig 20** shows image of the three-histogram view in a 3d method.

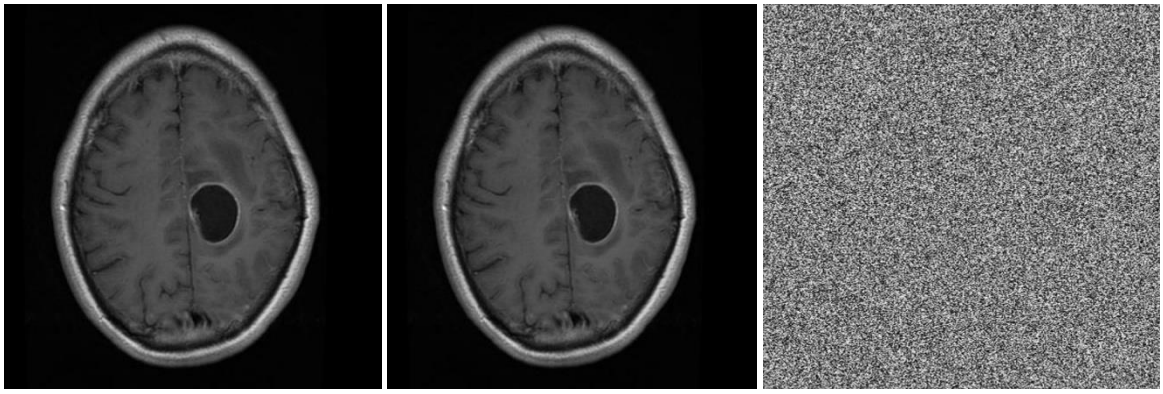

Fig 12. Magnetic Resonance Picture Initial Image, Permutation of Pixel Values Within Blocks, Permutation of Blocks Themselves.

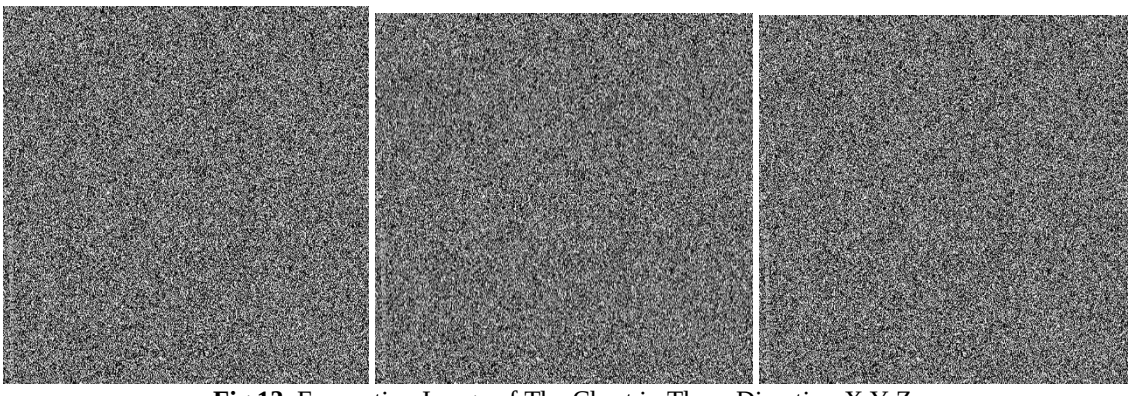

Fig 13. Encryption Image of The Chest in Three Direction X Y Z.

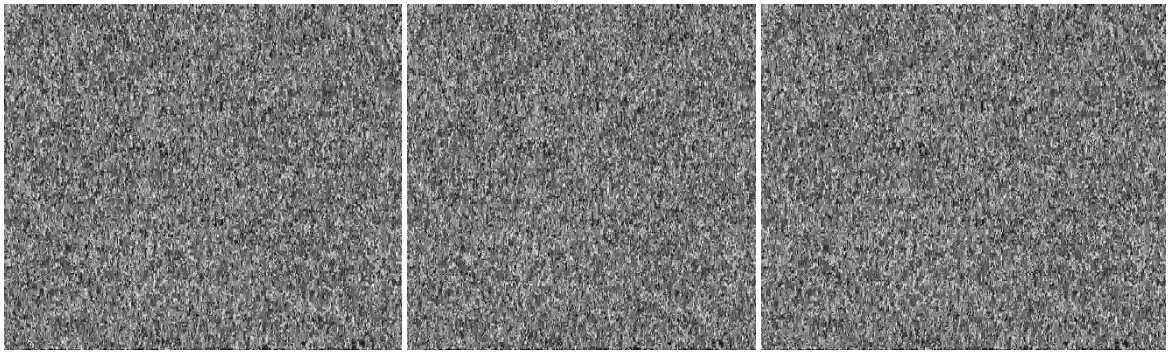

Fig 14. Cerebral Imaging Image Encrypted along The X-Axis Image Encrypted through The Y-Axis Picture and Z-Axis Picture.

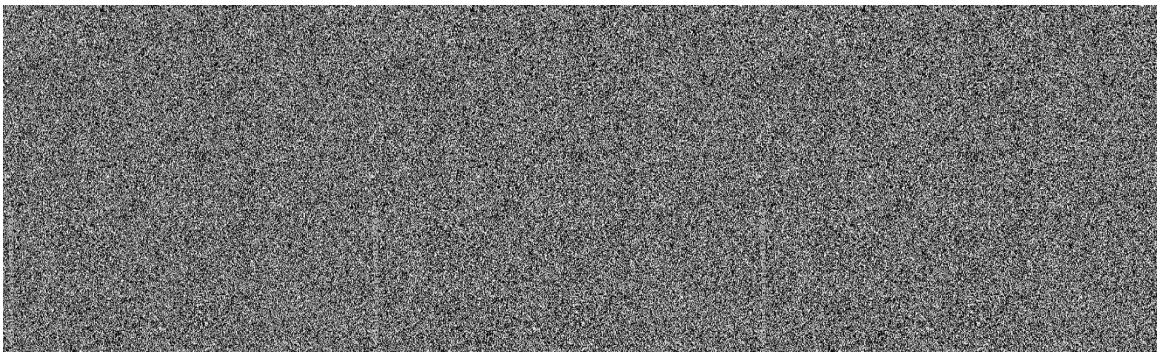

Fig 15. Magnetic Resonance Picture Encrypted through X-Axis, Y-Axis, Z-Axis Picture.

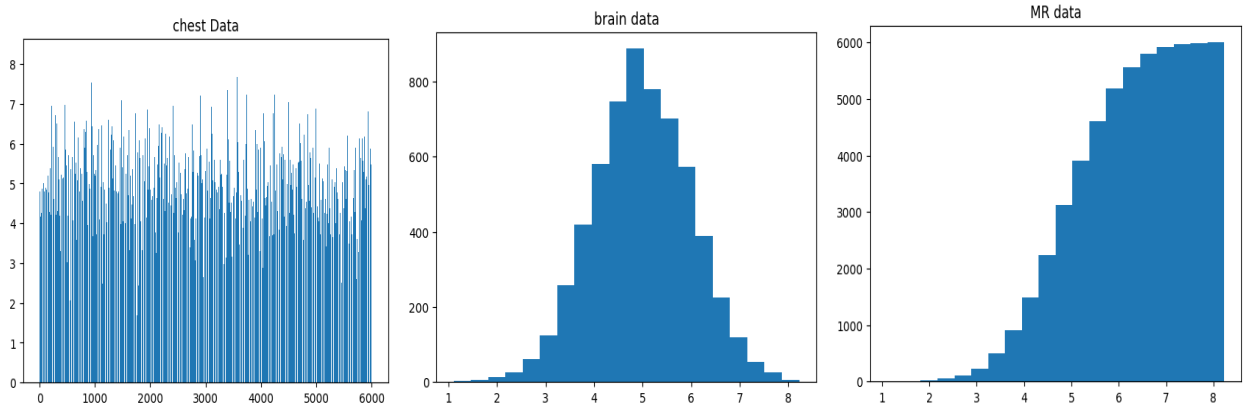

Fig 16. The Image of Chest, Brain and MR Image in a Histogram View.

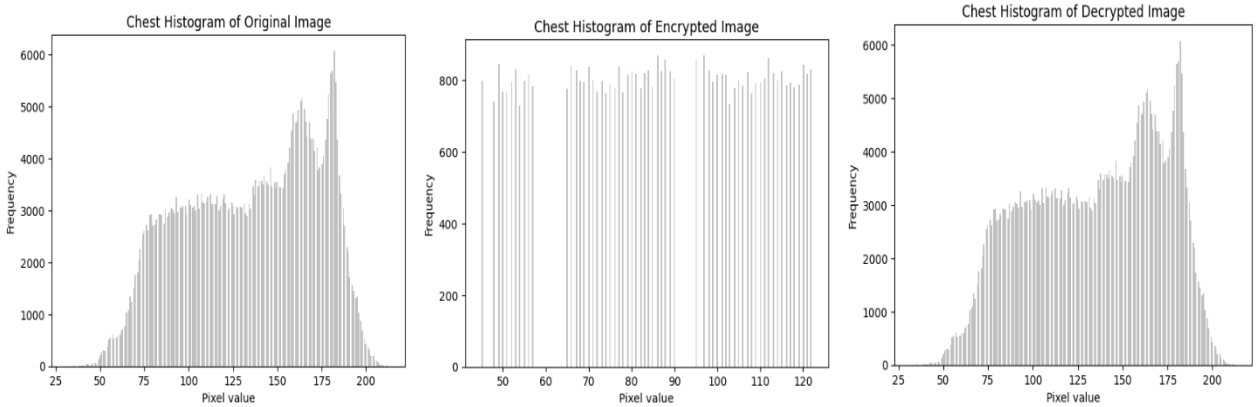

Fig 17. Graphical Representation of Chest Data.

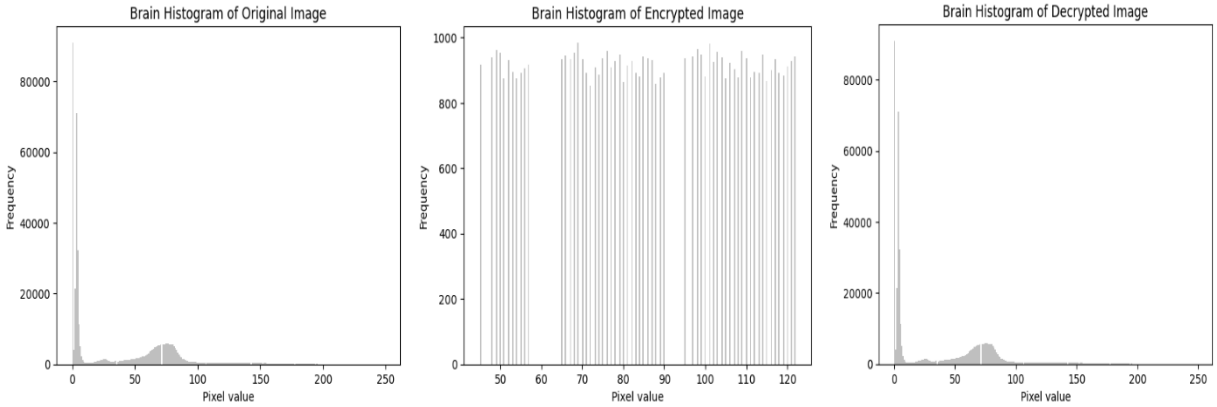

Fig 18. Graphical Representation of Brain Data.

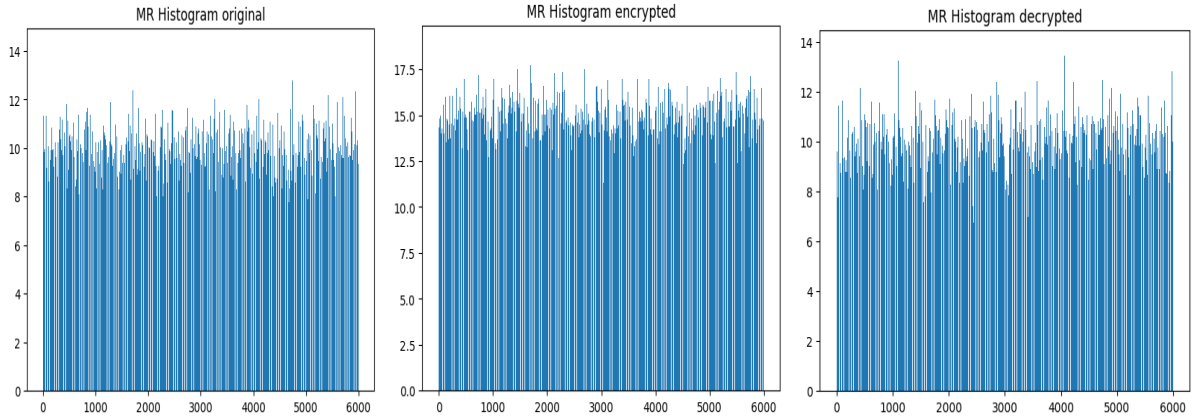

Fig 19. Graphical Representation of MR Data.

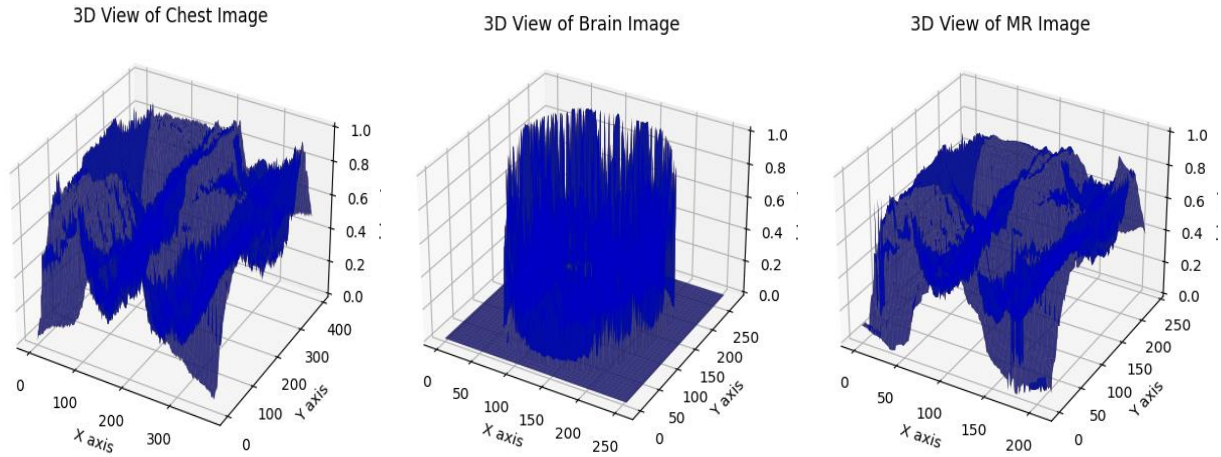

Fig 20. Image of The Three Histogram View in a 3D Method.

Analysis of Adjacent Pixel Correlation

Correlation between neighbouring pixels is a crucial characteristic to show the cipher-text image's dispersion and confusion characteristics [27]. **Fig 21** shows radiography view of a 3d method along x direction horizontally, diagonally and vertically. **Fig 22** depicts histograms of 3d display of chest images chest x-ray graphical representation along y in three different orientations: horizontally, diagonally, and vertically and **Fig 23** illustrates the histogram of chest image in 3d method as horizontally, diagonally and vertically. **Fig 24** shows pixel's correlation along X, correlation along Y, correlation along Z.

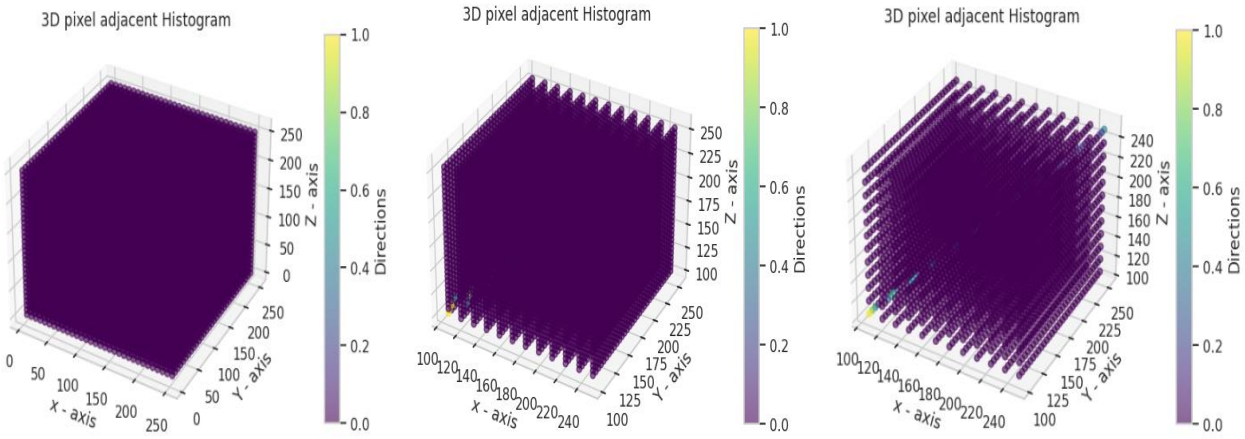

Fig 21. Radiography View of a 3d Method Along x Direction Horizontally, Diagonally and Vertically.

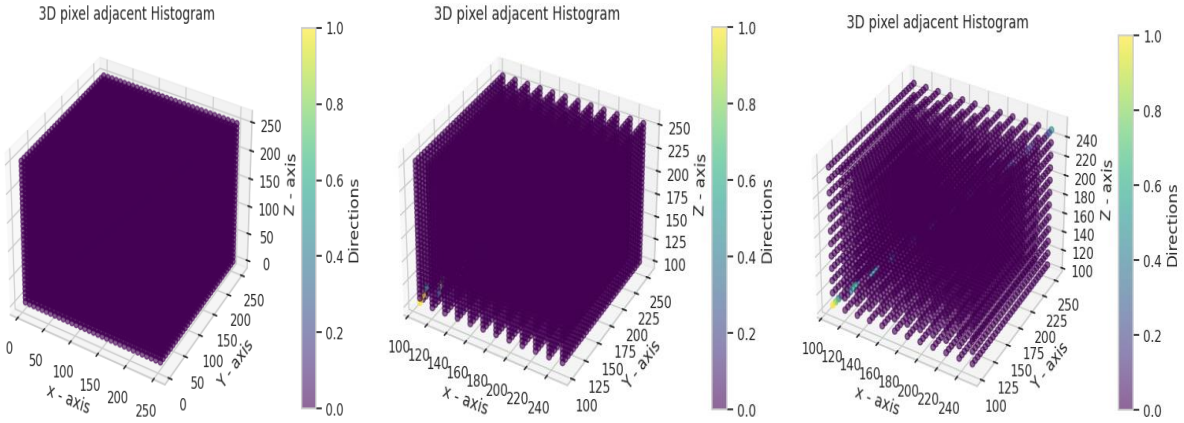

Fig 22. Histograms of 3D Display of Chest Images Chest X-Ray Graphical Representation along Y in Three Different Orientations: Horizontally, Diagonally, and Vertically.

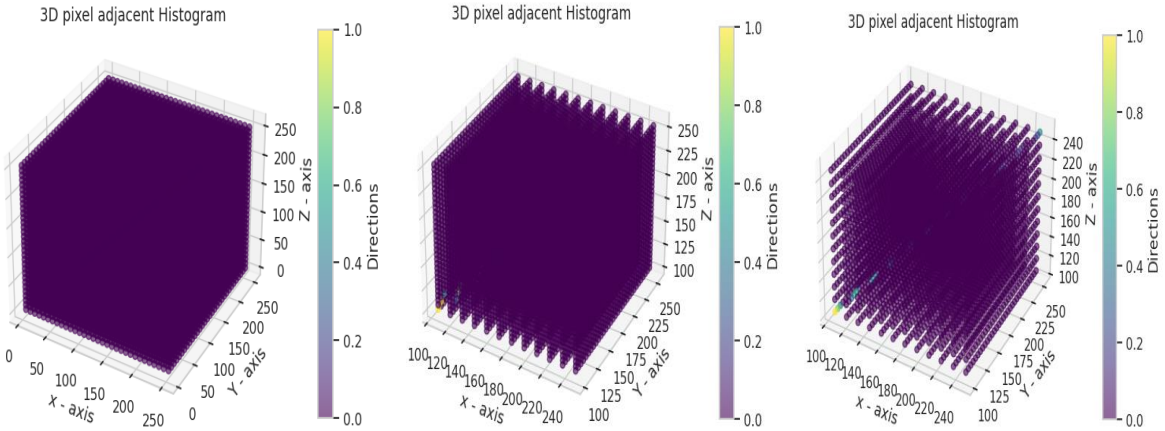

Fig 23. The Histogram of Chest Image in 3D Method as Horizontally, Diagonally and Vertically.

Correlation can be computed mathematically as follows:

$$r_{xy} = \frac{E\big((x-E(x))(y-E(y))\big)}{\sqrt{D(x)D(y)}} \tag{6}$$

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

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)^2 \tag{8}$$

Table 1. Values of the Correlation Coefficient for Every Dimension

S.No	Images	Dimensions of Plain Image			Dimension of an encrypted image		
		Hori Dim	Diag Dim	Vert Dim	Hori Dim	Diag Dim	Vert Dim
1	Thorax-X direction	0.9772	0.9459	0.9569	0.02	0.0003	0.001
2	Thorax -Y direction	0.9772	0.9459	0.8969	0.01	0.0003	0.0001
3	Thorax -Z direction	0.9772	0.9459	0.8969	0.01	0.0001	0.0001
4	Neurological organ -X direction	0.9745	0.9493	0.9378	0.01	0.0001	0.0001
5	Neurological organ -Y direction	0.9745	0.9493	0.9378	0.02	0.0002	0.0001
6	Neurological organ -Z direction	0.9745	0.9483	0.9378	0.02	0.0002	0.0001
7	MRI-X direction	0.9713	0.9412	0.8643	0.01	0.0002	0.0001
8	MRI-Y direction	0.9713	0.9412	0.8643	0.02	0.0002	0.0001
9	MRI-Z direction	0.9713	0.9412	0.8643	0.01	0.0003	0.0001

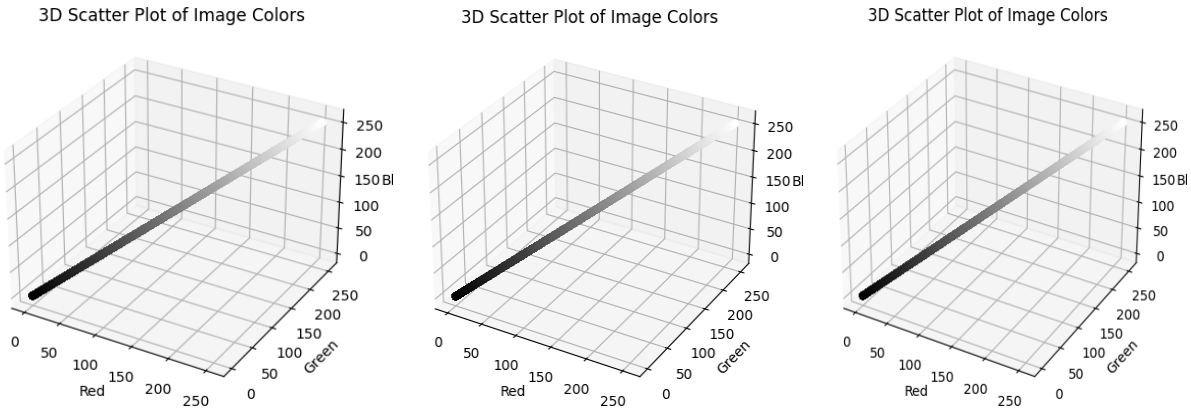

Fig 24. Pixel's Correlation along X, Correlation along Y, Correlation along Z.

Table 1 displays the results of our proposed approach for the integers [5, 18, 25, 35]. **Fig 25** shows the grayscale image in three directions and views the pixels moving in ciphertext to encrypt mode, as shown in **Fig 26–27**. The average values of the unaltered images for the chest, brain, and MR dimensions in **Table 1** are around 0.9772, 0.9493, and 0.9569, respectively. If the value is 1, it indicates a strong bidirectional connection. Researchers evaluate the values in all directions [28]. The evaluated averages of the given values are 0.02, 0.02, and 0.0001. After encryption, the image falls within the range of 0 to -1. This result demonstrates the efficiency of the proposed work.

Analysing Method with Homogeneity and Energy

In this analysis method, we find that the grey scale level vectors are closer to either one. The GLCM tables provide an illustration of statistical combinations involving pixel intensity or grey levels. If the homogeneity value is lower, it indicates the use of an encryption technique.

Fig 25. Thorax Image Histogram in x Direction.

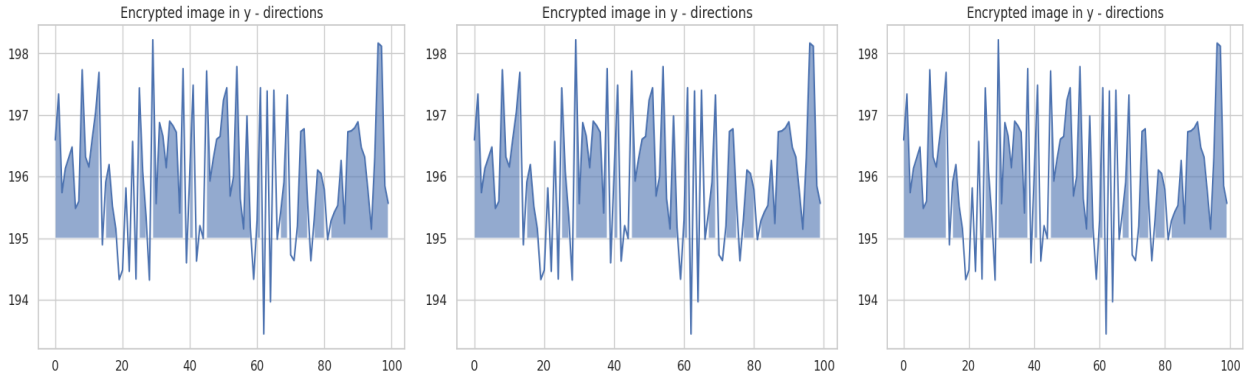

Fig 26. Thorax Image Histogram in y Direction.

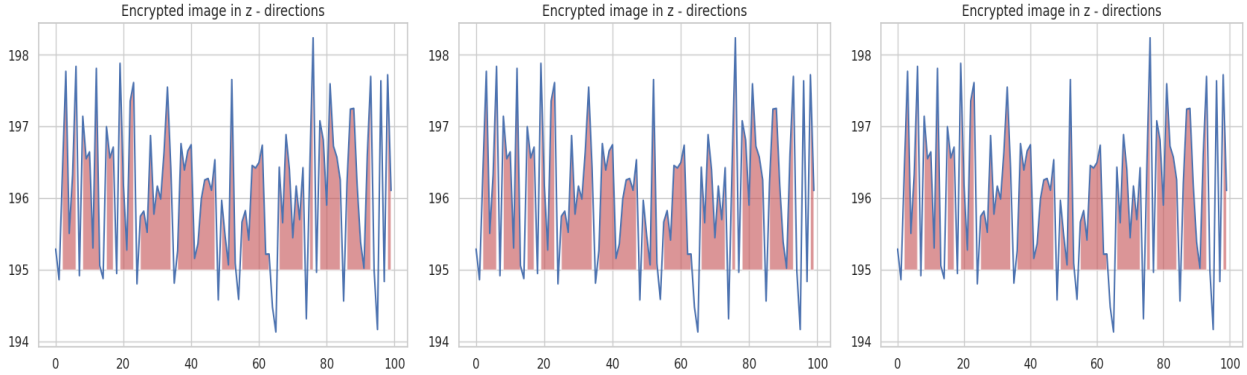

Fig 27. Thorax Image Histogram in z Direction.

Formula is:

$$H = \sum_{x,y=1}^{M} \frac{g(x,y)}{1+|x-y|} \tag{9}$$

Formula for a contrast:

$$Contrast = \sum_{i,j=1}^{M} |x - y|^2 \, p(x,y) \tag{10}$$

Therefore p(x, y) shows a generalized method of cubic model

Table 2. Table for a Direction X

S.no	Image	Consistency	Vitality	Discrepancy
1.	Thorax	0.3610	0.0182	10.4301
2.	Neurological organ	0.3616	0.0182	10.3928
3.	MRI	0.3519	0.0184	10.4276

Table 3. An investigation of Consistency, Vitality, and Discrepancy is conducted along the Y direction, and the Average Values are Calculated.

S.no	Image	Consistency	Vitality	Discrepancy
1	Thorax	0.3787	0.0182	10.4409
2	Neurological organ	0.3619	0.0173	10.1928
3	Magnetic resonance	0.3275	0.0161	10.2272

Table 4. Analysis of Consistency, Vitality, and Discrepancy is Conducted on Average Values along the Z Direction.

S.no	Image	Consistency	Vitality	Discrepancy
1	Thorax	0.3787	0.0182	10.4409
2	Neurological organ	0.3619	0.0173	10.1928
3	Magnetic resonance	0.3275	0.0161	10.2272

Table 5. Current findings from the Analysis of Consistency, Vitality, and Discrepancy

S no	Image	Consistency	Vitality	Discrepancy
1	Encrypted image	0.4533	0.0198	6.9123
2	Encrypted image	0.9214	0.1943	0.2196

Another quantity that can be computed using the GLCM is energy.

The following is the equation used for calculating energy:

$$\text{Vitality} = p\,(x\,,\,y)^2 \tag{11}$$

where the total count of grey-level co-occurrence. matrices is indicated by symbol p(x, y).

Tables 2, 3, and **4** display the same value as the given image. For each image, we obtain an average value, which is 0.3787 in all three directions. In contrast, other plans are recommended. **Table 5** displays the output. The output in **Table 5** yields a value that is relatively small. Achieving a low value demonstrates that plaintext can view the cryptosystem from all three directions. However, the result is significantly higher than the values that were achieved. Therefore, it establishes the superiority of the proposed work over other existing schemes by attacking them more effectively.

Analysis of Differential Attacks

An encryption algorithm must possess immunity to divergent attacks, which is a crucial characteristic [29]. There are two tests that can assess resistance to different types of attacks: (1) the rate at which the count of pixels shifts with the average amount of changes. We conducted these tests on two scrambled photos, ensuring that the accompanying unencrypted images differed by only one pixel.

NPCR and UACI

NPCR and UACI were calculated to analyse the perceptiveness of the encoded work with small execution in plaintext.

NPCR: 99.61%

UACI: 33.52%

High NPCR and UACI counts confirm with encryption algorithm is highly perceptiveness for minor modification in the cipher text, ensuring robust security. **Table 6** shows NPCR and UACI comparison, **Table 7** shows NPCR and UACI value in 3-D and **Table 8** shows implemented value of MSE and PSNR scheme.

Given formula for NPCR is

$$\text{NPCR} = \frac{\sum_{ij} D(i,j)}{M\ X\ N}\ X\ 100\% \tag{12}$$

The data of the two given dataset present equal count in plaintext, as D(i, j) is equal to 0. Conversely plain text of two given data have different values same as D(i, j) is equal to 1. The maximum threshold for the NCPR is set at 100%, but, in order for a cryptosystem to be considered effective, the NCPR value should exceed 98.9%.

Unified Average Changing Intensity

The UACI test was implemented for calculating degree of median intensity change among two encrypted text images, provided that there is a one-pixel variance between the two associated unencrypted data.

Formula of UACI is:

$$UACI = \frac{1}{M\ X\ N}\left[\sum_{i\ j} \frac{|c1\ (i,j)\ -\ c2(i,j)|}{255}\right]\ X\ \ 100\ \% \tag{13}$$

Table 6. NPCR and UACI Comparison

S.No	Images	Direction	NPCR count	UACI count
1	Thorax	Direction X	98.92	35.76
2	Thorax	Direction Y	98.99	35.81
3	Thorax	Direction Z	98.90	35.12

Table 7. NPCR and UACI Value in 3-D

S.No	Medical data	Diagonals	NPCR accuracy	UACI accuracy
1	Thorax	X Axis	99.92	35.76
2	Thorax	Y Axis	99.99	35.81
3	Thorax	Z Axis	98.90	35.12
4	Neurological organ	X Axis	98.91	35.72
5	Neurological organ	Y Axis	98.92	35.02
6	Neurological organ	Z Axis	98.97	35.98
7	MRI	X Axis	98.96	35.65
8	MRI	Y Axis	98.92	35.95
9	MRI	Z Axis	98.64	35.05

Table 8. Implemented Value of MSE and PSNR Scheme

S No	Image	x Axis	y Axis	z Axis	x Axis	y Axis	z Axis
1	Thorax	11415.76	12774.31	11131.61	6.98	6.99	6.98
2	Neurological organ	11035.54	11213.07	12092.04	6.47	6.48	6.47
3	MR	12397.32	10593.61	11633.29	6.59	6.60	6.46

Performance Evaluation

The encode and decode many times and it was measured to observe computational efficiency in my implemented algorithm [30].

Average Encryption Time: 0.56 seconds (for a 512x512 image)

Average Decryption Time: 0.55 seconds (for a 512x512 image)

The output shows the implemented work as efficient and suitable for practical applications, even in resource-constrained environments.

Security Performance

The safety of our implemented encrypt value was analysed opposite to other various intruders attack

Brute-Force Attack

It is a large key space provided by starting work with given equation in chen network makes brute-force attacks computationally infeasible.

Statistical Attack

The uniform histogram and low correlation coefficients in the result achieved by encrypt data to safe the quantitative intruders.

Differential Attack

Increased in NPCR and UACI scheme indicate in our algorithm is prevented from various intruding so in this minor correction is take place in the cipher text for achieving a exact output.

V. CONCLUSION

It offers a robust approach to protecting sensitive medical data. By combining random shuffling techniques with advanced cryptographic methods, this system ensures that medical images are securely encrypted, mitigating the risk of unauthorized access and data breaches. The shuffling process adds an additional layer of complexity by randomizing pixel positions, making it more difficult for attackers to decipher the image without the proper decryption keys. Cryptographic algorithms, such as AES or RSA, further enhance security by encrypting the shuffled data using strong, widely-accepted standards. This dual-layered protection preserves the integrity and confidentiality of medical images, which is crucial in healthcare where data privacy and security are paramount. Implementing such encryption methods not only complies with regulatory standards like HIPAA but also fosters trust between patients and healthcare providers. Furthermore, the efficiency of the system ensures that encryption and decryption processes can be carried out without significant computational overhead, making it a feasible solution for real-time applications in telemedicine and digital health systems.

CRediT Author Statement

The authors confirm contribution to the paper as follows:

Conceptualization: Attili Venkata Ramana, Vignesh M, Srinivasan R, Vishnupriya Borra, Senthilkumaran B and Desidi Narsimha Reddy; **Methodology:** Attili Venkata Ramana, Vignesh M and Srinivasan R; **Software:** Vishnupriya Borra, Senthilkumaran B and Desidi Narsimha Reddy; **Data Curation:** Srinivasan R, Vishnupriya Borra and Senthilkumaran B;

Writing- Original Draft Preparation: Attili Venkata Ramana, Vignesh M and Srinivasan R; **Visualization:** Attili Venkata Ramana, Vignesh M, Srinivasan R, Vishnupriya Borra, Senthilkumaran B and Desidi Narsimha Reddy; **Investigation:** Vishnupriya Borra, Senthilkumaran B and Desidi Narsimha Reddy; **Supervision:** Attili Venkata Ramana, Vignesh M and Srinivasan R; **Validation:** Attili Venkata Ramana, Vignesh M, Srinivasan R, Vishnupriya Borra, Senthilkumaran B and Desidi Narsimha Reddy; **Writing- Reviewing and Editing:** Attili Venkata Ramana, Vignesh M and Srinivasan R; All authors reviewed the results and approved the final version of the manuscript.

Data Availability
No data was used to support this study.

Conflicts of Interests
The author(s) declare(s) that they have no conflicts of interest.

Funding
No funding agency is associated with this research.

Competing Interests
There are no competing interests

References

[1]. G. Chen and T. Ueta, “Yet Another Chaotic Attractor,” International Journal of Bifurcation and Chaos, vol. 09, no. 07, pp. 1465–1466, Jul. 1999, doi: 10.1142/s0218127499001024.
[2]. E. N. Lorenz, “Deterministic Nonperiodic Flow,” Journal of the Atmospheric Sciences, vol. 20, no. 2, pp. 130–141, Mar. 1963, doi: 10.1175/1520-0469(1963)020.
[3]. J. Fridrich, “Symmetric Ciphers Based on Two-Dimensional Chaotic Maps,” International Journal of Bifurcation and Chaos, vol. 08, no. 06, pp. 1259–1284, Jun. 1998, doi: 10.1142/s021812749800098x.
[4]. Y. Mao, G. Chen, And S. Lian, “A Novel Fast Image Encryption Scheme Based On 3d Chaotic Baker Maps,” International Journal of Bifurcation and Chaos, vol. 14, no. 10, pp. 3613–3624, Oct. 2004, doi: 10.1142/s021812740401151x.
[5]. N. K. Pareek, V. Patidar, and K. K. Sud, “Image encryption using chaotic logistic map,” Image and Vision Computing, vol. 24, no. 9, pp. 926–934, Sep. 2006, doi: 10.1016/j.imavis.2006.02.021.
[6]. R. Rhouma and S. Belghith, “Cryptanalysis of a new image encryption algorithm based on hyper-chaos,” Physics Letters A, vol. 372, no. 38, pp. 5973–5978, Sep. 2008, doi: 10.1016/j.physleta.2008.07.057.
[7]. L. Kocarev and Z. Tasev, “Public-key encryption based on Chebyshev maps,” Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS ’03., vol. 3, pp. III-28-III–31, doi: 10.1109/iscas.2003.1204947.
[8]. S. Lian, J. Sun, and Z. Wang, “A block cipher based on a suitable use of the chaotic standard map,” Chaos, Solitons & Fractals, vol. 26, no. 1, pp. 117–129, Oct. 2005, doi: 10.1016/j.chaos.2004.11.096.
[9]. Wang, X., & Zhang, Q. (2012). A color image encryption algorithm based on chaotic maps. *Journal of Computers*, 7(5), 1233-1240.
[10]. k. Zhu, C., Sun, K., Zhu, Z., & Tao, C. (2012). An image encryption algorithm based on hyper-chaos. *Nonlinear Dynamics*, 70, 861-866.
[11]. A. Kanso and N. Smaoui, “Logistic chaotic maps for binary numbers generations,” Chaos, Solitons & Fractals, vol. 40, no. 5, pp. 2557–2568, Jun. 2009, doi: 10.1016/j.chaos.2007.10.049.
[12]. Yadav, R. S., Kumar, A., & Rana, V. S. (2014). Medical image encryption using improved chaotic based encryption technique. *Proceedings of the IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, 634-639.
[13]. M. S. Baptista, “Cryptography with chaos,” Physics Letters A, vol. 240, no. 1–2, pp. 50–54, Mar. 1998, doi: 10.1016/s0375-9601(98)00086-3.
[14]. T. Xiang, X. Liao, G. Tang, Y. Chen, and K. Wong, “A novel block cryptosystem based on iterating a chaotic map,” Physics Letters A, vol. 349, no. 1–4, pp. 109–115, Jan. 2006, doi: 10.1016/j.physleta.2005.02.083.
[15]. Zhu, H., & Liu, J. (2015). A robust and secure image encryption scheme based on hyperchaotic system and singular value decomposition. *Journal of Computational and Theoretical Nanoscience*, 12(5), 715-722.
[16]. S. Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative Encryption and Watermarking in Video Compression,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 6, pp. 774–778, Jun. 2007, doi: 10.1109/tcsvt.2007.896635.
[17]. Alfalou, A., & Bouridane, A. (2013). Robust and secure image encryption based on chaotic maps and compressive sensing. *Signal Processing: Image Communication*, 28(10), 1242-1254.
[18]. C. Fu, J. Chen, H. Zou, W. Meng, Y. Zhan, and Y. Yu, “A chaos-based digital image encryption scheme with an improved diffusion strategy,” Optics Express, vol. 20, no. 3, p. 2363, Jan. 2012, doi: 10.1364/oe.20.002363.
[19]. Y. Zhou, L. Bao, and C. L. P. Chen, “A new 1D chaotic system for image encryption,” Signal Processing, vol. 97, pp. 172–182, Apr. 2014, doi: 10.1016/j.sigpro.2013.10.034.
[20]. Abd El-Latif, A. A., Niu, X., Li, L., Wang, N., & El-Samie, F. E. A. (2012). A new approach to chaotic image encryption based on the modified Henon map. *Nonlinear Dynamics*, 70, 2389-2399.
[21]. Ye, R., Wang, X., Zhang, X., & Liu, S. (2014). A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. *Optics and Lasers in Engineering*, 62, 1-11.
[22]. El-Samie, F. E. A., & Abd El-Latif, A. A. (2012). A hybrid chaotic system and cyclic elliptic curve for image encryption. *Signal Processing: Image Communication*, 27(3), 292-304.
[23]. X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, “A novel chaotic image encryption scheme using DNA sequence operations,” Optics and Lasers in Engineering, vol. 73, pp. 53–61, Oct. 2015, doi: 10.1016/j.optlaseng.2015.03.022.
[24]. Wu, Y., & Hu, W. (2012). Chaos-based image encryption using plaintext-related permutation and diffusion. *Nonlinear Dynamics*, 70, 867-874.
[25]. Wang, X., Liu, Y., & Bao, X. (2011). Image encryption algorithm based on hyper-chaotic system and dynamic S-boxes. *IET Information Security*, 5(2), 111-116.

[26]. Pisarchik, A. N., & Zanin, M. (2008). Chaotic map cryptography and secure communication: Principles and applications. *Nonlinear Dynamics*, 56, 341-352.
[27]. 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, Jul. 2004, doi: 10.1016/j.chaos.2003.12.022.
[28]. Parvaz, R., & Homayounpour, M. M. (2011). A fast chaotic encryption scheme based on piecewise linear chaotic maps. *Physics Letters A*, 375(34), 3924-3932.
[29]. Tong, X., & Cui, Y. (2012). Image encryption algorithm based on the image decomposition. *Optics Communications*, 285(4), 1065-1071.
[30]. Zhu, H., & Li, Y. (2013). A novel image encryption scheme based on a chaotic system and an image block cipher. *Signal Processing*, 93(11), 3118-3129.