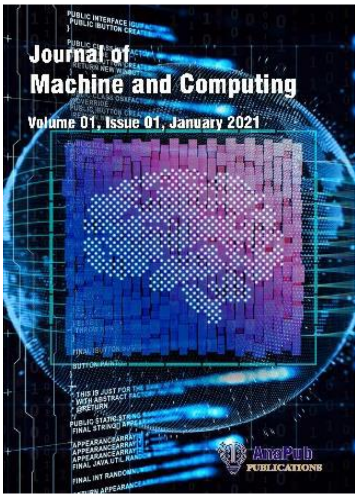
Journal Pre-proof



Secure Medical Image Encryption Using Random Shuffling and Cryptography

Attili Venkata Ramana, Vignesh M, Srinivasan R, Vishnupriya Borra, Senthilkumaran B and Desidi Narsimha Reddy

DOI: 10.53759/7669/jmc202505009

Reference: JMC202505009

Journal: Journal of Machine and Computing.

Received 15 April 2024

Revised form 28 August 2024

Accepted 14 October 2024

Please cite this article as: Attili Venkata Ramana, Vignesh M, Srinivasan R, Vishnupriya Borra, Senthilkumaran B and Desidi Narsimha Reddy, “Secure Medical Image Encryption Using Random Shuffling and Cryptography”, Journal of Machine and Computing. (2025). Doi: https://doi.org/10.53759/7669/jmc202505009

SECURE MEDICAL IMAGE ENCRYPTION USING RANDOM SHUFFLING AND CRYPTOGRAPHY

Dr.Attili Venkata Ramana
Associate Professor,
Department of Computer Science and Engineering -Data Science,
Geethanjali College of Engineering and Technology,
Cheeryala, Kesara, Hyderabad, Telangana, India
Email : avrrdg@gmail.com

M.Vignesh
M.Tech Chemical Engineering,
Sri Venkateswara College of Engineering, Sriperumbudur, Tamil Nadu, India
Email: mvignesh290102@gmail.com

Dr.R.Srinivasan
Associate Professor & Head
Department of Computer Science, SLS MAVMM Ayira Vaisya College, Madurai, Tamil Nadu, India.
Email: srinithilak@gmail.com

Vishnu[illegible] Bo[illegible]
Assistant Professor in CSE Department,
KLEF Deemed to be University,
Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India
Email: vishup[illegible]ab@kluniversity.in

Dr.B.Senthilkumaran
Assistant Professor
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
Email: skumaran.gac16@gmail.com

Mr.Desidi Narsimha Reddy,
Data Consultant (Data Governance, Data Analytics: Enterprise Performance Management, AI & ML),
[illegible]niks consulting LLC, 101 E Park Blvd Suite 600, Plano, TX 75074, United States.
dn.narsimha@gmail.com

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.

Encryption Process:

1. **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.

2. **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.

3. **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.

4. **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 [1[illegible]].

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.

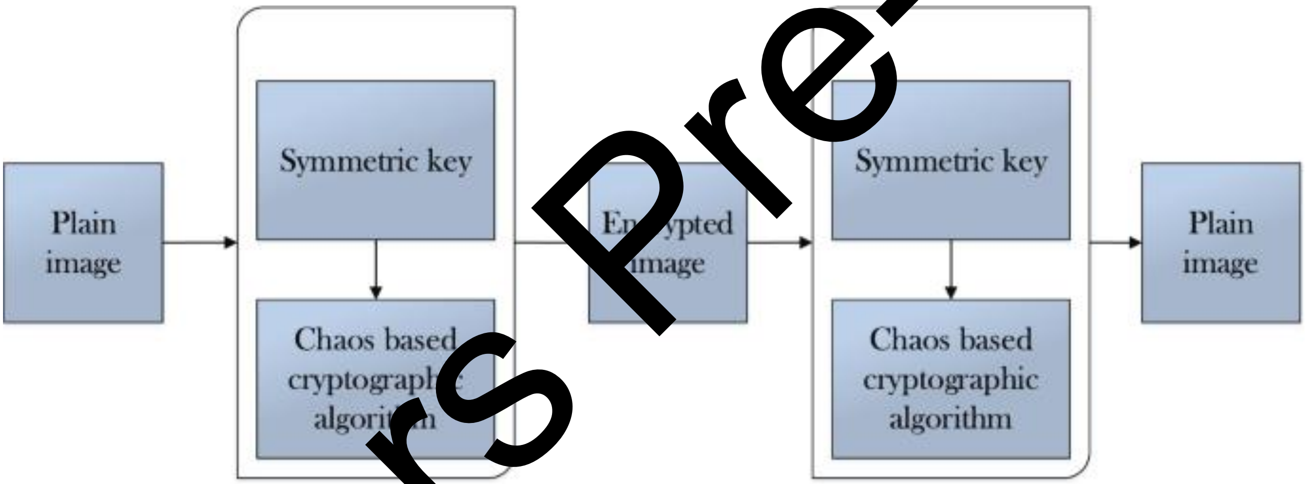


Fig 1. Displays a schematic chart illustrating the process in cryptography key for both encode and decode.

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.

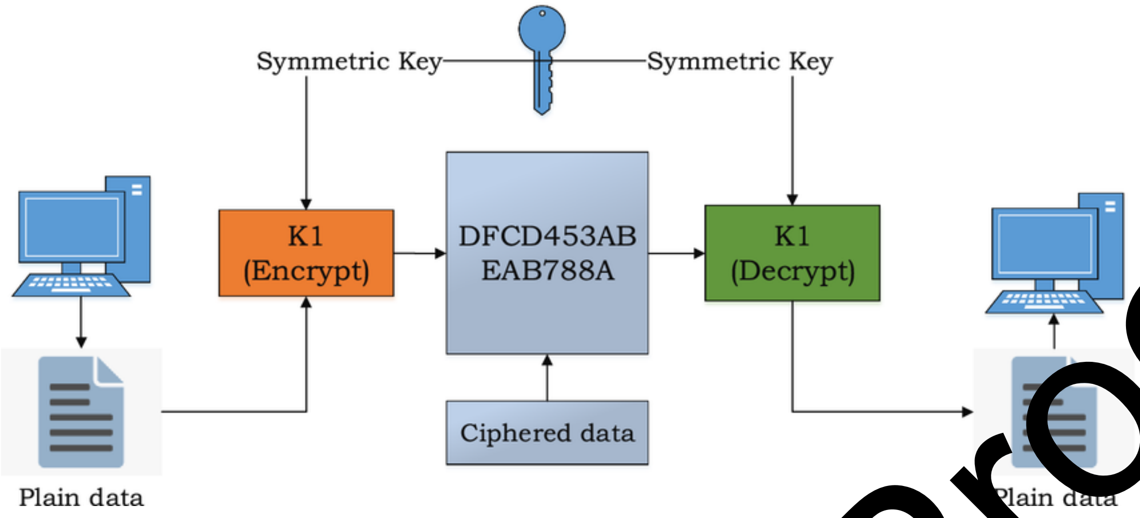


Fig 2. Depicts an alternative perspective on the process of symmetric key encryption and decryption.

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:** Hua, Y., et al. ([illegible]) leveraged the Logistic Map 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:** Pa[illegible]k, [illegible] K., et al. (2006) utilized the Lorenz System 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: Zhang, Y (2013) 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:** Wang, X., et al. (2015) 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: Liu, H., et al. (2012).This combination leveraged AES's strong cryptographic properties and the unpredictability of chaotic sequences, resulting in enhanced security and performance. **DES and Chaos:** Patidar, V., et al. (2011) explored the 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.

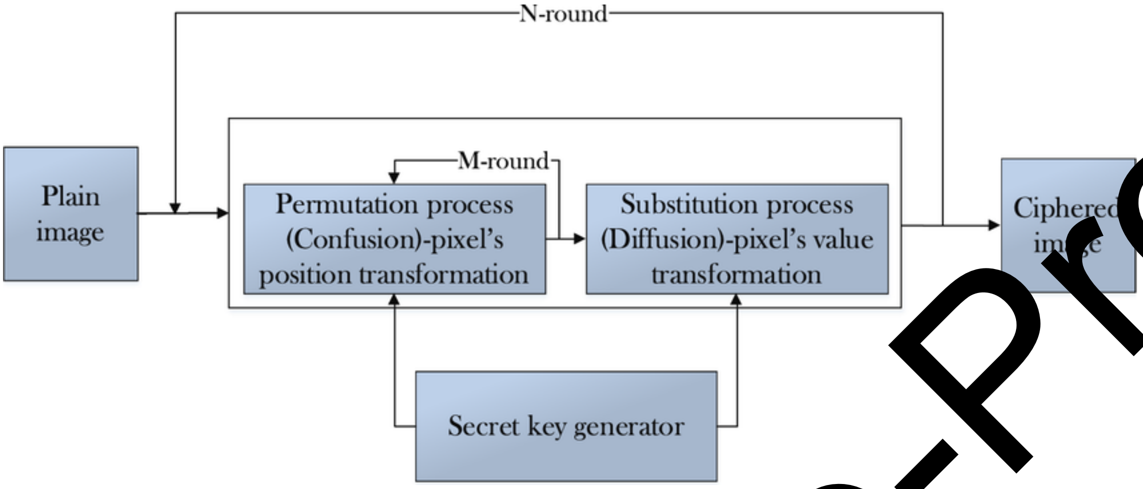


Fig 3. ***Illustrates the process of pixel permutation and substitution in each round.***

Comparative Analysis

Comparative studies have shown that chaos-based encryption schemes often outperform traditional methods in terms of security and efficiency. For instance, Pareek, N.K. (2010) 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:

I) 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. [13][14].

ii) 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.

iii) 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.

iv) 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.

v) 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.

vi) 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 behaviour.

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. Figure 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.

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:

A 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.

$$X = r \sin a \cos b$$

$$Y = r \sin a \sin b$$

$$Z = r \cos a \tag{2}$$

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 N steps to generate the trajectory of the particle.

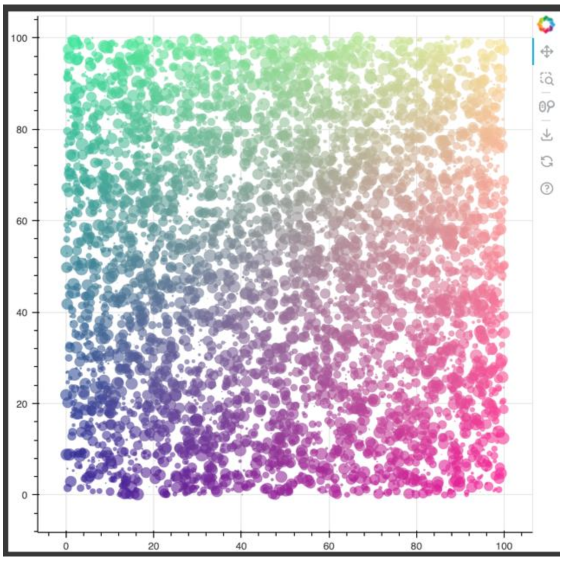


Fig 4. 2-D Brownian motion map for 6000 iterations with coordinates as [illegible] and b = 0.6

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].

Characteristics of the Chen System:

The Chen network was explained in a given three coupled nonlinear distributional formula:

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

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:

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

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

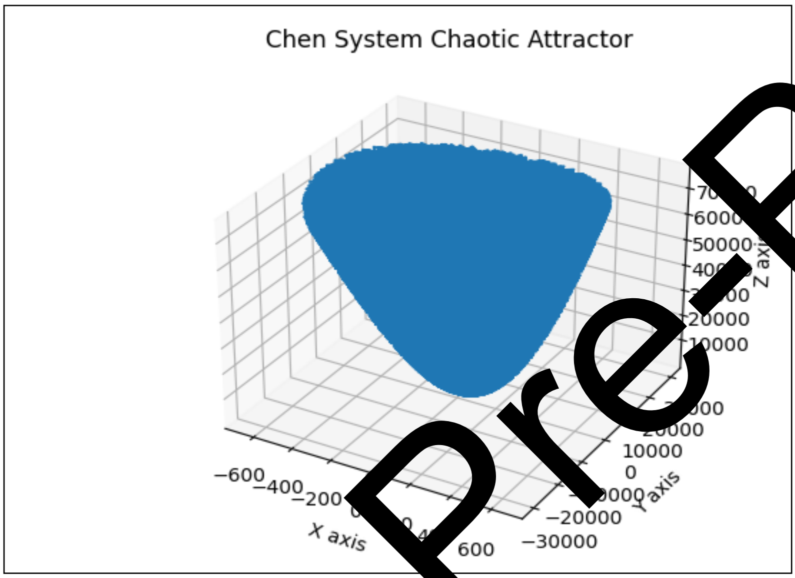


Fig. 5 Chen system along X,Y,Z with a,b,c directions

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

1. 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).

2. Generate chaotic sequence - Following this chen network to produce a chaotic. sequence:

$$X' = a(y - x)$$

$$Y' = (c - a)x - xz + cy$$

$$Z' = xy - bz$$

3. Random Shuffling - Normalize the chaotic order x y z to its range in the image pixel indices.

4. Output the Encrypted Image

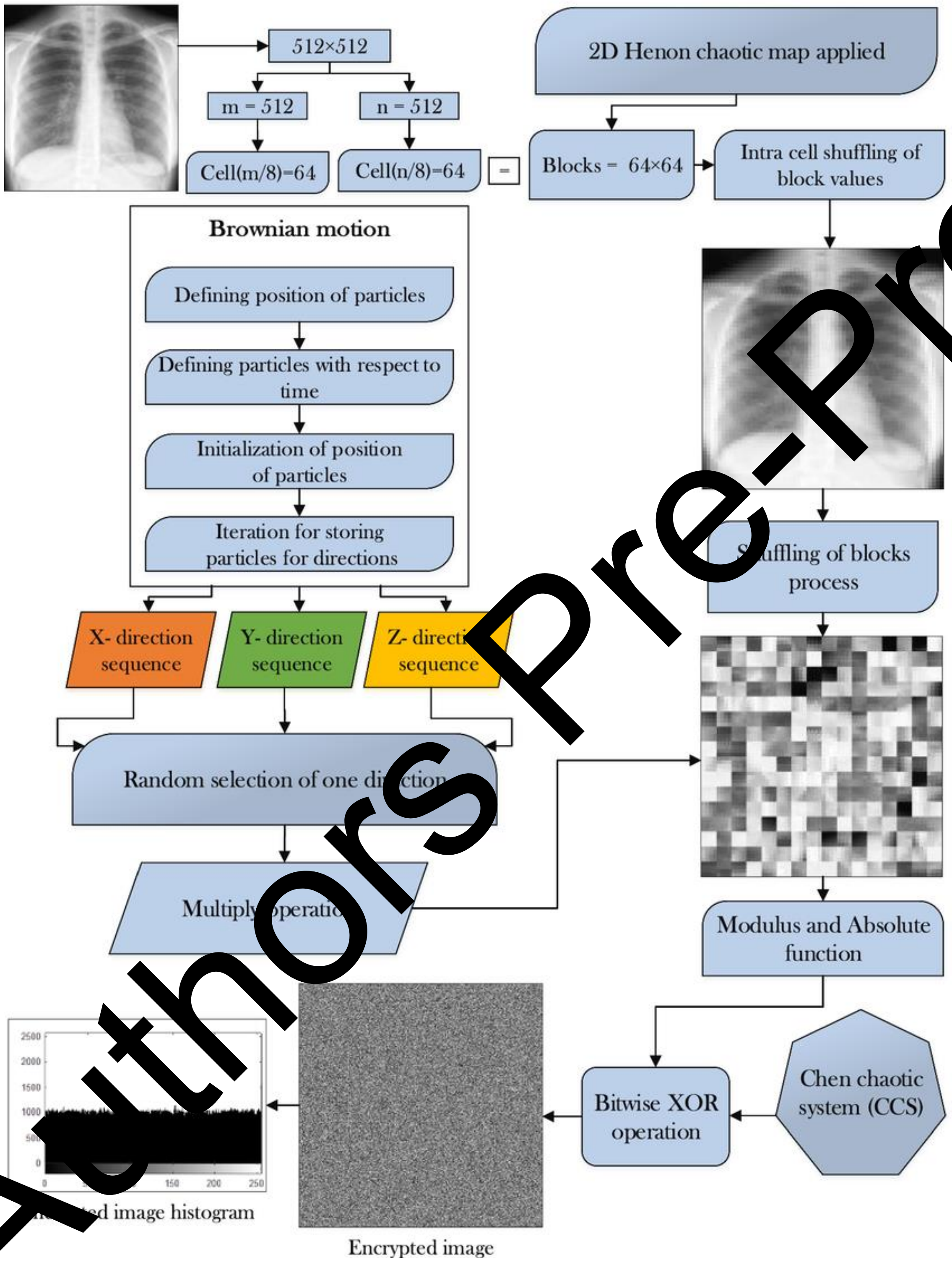


Fig 6. Diagram showing the proposed medical cryptosystem's flow

Decryption Algorithm

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

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

3. Pixel Inverse Modification - XOR the decrypted pixel values with the same chaotic values used during encryption.

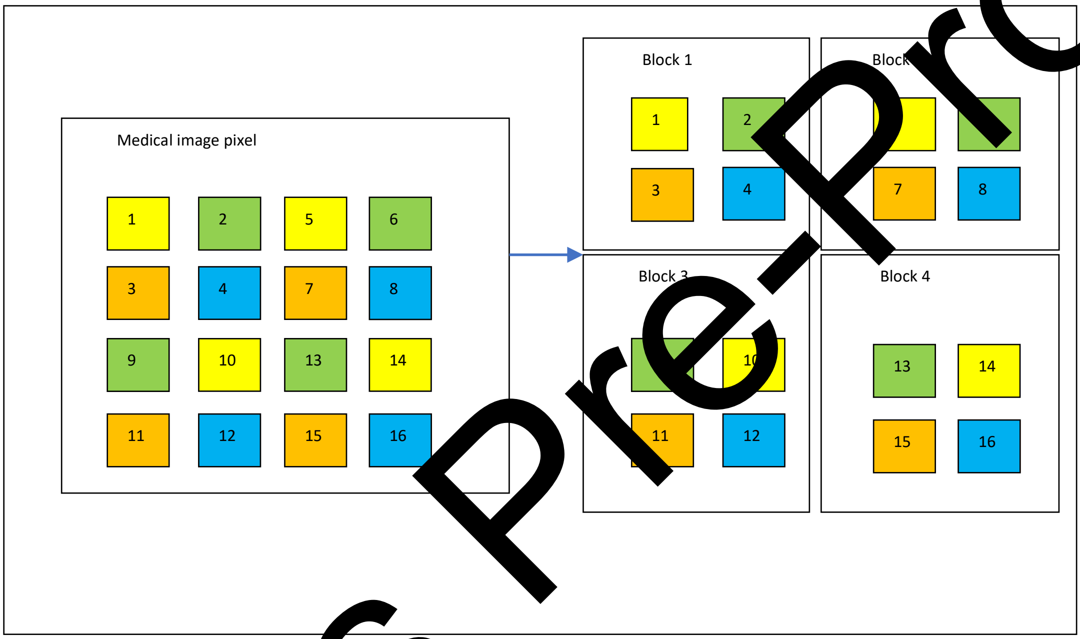


Fig 7. Starting rotation of given models No. of blocks. = 4096

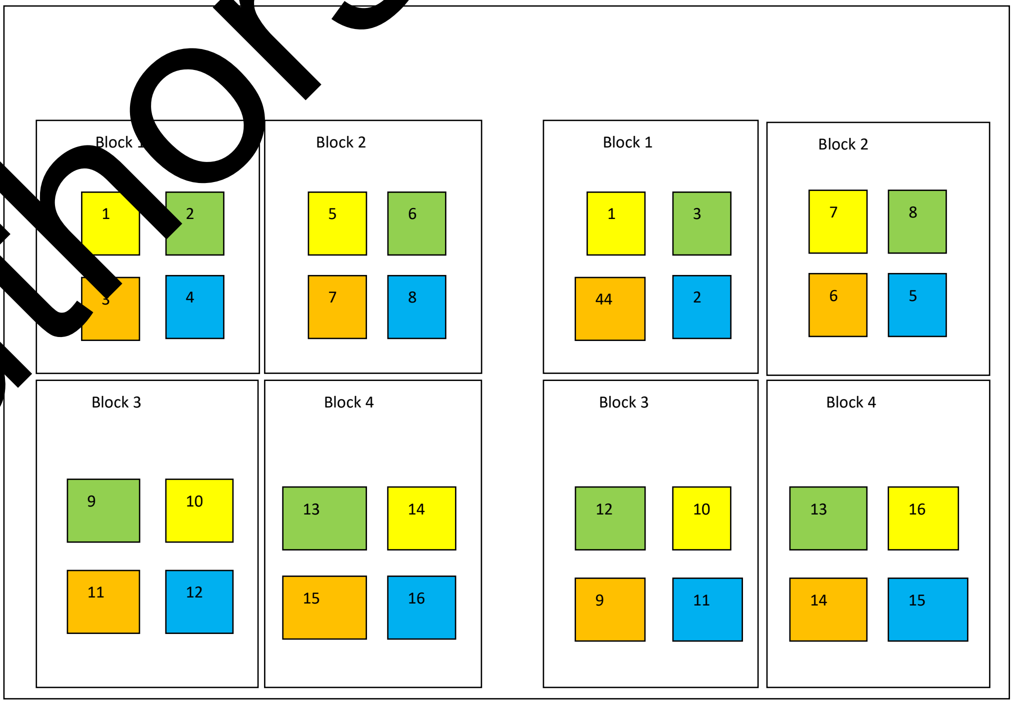


Fig 8. Next round displacement of blocks in inner side

4. 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].

5. Output the Decrypted Image - Reshape the decrypted pixel array back into the original image dimensions. Save or display the decrypted image.

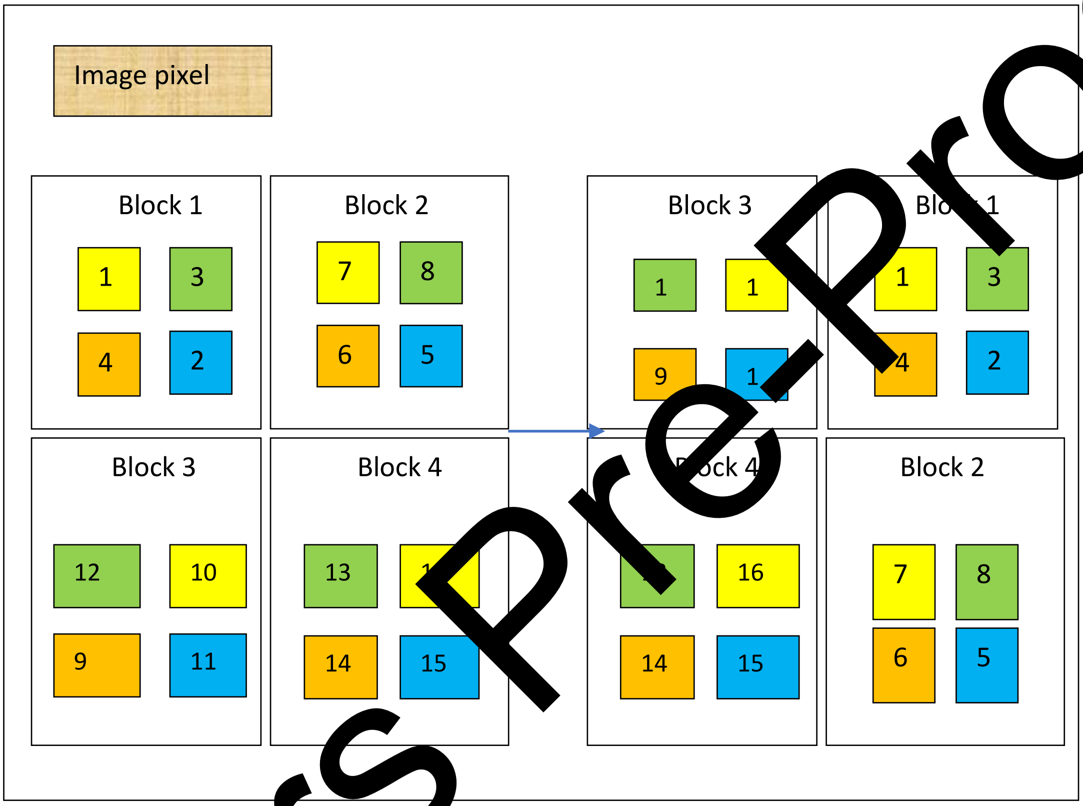


Fig 9. Third phase displacement of blocks shuffle in inside

IV. EXPERIMENTAL ANALYSIS &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.

Original Image: **Encrypted Image:**

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.

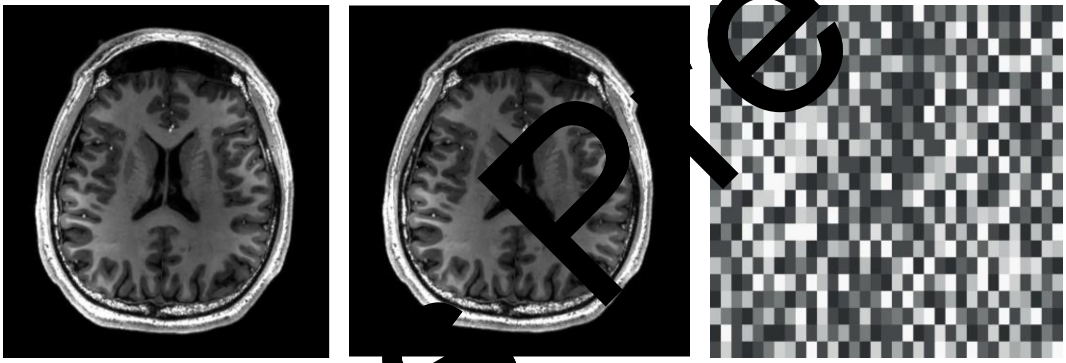


Fig 11. Cerebral imaging initial image, permutation of block values, permutation of blocks

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].

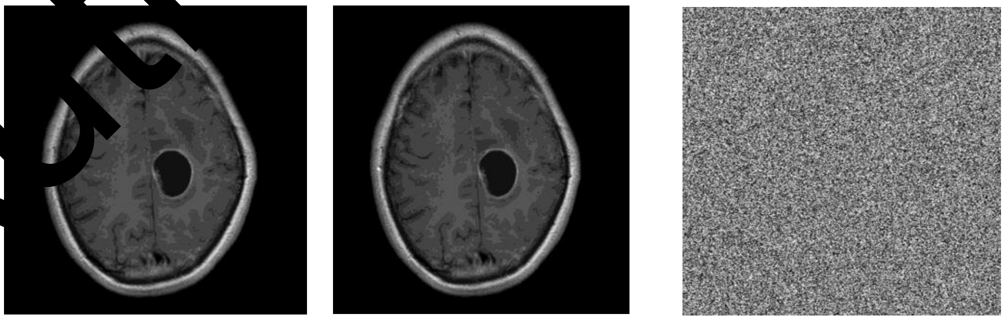


Fig 12. Magnetic resonance picture Initial image, permutation of pixel values within blocks, permutation of blocks themselves

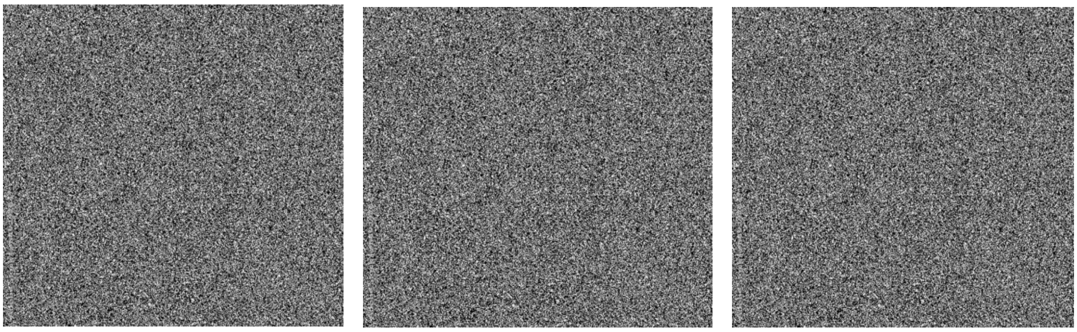


Fig 13 Encryption image of the chest in three direction X Y Z

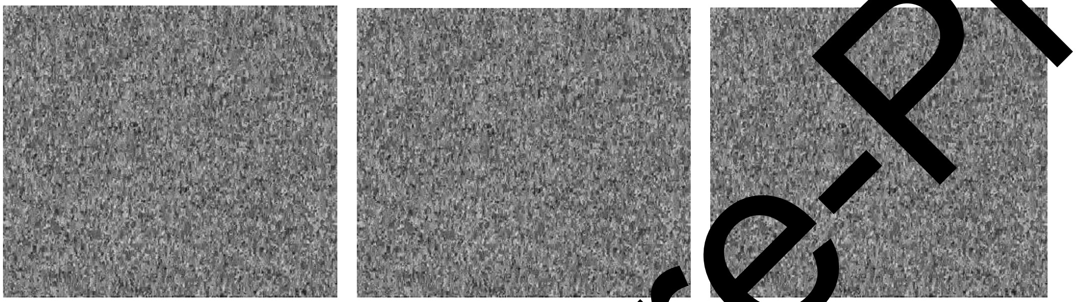


Fig 14. Cerebral imaging Image encrypted along the X-axis image encrypted through the Y-axis picture and Z-axis picture.

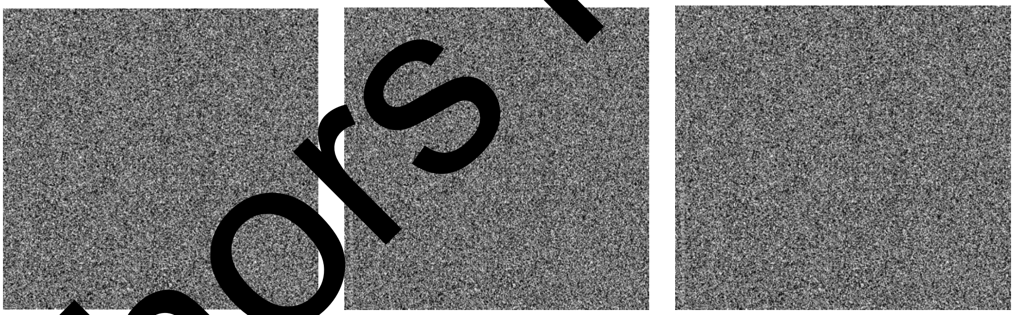


Fig 15. Magnetic resonance picture encrypted through X-axis, Y-axis, Z-axis picture.

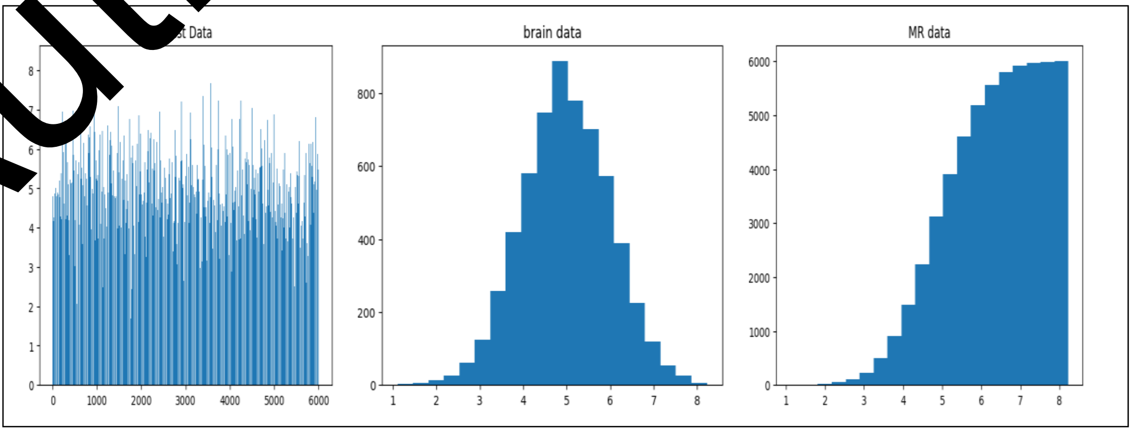


Fig 16. The image of chest, brain and MR image in a histogram view.

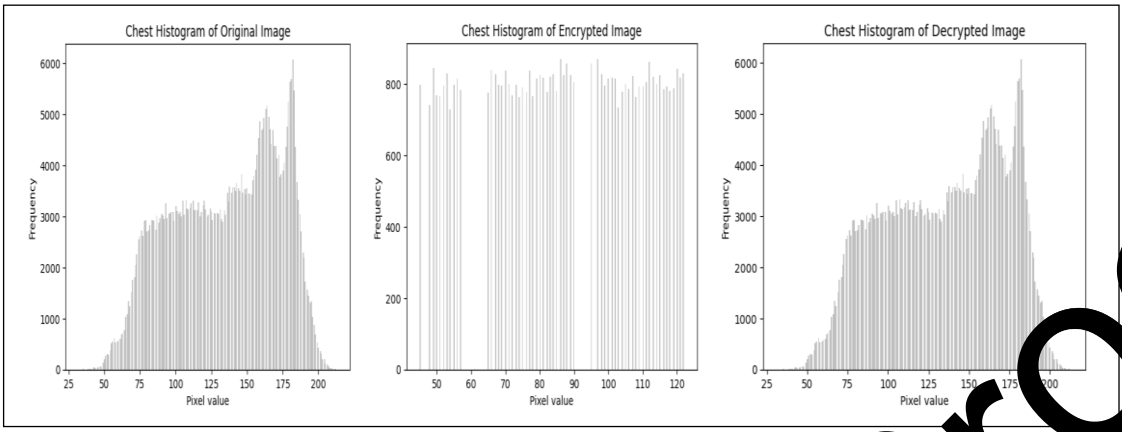


Fig 17. Graphical representation of chest data

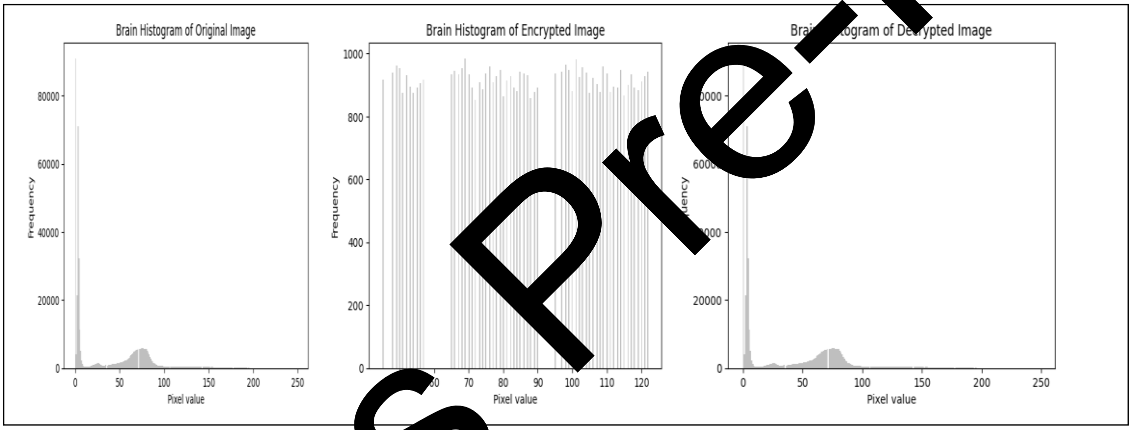


Fig 18. Graphical representation of Brain data

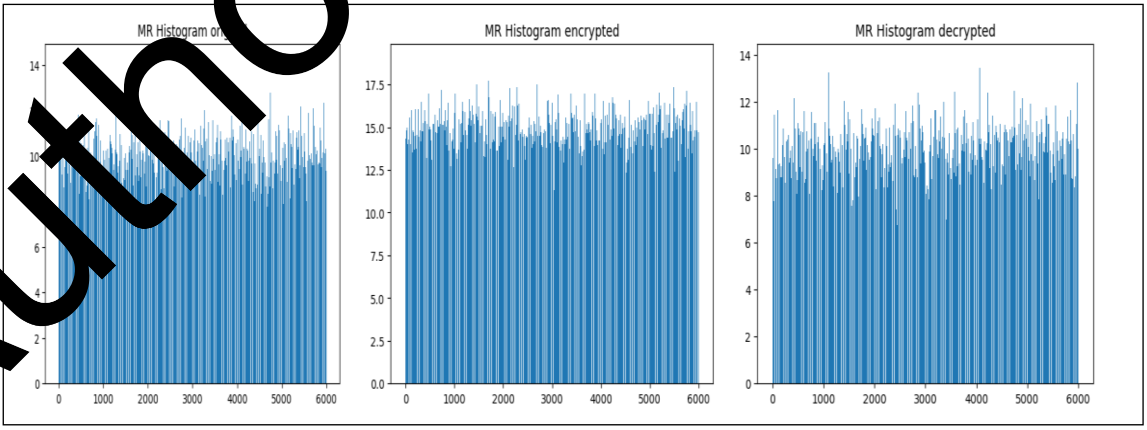


Fig 19. Graphical representation of MR data

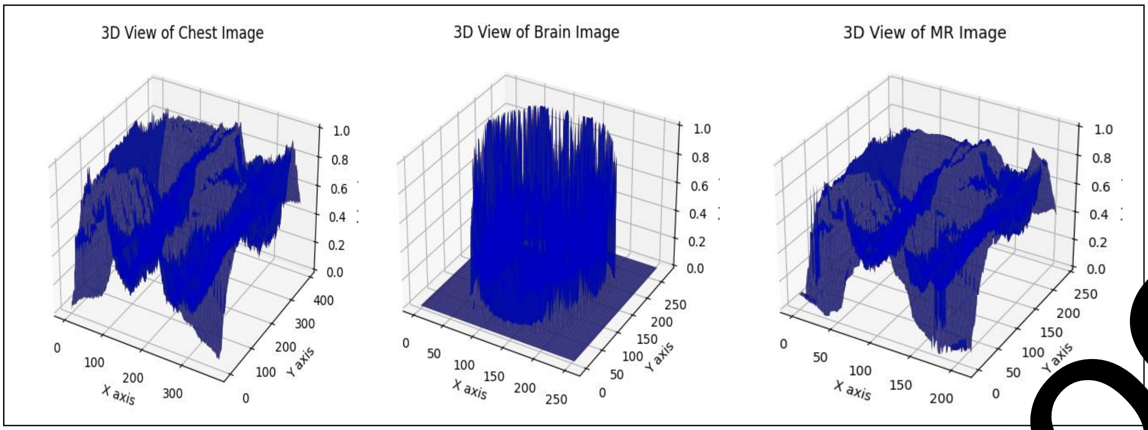


Fig 20. Image of the three histogram view in a 3D method.

b) 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].

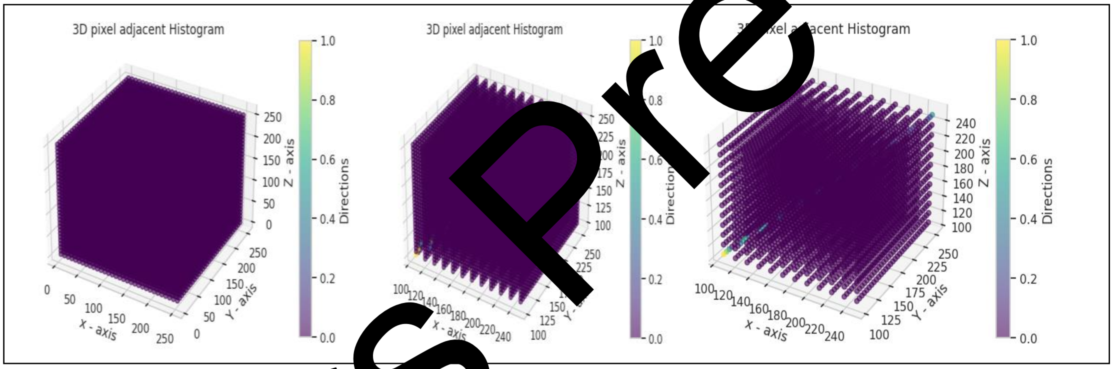


Fig 21. Radiography view of a 3d method along x direction horizontally, diagonally and vertically.

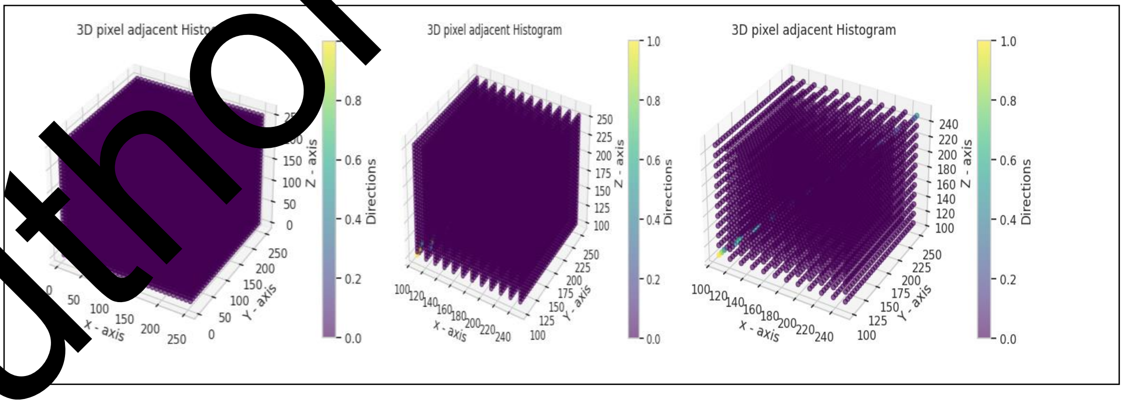


Fig 22. Histograms of 3D display of chest images Chest X-ray graphical representation along Y in three different orientations: horizontally, diagonally, and vertically.

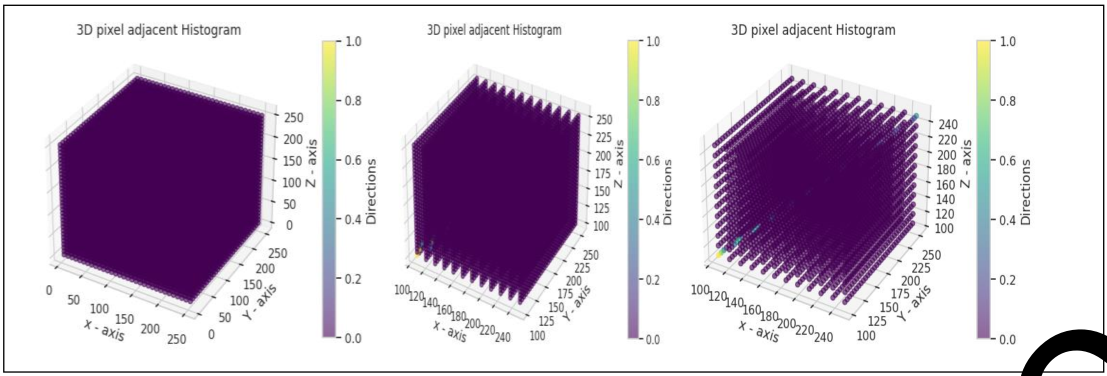


Fig 23. The histogram of chest image in 3D method as horizontally, diagonally and vertically.

Correlation can be computed mathematically as follows:

$$r_{xy} = \frac{E\big((x-E(x))(y-E(y))\big)}{\sqrt{D(x)D(y)}} \qquad (5)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (6)$$

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

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

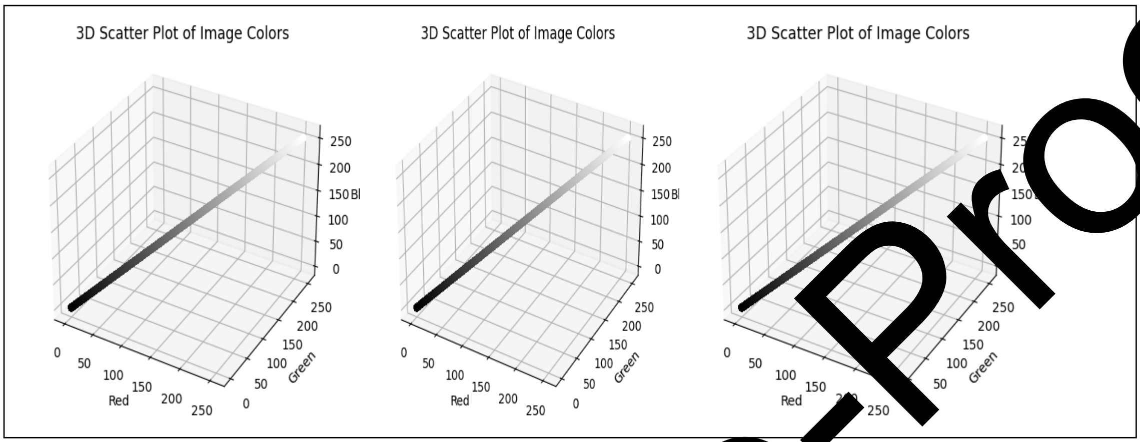


Fig 24. Pixel’s correlation along X, Correlation along Y, Correlation along Z

Table 1 displays the results of our proposed approach for the integers [[illegible], 18, [illegible], 35]. Figure 25 shows the grayscale image in three directions and views the pixels moving [illegible]herent to encrypt mode, as shown in Figures 26–27. The average values of the unaltered images for the chest, brain, and MRI 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.

c) 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.

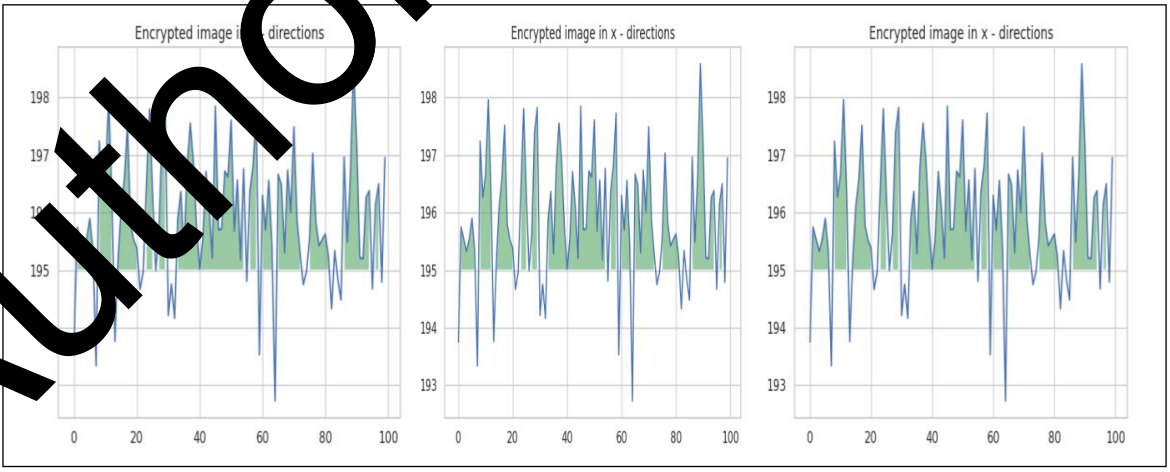


Fig 25. thorax image histogram in x direction

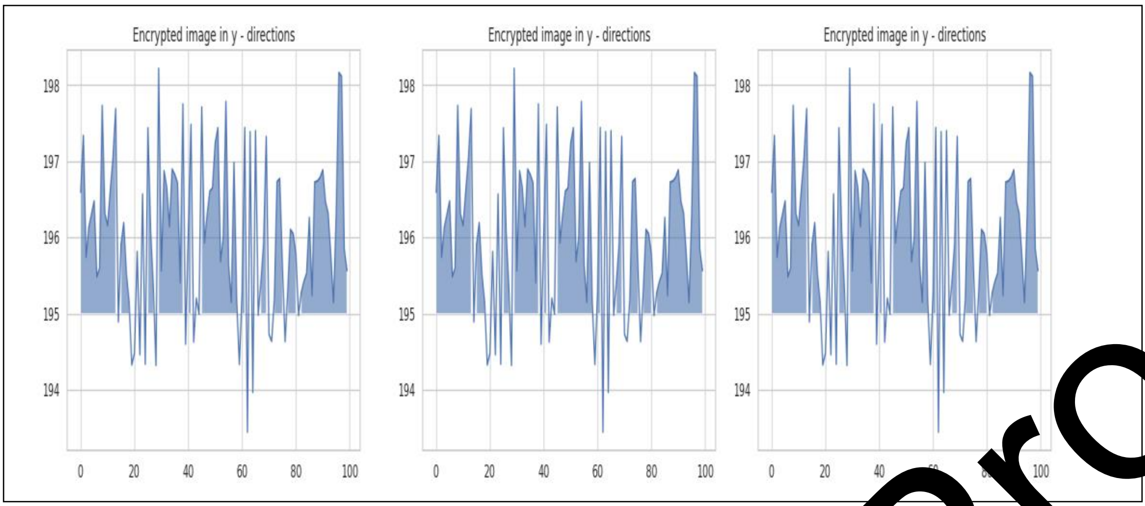


Fig 26. thorax image histogram in y direction

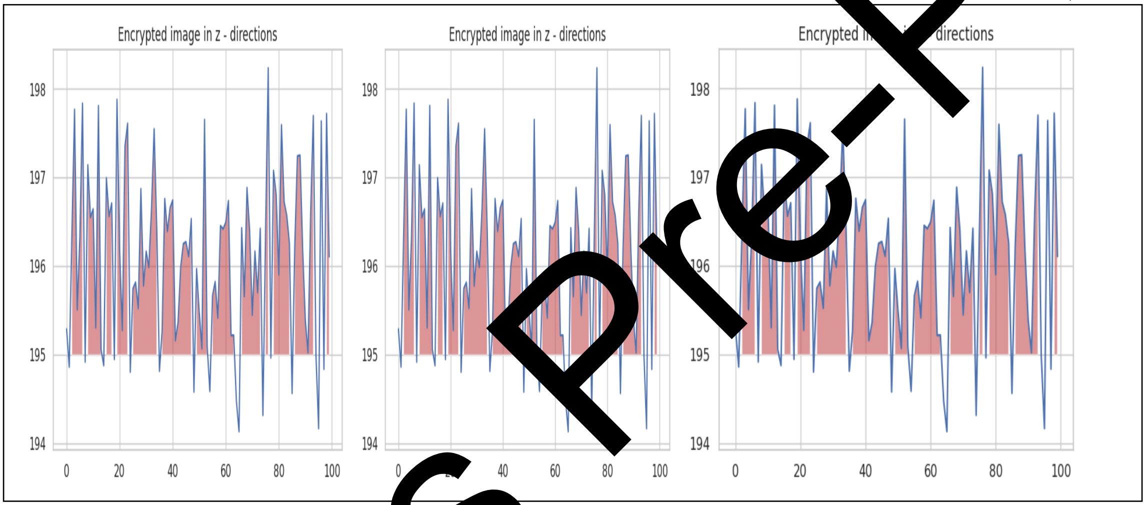


Fig 27. Thorax image histogram in z direction

Formula is:

$$H = \sum_{x,y=1}^{M} \frac{\mathrm{g(x,y)}}{1 + |\mathrm{x} - \mathrm{y}|} \qquad (8)$$

Formula for a contrast:

$$Contrast \ = \sum_{i,j\,=\,1}^{M} |x \ - \ y|^2 \, p(x,y) \qquad (9)$$

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	[illegible]	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
[illegible]	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:

$$\text{Vitality} = p\,(x\,,\,y)^2 \qquad (10)$$

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.

d) **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.

3.5 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.

Given formula for NPCR is

$$\text{NPCR} = \frac{\sum_{ij} D(i,j)}{M\ X\ N}\ X\ 100\% \qquad (11)$$

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:

$$UACI = \frac{1}{M \; X \; N} \left[\sum_{i\,j} \frac{|c1\,(i, j) - c2(i, j)|}{255} \right] \; X \;\; 100\,\% \qquad (12)$$

Table 6. NPCR 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

4. 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.

5 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 stop 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.

References

[1]. **Chen, G., Ueta, T.** (1999). Yet another chaotic attractor. *International Journal of Bifurcation and Chaos*, 9(7), 1465-1466.

[2]. **Lorenz, E. N.** (1963). Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*, 20(2), 130-141.

[3]. **Fridrich, J.** (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos*, 8(6), 1259-1284.

[4]. **Mao, Y., Chen, G.**, & **Lian, S.** (2004). A novel fast image encryption scheme based on 3D chaotic Baker maps. *International Journal of Bifurcation and Chaos*, 14(10), 3613-3624.

[5]. **Pareek, N. K., Patidar, V., & Sud, K. K.** (2006). Image encryption using chaotic logistic map. *Image and Vision Computing*, 24(9), 926-934.

[6]. **Rhouma, R., Solak, E., Belghith, S.** (2007). Cryptanalysis of a new image encryption algorithm based on hyper-chaos. *Physics Letters A*, 372(3), 413-417.

[7]. **Kocarev, L., Tasev, Z.** (2003). Public-key encryption based on Chebyshev maps. *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, 28(6), 28-31.

[8]. **Lian, S., Sun, J., Wang, Z., & Zhang, Y.** (2005). A block cipher based on a suitable use of the chaotic standard map. *Chaos, Solitons & Fractals*, 26(1), 117-129.

[9]. **Wang, X.**, & **Zhang, Q.** (2012). A color image encryption algorithm based on chaotic maps. *Journal of Computers*, 7(5), 123[illegible] 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]. **Kanso, A., & Smaoui, N.** (2009). Logistic chaotic maps for binary numbers generations. *Chaos, Solitons & Fractals*, 40(5), 2557-2568.

[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]. **Baptista, M. S.** (1998). Cryptography with chaos. *Physics Letters A*, 240(1-2), 50-54.

[14]. **Xiang, T., Liao, X., Wong, K.-W., & Tang, Y.** (2007). A novel block cryptosystem based on iterating a chaotic map. *Physics Letters A*, 349(1-4), 109-115.

[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[illegible] 715-[illegible]2.

[16]. **Lian, S.**, **Liu, Z.**, **Rong, Y.**, & **Wang, H.** (2006). Commutative encryption and watermarking in video compression. *IEEE Transactions on Circuits and Systems for Video Technology*, 17(6), 774[illegible]78.

[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]. **Fu, C., Chen, Q., Zou, Y., Zhang, L., & Meng, Y.** (2012). A chaos-based digital image encryption scheme with an improved diffusion strategy. *Optics Communications*, 285(5), [illegible]3-521.

[19]. **Zhou, Y., & Bao, L.** (2010). A new 1D chaotic system for image encryption. *Signal Processing*, 90(9), 2714-2723.

[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[illegible]99.

[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[illegible], 292[illegible]

[23]. **Wang, X., Zhang, Q., & Bao, X.** ([illegible]). A novel chaotic image encryption scheme using DNA sequence operations. *Optics and Lasers in Engineering*, 49(2), 23[illegible]38.

[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, [illegible]** (201[illegible]). Image encryption algorithm based on hyper-chaotic system and dynamic S-boxes. *IET Information Security*, [illegible](2), 111-1[illegible]

[26]. **Pisarchik, A. N., & Zanin, M.** (2008). Chaotic map cryptography and secure communication: Principles and applications. *Nonlinear Dynamics*, [illegible]6, 341-352.

[27]. **Chen, G., Mao, [illegible], & C[illegible], C. K.** (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals*, 21(3), 7[illegible]761.

[28]. **Parvaz, [illegible] & Homayounpour, M. M.** (2011). A fast chaotic encryption scheme based on piecewise linear chaotic maps. *Physics Letters A*, 37[illegible](34), 3924-3932.

[29]. **T[illegible], X., & [illegible]i, Y.** (2012). Image encryption algorithm based on the image decomposition. *Optics Communications*, 285(4), 1065-1[illegible]1.

[30]. **[illegible]hu, H., [illegible]i, Y.** (2013). A novel image encryption scheme based on a chaotic system and an image block cipher. *Signal Processing*, 93(11), 3118-3129.

Author Biography

Dr.Attili Venkata Ramana, received MCA degree from Osmania University, M. Tech (Information Technology) degree from Satyabama University. He has received Ph.D. degree from Sri Venkateswara University, Tirupati. All three degrees are Computer Science and Engineering discipline. He has Completed Ph.D. in the area of Text Mining. He is Currently working as Associate Professor in the Department of CSE (DATA SCIENCE), Geethanjali College of Engineering and Technology, Hyderabad. He is involved in research & teaching MCA, B.Tech, M.Tech. Students and has more than 28 years of Teaching Experience. Reviewed papers in Reputed Journals like Inder Science, IGI Global and PC member for few Conferences. Member of BOS , IQAC and Member of Editorial Board in Glacier Journal of Scientific Research. To his credit, there are nearly 40+ Papers in National and International Journals, Conferences, Seminars and Workshops. Published 6 Patents, 3 Book Chapters. Attended many Workshops, Seminars, STTPS, FDP and Symposia. He is a Lifetime member of CSI and Organized FDPs, Technical Fests, Hackathons, Industrial visits. Guided more than 85 Projects under UG and PG level. He Awarded as Adarsh Vidya Saraswathi Rastriya Puraskar given by Global Management Council for the year 20[illegible] and also received Best Researchers' award continuously (2019 to 2023) 3 years from Sreenidhi Institute of Science and Technology.. His research areas of interest are Mining, Data Science, Machine Learning, Artificial Intelligence, Big Data etc. Orcid ID: 0000-0002-0149-5039.

M.Vignesh is a passionate Student of M.Tech Chemical Engineering, Sri Venkateswara College of Engineering, Sriperumbudur, Tamil Nadu with a burgeoning interest in writing. Currently pursuing advanced studies in Chemical Engineering at Sri Venkateswara College. He is dedicated to exploring innovative solutions to medical image processes and contributing to the field's advancement. Alongside their technical pursuits, He nurtures a deep love for storytelling and literature. They have harnessed their technical expertise to craft narratives that blend scientific concepts with imaginative fiction. Their writing often explores themes of technology, innovation, and the human experience, drawing from their academic background to create rich, informed worlds.

Dr.R.Srinivasan is working as an Associate Professor & Head in the Department of Computer Science, SLS. MAVMM. Ayira Vasiyar College, Kallampatti, Madurai. He has 14 years Teaching Experience and [illegible] years Research Experience. He has Organized 30 National and International Seminars. He has published 6 International Level and 3 National Level Papers. He has to his credit an Intellectual patent right of Government of India Ministry of commerce and Industry. He has held many prestigious Academic positions such as Academic Council Member of Madurai Kamaraj University, IQAC Co-Coordinator, NAAC Coordinator, Institution's Innovation Council (IIC) Coordinator. Presently, he is Member of Lions Club, saravanampatty, Coimbatore. He received An[illegible]athy Award from Lions Public Charitable Trust.

Vishnupriya Borra, Assistant Professor at KLEF Deemed to be University in CSE department with experience of 3 years in Academics. Her specialized diverse expertise in her areas of interest such as Big Data Analytics, Cloud Security, Network Security, Cryptography, Artificial Intelligence, Database Security, and Database Management systems. She has two research publications, one in Scopus indexed journal and another one in the UGC Care journal. She attended one International Conference. She has Microsoft online course certification.

Dr. B. Sen[illegible]kumaran is working as an Assistant Professor at the Department of Computer Science and Engineering, School of Computing, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology (Deemed to be a university), Chennai, India. He has published 15 research articles and filed two patents. He is acting as a research coordinator. He guides four Ph.D. scholars. He got five awards for his academic performances. He has delivered many special lectures in different institutions and attended about 25 international and national conferences, seminars, and workshops. He has conducted 10 international and national conferences, workshops, and seminars. He can be contacted at skumaran.gac16@gmail.com. ORCID: https://orcid.org/0000-0002-7111-1950

Desidi Narsimha Reddy is an accomplished professional with an impressive educational background and extensive experience in the field. He holds a postgraduate degree in Machine Learning & AI from Purdue University, complemented by an MBA in Finance and Information Systems from MG University. Additionally, he has completed a program on Business Analytics: From Data to Insights from Wharton Management School and is a certified Project Management Professional (PMP) from the PMI Institute.

With close to two decades of professional experience, Narsimha Reddy has carved a niche in Business Intelligence. His proficiency encompasses various domains, including Financial Reporting Applications, Data Management, Master Data Management, Data Governance, Data Science, and Artificial Intelligence & Machine Learning. Throughout his career, he has contributed significantly to the field, reflected in the publication of papers in several esteemed journals. Narsimha Reddy's dedication to continuous learning and his diverse skill set makes him a valuable asset in the dynamic landscape of data management and analytics. He is also a member of IEEE.