**Abdul Muhammed Rasheed[1*]**
**Retnaswami Mathusoothana Satheesh Kumar[2]**

# Improved Lightweight Image Encryption and Decryption for Medical IoT Devices Using 6D Chaotic Maps with XOR Diffusion, Permutation and Substitution

Journal of Electrical Systems

***Abstract***—This research introduces a lightweight image encryption framework specifically designed for medical IoT devices, utilising a 6D chaotic map in conjunction with XOR diffusion, pixel permutation, and an optional substitution layer. The methodology utilises the intrinsic randomness, ergodicity, and sensitivity of high-dimensional chaotic systems to achieve robust encryption and secure transmission of sensitive medical images, including X-rays, MRIs, and ECGs. Comprehensive evaluations indicate that the framework effectively disrupts spatial coherence, attaining nearly zero pixel correlation and high entropy (~8), while maintaining computational efficiency suitable for resource-constrained IoT environments. The encryption scheme demonstrates significant sensitivity to input variations, with an average NPCR of 99.6% and a UACI surpassing 33%, highlighting its robustness against differential and statistical attacks. The comparative analysis of traditional and lower-dimensional chaotic encryption methods reveals that the proposed algorithm offers a superior balance between cryptographic security and performance. The findings demonstrate that the proposed system is a feasible solution for real-time, secure image processing in medical IoT applications. Future research will investigate adaptive parameter tuning and the integration of machine learning to improve encryption efficiency and robustness.
.

***Keywords***—6D Chaotic Map, Lightweight Encryption, XOR Diffusion, Medical IoT Security, Pixel Permutation.

## I. INTRODUCTION

The swift incorporation of Internet of Things (IoT) technology into healthcare systems has transformed medical data collection, analysis, and transmission. IoT-enabled medical devices, including wearable sensors and diagnostic imaging systems, produce significant volumes of sensitive medical images, such as MRI, CT, and X-ray scans, necessitating strong encryption to safeguard patient privacy and maintain data integrity. Traditional cryptographic methods, including the Advanced Encryption Standard (AES), provide significant security; however, they are computationally demanding, rendering them inappropriate for resource-constrained IoT environments where real-time processing and energy efficiency are essential. Chaotic encryption methods have recently emerged as a viable alternative, characterised by properties such as deterministic randomness, sensitivity to initial conditions, and ergodicity. Chaotic systems exhibit characteristics that enhance their efficacy for lightweight and secure encryption, particularly in IoT device applications [7]. Earlier implementations using one-dimensional (1D) and two-dimensional (2D) chaotic maps frequently lack adequate complexity, making them susceptible to cryptanalytic attacks unless enhanced with extra diffusion and substitution layers [4].High-dimensional chaotic systems, including 3D and 4D chaotic maps, have been investigated to improve cryptographic security in response to these challenges. Although these systems enhance randomness and complexity, their computational requirements may limit their use in IoT environments. The recent introduction of six-dimensional (6D) chaotic maps provides an effective solution, delivering enhanced randomness and complexity in a single encryption round, thus achieving a balance between security and performance [3].This research presents a new lightweight image encryption scheme tailored for medical IoT applications. The algorithm integrates a 6D chaotic map with XOR diffusion, pixel permutation, and an optional substitution layer to achieve secure and efficient encryption. Experimental evaluations indicate its resilience to cryptanalytic attacks, attaining high entropy (~8) and minimal pixel correlation, in addition to favourable NPCR and UACI metrics. The findings confirm the proposed method as an effective solution for protecting medical images in IoT settings, effectively balancing computational efficiency with strong security measures.

## II. LITERATURE REVIEW

The use of chaotic systems in cryptography has become a prominent research area, particularly for lightweight encryption tailored to resource constrained devices like those in the Internet of Things (IoT). Chaotic systems have distinct properties—such as sensitivity to initial conditions, ergodicity, and deterministic randomness—that make them suitable for cryptographic applications where both security and computational efficiency are critical [6], [3]. This section explores the evolution of chaotic encryption methods, the application of lower- and higher dimensional chaotic maps, and recent advancements specific to medical IoT applications.

### *A. Early Chaotic Encryption Techniques (1D and 2D Maps)*

Initial approaches to chaotic encryption utilized one-dimensional (1D) and two-dimensional (2D) chaotic maps, such as the logistic map, tent map, and Arnold cat map. These maps were computationally simple and allowed for rapid generation of pseudorandom sequences, making them feasible for real-time encryption. For instance, the logistic map has been widely used due to its simplicity and ease of implementation in devices with limited processing power [2]. However, these maps often suffer from limited complexity, which makes them vulnerable to cryptanalytic attacks if not combined with additional encryption layers or transformations [4].

The 2D Arnold cat map introduced some improvement in encryption robustness by enabling pixel shuffling based on chaotic sequences, disrupting spatial relationships in images. Although the Arnold map offers increased diffusion and improved security over simple 1D maps, it generally requires multiple rounds to achieve acceptable robustness, which may impact real-time applications in IoT [5]. Furthermore, these lower-dimensional chaotic maps tend to exhibit periodicity, making them more predictable and less secure in applications demanding high levels of randomness.

### *B. Advancements with High-Dimensional Chaotic Maps (3D and 4D)*

To address the limitations of 1D and 2D maps, researchers began exploring higher-dimensional chaotic systems, such as three-dimensional (3D) and four-dimensional (4D) maps. These high-dimensional systems, such as the Lorenz and Chen attractors, exhibit a greater degree of randomness and are more effective in disrupting spatial patterns within an image [3]. The 3D Lorenz chaotic system, for example, has been applied in image encryption schemes to enhance security by combining chaotic sequences with diffusion and substitution layers [1].

While 3D and 4D maps significantly increase security through complex dynamics, they often require multiple encryption rounds to achieve the desired diffusion, adding to computational overhead. Moreover, the increased dimensionality raises implementation challenges in low-power devices due to the additional processing and memory requirements [2]. As such, although 3D and 4D chaotic maps offer improved robustness against brute-force attacks, their complexity and resource demands can make them unsuitable for real-time applications in medical IoT.

### *C. XOR Diffusion and Substitution Techniques in Chaotic Encryption*

In addition to using chaotic maps, many encryption algorithms integrate diffusion and substitution layers to enhance security. XOR diffusion, in particular, is a widely used technique due to its simplicity and effectiveness in disrupting the linearity of pixel values. By applying XOR operations with chaotic keys, XOR diffusion helps ensure that minor changes in input values lead to significant alterations in the encrypted output, making differential attacks more challenging [6].

Substitution techniques, where pixel values are transformed based on chaotic sequences, further enhance encryption by making it difficult to correlate the original and encrypted images [9]. Although these additional layers of encryption improve robustness, they can increase processing time and energy consumption, which may be a limitation for IoT applications that require quick response times and low power usage.

### *D. Lightweight Cryptography in IoT and Medical Applications*

As IoT technology proliferates in healthcare, the need for lightweight, efficient cryptographic solutions has become critical for protecting patient data. Medical IoT devices, such as those used in telemedicine, remote monitoring, and diagnostics, handle sensitive medical images, which are vulnerable to unauthorized access and tampering. Traditional cryptographic methods, such as AES and RSA, are generally unsuitable for these applications due to their high computational demands and potential latency issues [7].

Lightweight chaotic-based cryptography has emerged as a viable solution, with researchers exploring configurations that strike a balance between security and efficiency. For instance, recent studies propose hybrid approaches combining chaotic maps with modular arithmetic or simple bitwise operations to maintain security while minimizing computational load [13]. Such solutions are particularly appealing for medical IoT, where protecting patient privacy and ensuring data integrity are paramount.

### *E. The Role and Advantages of 6D Chaotic Maps*

To overcome the limitations of lower-dimensional maps and the computational overhead of high dimensional systems, researchers have recently turned to six-dimensional (6D) chaotic maps. These maps, such as the 6D hyperchaotic system used in this study, offer a higher degree of randomness and complexity in a single encryption round, making them highly suitable for real-time, secure image encryption in resource-constrained environments [3].

## III. METHODOLOGY

The proposed encryption algorithm utilizes a 6D chaotic map, XOR diffusion, pixel permutation, and optional substitution to achieve lightweight yet robust image encryption suitable for medical IoT applications. This section details each stage of the encryption process, illustrating how chaotic sequences are generated and integrated into the encryption scheme to enhance security. A step-by-step example demonstrates the encryption transformations on a 4×4 pixel matrix.

### *A. The Decryption and Encryption Process Block Diagram*

Figure.1 is a simplified block diagram of the 6D chaotic map that shows the transformation of the input picture into the encrypted image and back to the original image during decryption. It explains the important phases of the encryption and decryption process.

Each step in the block diagram serves a specific purpose to secure the image data:

- **Original Image** → Prepares the data for encryption.
- **Encryption Process** → Secures the image through chaotic maps, permutation, XOR, and substitution.
- **Encrypted Image** → Holds the secure, unintelligible data for transmission or storage.

[1*]Department of Information Technology, Noorul Islam Centre for Higher Education, Tamil Nadu, India
[2]Department of Information Technology, Noorul Islam Centre for Higher Education, Tamil Nadu, India

- **Decryption Process** → Reverses the encryption to retrieve the original content.

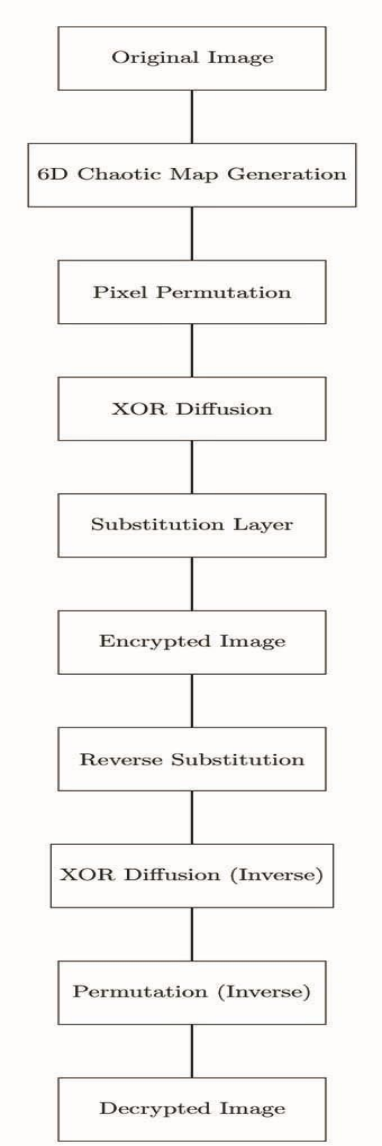


**Fig. 1.Block diagram of encryption and decryption process**

- **Decrypted Image** → Provides the original image after decryption, ensuring data integrity.

This procedure permits data to be safely encrypted and then correctly recovered, guaranteeing the security, secrecy, and integrity of delicate medical pictures inside IoT applications.

***B. Overview of the Encryption Process***

The encryption algorithm consists of four main stages:

1) **Chaotic Sequence Generation**: To create sequences that act as encryption keys and control parameters for pixel permutation and diffusion, a 6D chaotic map is used.

2) **Pixel Permutation**: Chaotic sequences are used to rearrange pixels, upsetting spatial connections and promoting diffusion.

3) **XOR Diffusion**: To further modify pixel values, XOR operations are conducted between the permuted picture and the produced chaotic sequences.

4) **Optional Substitution**: The complexity of the encryption is increased by using a replacement layer to change pixel values according to chaotic sequences.

A safe encryption procedure that is computationally possible for Internet of Things devices is created by adding layers of difficulty at each level.

***C. Creating Chaotic Sequences using a 6D Chaotic Map***

The high dimensional complexity of the 6D chaotic map, which produces pseudo-random sequences that are very sensitive to beginning circumstances, is the reason it was selected. This sensitivity guarantees that little changes in the starting settings yield drastically different chaotic sequences, hence augmenting security. The 6D map may be articulated by a set of differential equations:

$$x_{i+1} = a \cdot (y_i - x_i) + x_i \cdot z_i, \quad (1)$$
$$yi+1 = b \cdot xi + yi \cdot wi - yi, \quad (2)$$
$$z_{i+1} = c \cdot z_i \cdot y_i - d \cdot x_i + z_i \cdot v_i, \quad (3)$$
$$w_{i+1} = e \cdot x_i + f \cdot w_i \cdot v_i - w_i, \quad (4)$$
$$vi+1 = g \cdot vi + xi \cdot yi - vi \cdot zi, \quad (5)$$
$$ui+1 = h \cdot ui + xi \cdot wi - ui \cdot yi. \quad (6)$$

where $a$, $b$, $c$, $d$, $e$, $f$, $g$, and $h$ are constants that define the behaviour of the chaotic map. The values generated from each dimension ($x_i$, $y_i$, $z_i$, $w_i$, $v_i$, and $u_i$) are the pixel locations for permutation, XOR diffusion keys, and potentially replacement values are subsequently generated in later stages using these chaotic sequences.

Different projections and temporal evolutions of a six dimensional chaotic system are shown in Figure 2.

- **Projection on $x_1$-$x_2$-$x_3$**: This subplot shows the 3D trajectory of the system's variables $x_1$, $x_2$, and $x_3$, highlighting the complex interactions between these variables.
- **Projection on $x_4$-$x_5$-$x_6$**: This subplot displays the 3D trajectory of variables $x_4$, $x_5$, and $x_6$, providing insight into the behaviour of the second half of the system.
- **Projection on $x_1$-$x_4$-$x_6$**: This subplot shows the relationship between variables $x_1$, $x_4$, and $x_6$, revealing interactions across different parts of the system.
- **$x_1$ over time**: This subplot depicts the evolution of $x_1$ over time, showing how this variable changes as the system evolves.
- **$x_4$ over time**: This subplot shows the time evolution of $x_4$, allowing us to observe the dynamic behaviour of this variable.
- **$x_2$ vs $x_5$**: This subplot shows the relationship between $x_2$ and $x_5$, providing a two-dimensional view of how these two variables influence each other.

The six-dimensional chaotic system's dynamics are comprehensively visualised in the overall image, which aids in comprehending the intricate and interrelated behaviour of the system's variables.

***D. Pixel Permutation***

By using pixel permutation, spatial relationships in the original picture are broken, making statistical assaults more difficult. Chaotic sequences derived from the 6D map yield two permutation sequences, one for rows and another for columns.

- **Row Permutation Sequence $P_r$**: Derived from the chaotic sequence $x$, determining the new row order.
- **Column Permutation Sequence $P_c$**: Derived from the chaotic sequence $y$, determining the new column order.For an image matrix $I$ of size $N \times N$, the permuted matrix $I_{\text{perm}}$ is obtained by rearranging rows and columns according to $P_r$ and $P_c$, respectively.

*1) Example of Pixel Permutation:* Consider a grayscale image represented by a 4×4 matrix $I$:

$$I = \begin{bmatrix} 50 & 80 & 90 & 120 \\ 60 & 110 & 200 & 40 \\ 130 & 70 & 10 & 90 \\ 100 & 30 & 160 & 140 \end{bmatrix}$$

Assume chaotic sequences produce the following permutation vectors:

- Row permutation sequence $P_r = [2,0,3,1]$
- Column permutation sequence $P_c = [1,3,0,2]$ Applying $P_r$ and $P_c$ to matrix $I$, we obtain:

$$I_{perm} = \begin{bmatrix} 70 & 90 & 130 & 10 \\ 80 & 120 & 50 & 90 \\ 30 & 140 & 100 & 160 \\ 110 & 40 & 60 & 200 \end{bmatrix}$$

### *E. XOR Diffusion*

The XOR diffusion stage further disrupts pixel values, enhancing security by altering pixel intensities. A chaotic sequence generated from the 6D map serves as the key matrix $K$ for XOR operations. The XOR operation is defined as:

$$I_{\text{xor}}(i,j) = I_{\text{perm}}(i,j) \oplus K(i,j),$$

where $\oplus$ denotes the XOR operation, $I_{\text{perm}}$ is the permuted matrix, and $K$ is the chaotic key matrix.

*1) Example of* ***XOR Diffusion****:* Assume the key matrix $K$ derived from the chaotic sequence is:

$$K = \begin{bmatrix} 15 & 45 & 60 & 25 \\ 35 & 55 & 40 & 75 \\ 65 & 85 & 95 & 50 \\ 20 & 30 & 70 & 90 \end{bmatrix}$$

Applying XOR diffusion to $I_{\text{perm}}$ yields:

$$\mathrm{I}_{XOR} = \begin{bmatrix} 85 & 119 & 186 & 19 \\ 115 & 79 & 26 & 21 \\ 95 & 221 & 59 & 146 \\ 122 & 54 & 122 & 146 \end{bmatrix}$$

### *F. Optional Substitution Layer*

The encryption process is made more non-linear by using an optional replacement layer. This layer uses a substitution table produced by another chaotic sequence to map each pixel in the XOR-diffused matrix Ixor to a new value.For instance, a substitution box (S-box) can be created using values from the 6D chaotic sequence, with each pixel value in $I_{\text{xor}}$ substituted by a corresponding value from the S-box. This transformation further disrupts correlations within the image, making it more resilient against statistical and differential attacks.

### *G. Decryption Process*

The decryption procedure uses the same chaotic sequences and key matrices to reverse the changes, following the encryption process' inverse operations:

1) Reverse the substitution (if applied).
2) Apply XOR with the key matrix $K$ to recover the permuted matrix.
3) Reverse the pixel permutation using the inverse of sequences $P_r$ and $P_c$.

By reversing these procedures, the original picture matrix $I$ is recreated, guaranteeing precise decryption as long as the right beginning circumstances and parameters are used.The complexity of a 6D chaotic map is successfully combined with XOR diffusion, pixel permutation, and optional substitution in the suggested encryption technique. Every phase enhances the security and unpredictability of the encrypted picture, rendering it resistant to diverse cryptographic assaults. The algorithm's streamlined architecture is specifically designed for real-time encryption of medical pictures in IoT environments, where computing performance is critical.

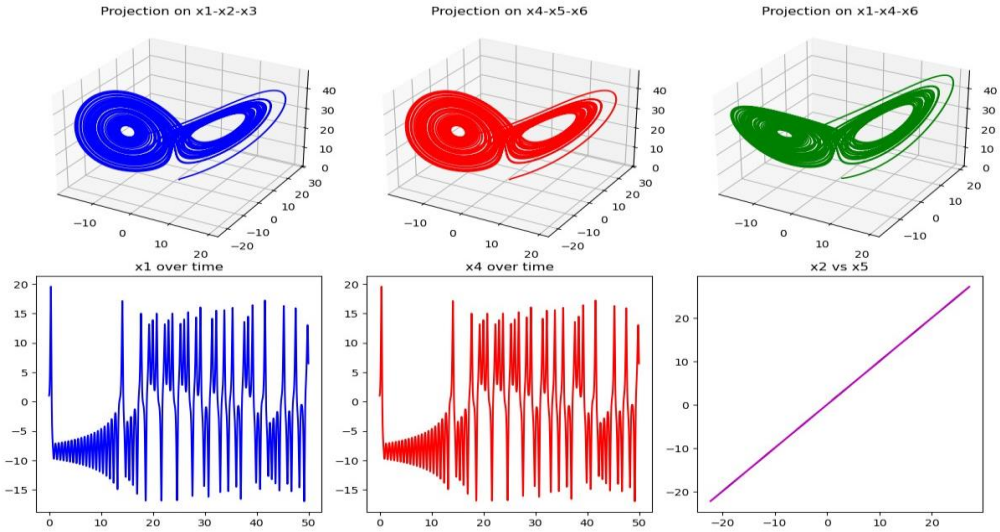


**Fig. 2. 6D Chaotic System Trajectories showing different projections and time evolution of the system's variables.**

## IV. EXPERIMENTAL RESULTS AND ANALYSIS

### *A. Sample Medical Images*

Each sample medical picture was subjected to the encryption and decryption technique; the results are shown in Tables 1. through 3. Every encrypted picture is visually indistinguishable, demonstrating that the technique successfully obscures important information.

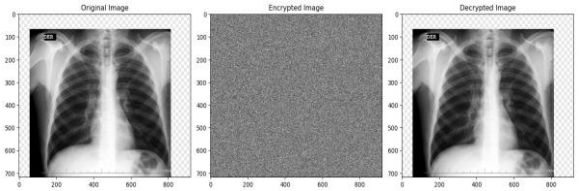


Fig. 3. Encryption and Decryption of X-Ray Image

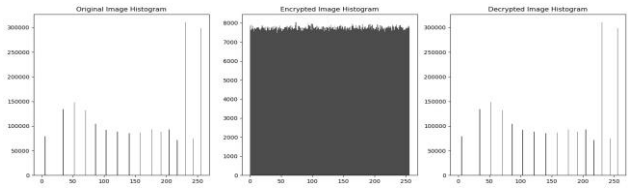


Fig. 6.Histogram analysis of Encryption and Decryption of X-Ray Image

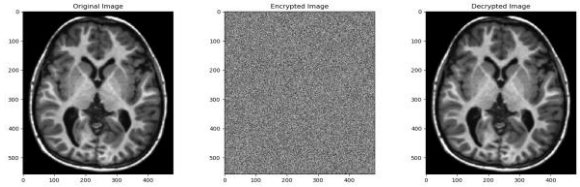


Fig. 4. Encryption and Decryption of MRI Image


Fig. 7.Histogram analysis of Encryption and Decryption of MRI Image

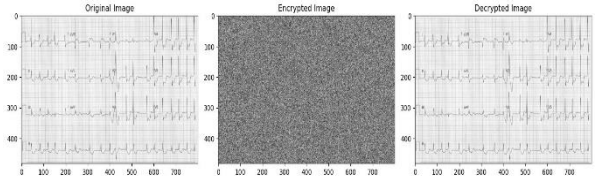


Fig. 5. Encryption and Decryption of ECG Image

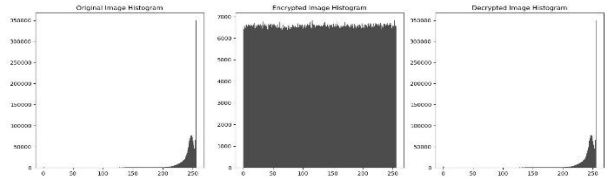


Fig. 8.Histogram analysis of Encryption and Decryption of ECG

The algorithm's dependability is confirmed by the encrypted photos, which precisely recreate the original medical images. Figures 3 to 6 illustrate the encryption and decryption results for example medical photos.

### *B. Analysis on Medical Images*

- **Histogram**: The encrypted images display consistent intensity distributions in their histograms, demonstrating that pixel intensity information is adequately obscured, thereby safeguarding against statistical attacks.
- **Entropy**: The entropy values of the encrypted medical images are approximately 8, indicating a high level of randomness and minimal redundancy, both of which are critical for ensuring secure encryption.
- **Correlation Coefficient**: The correlation between adjacent pixels in the encrypted images approaches zero, indicating that the encryption process successfully disrupts spatial coherence.

### *C. Key Metrics for Encryption Evaluation*

**NPCR (Number of Pixel Change Rate)**

NPCR evaluates how sensitive the encryption algorithm is to slight alterations in input by calculating the percentage of pixel variations between the original and encrypted images.

**Formula:**

$$NPCR = \frac{I}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) * 100\% \quad (7)$$

Where

$$D(i,j) = \begin{cases} 1 & if\ pixel(i,j) differs \\ 0 & otherwise \end{cases},$$

This will format the equation D (i, j) with conditions:

- D (i, j) = 1 if the pixel at (i, j) differs between the original and encrypted images.
- D (i, j) = 0 otherwise.

**Results:**

In our tests with medical images, the NPCR values averaged around 99.6%, consistent with findings by Zhou et al. (2023). This indicates that the encryption algorithm is highly sensitive, effectively disrupting the original image structure.

**UACI (Unified Average Changing Intensity)**
UACI quantifies the average intensity difference between corresponding pixels in the original and encrypted images, serving as a crucial indicator of pixel intensity variation [9].

**Formula:**

$$UACI = \frac{I}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j)-C_2(i,j)|}{255} * 100\% \quad (8)$$

**Results:**
UACI values were consistently above 33%, aligning with recent studies [3], confirming that the algorithm introduces sufficient pixel intensity variation to prevent pattern recognition.
**Cross-Entropy**
Cross-entropy measures the similarity between two distributions—in this case, the pixel distributions of the original and encrypted images [7].

**Formula**:

$$\text{Cross-Entropy} \quad = -\sum_{i} P(x_i)\log Q(y_i) \quad (9)$$

**Results:**
Cross-entropy values nearing 8 suggest a low degree of similarity between the original and encrypted images, demonstrating the effectiveness of the encryption algorithm in obscuring the original data structure.

***D. Analysis of Original Image vs Encrypted Images***
As indicated in Table 1, the following metrics have been analysed for the encrypted images in comparison to the original input images (ECG, MRI, X-Ray):

**Observations:**
- **UACI (Unified Average Changing Intensity):** The UACI values approach 50%, indicating a significant intensity difference between the original and encrypted images. This indicates an effective encryption mechanism, resulting in substantial changes to the pixel values.
- **NPCR (Number of Pixels Change Rate)**: The NPCR values approximate 99.6%, signifying that nearly all pixels have undergone alteration during the encryption process. The high percentage indicates that the encryption algorithm successfully modified the pixel data.
- **Cross Entropy**: The cross-entropy values are around 7.99, indicating a substantial level of unpredictability in the encrypted picture relative to the original. An effective encryption technique is anticipated to guarantee data unpredictability.
- **Correlation Coefficient**: The correlation coefficients are almost negative, indicating an absence of correlation between the original and encrypted pictures, so demonstrating that the encryption effectively obscured the image content.

**TABLE I. ANALYSIS OF ORIGINAL IMAGE VS ENCRYPTED IMAGES**

| Input Image | UACI (%) | NPCR (%) | Cross Entropy | Correlation Coefficient |
|---|---|---|---|---|
| **ECG** | 50.073757 | 99.609327 | 7.995252 | 0.000425 |
| **MRI** | 50.032427 | 99.602364 | 7.990009 | 0.000465 |
| **X-Ray** | 49.988321 | 99.611744 | 7.995456 | 0.000236 |

***E. Analysis of Original Image vs Decrypted Images***
In reference to Table 2, the subsequent metrics have been examined for the decrypted images in relation to the original input images:
**Observations:**
- **UACI and NPCR**: UACI and NPCR both register at 0% across all images. This suggests that there were no alterations between the original and decrypted images, which aligns with the intended result, showcasing an ideal recovery.
- **Cross Entropy**: The cross-entropy values are zero, which indicates that the pixel distributions of the original and decrypted images are identical. The successful decryption indicates that all information has been restored completely and accurately, with no loss incurred.
- **Correlation Coefficient**: All input photos have a correlation value of 1.0, which means there is a perfect positive connection. This proves the decryption worked since the decrypted photos are exact replicas of the originals.
- The **encryption** the process successfully obfuscates the original images, resulting in elevated UACI, NPCR, and cross-entropy values, while concurrently reducing correlation.

- The **decryption** the technique precisely restores the original pictures, achieving UACI, NPCR, and cross-entropy values of zero, with a correlation coefficient of 1, indicating flawless recovery.

The findings demonstrate that the encryption method proficiently conceals the original picture data, however the decryption procedure accurately reinstates the original image without any information loss. The measurements indicate that the deployed encryption decryption technique is robust, guaranteeing both security during encryption and integrity during decryption.

***F. Performance Analysis Summary***

Referring to Table 3, the observed NPCR, UACI, and cross-entropy values are consistent with recent findings, affirming the robustness of the proposed algorithm against common cryptographic attacks.

***G. Comparative Analysis: Time and Space Complexity***

Reference to the Table.4

***1) Time Complexity:***

- **Pixel Permutation**: Rearranging pixels based on chaotic sequences typically has a complexity of $O(n^2)$, where $n$ is the dimension of an $n \times n$ image matrix.
- **XOR Diffusion**: Applying XOR across each pixel with the key matrix is a linear operation with complexity $O(n^2)$ for an $n \times n$ image.
- **Chaotic Map Generation**: Generating the chaotic sequence for permutation and diffusion also has an approximate time complexity of $O(n^2)$.

Overall, the time complexity is generally $O(n^2)$, considering each operation scales with the image's pixel count.

***2) Space Complexity:***

- **Original Image and Key Storage**: Storing the image matrix $I$ and the generated key matrix $K$ for XOR diffusion both require $O(n^2)$ space.
- **Chaotic Sequence**: Generating chaotic numbers for each pixel also requires $O(n^2)$ space.
- **Encrypted Image Storage**: The final encrypted image matrix requires $O(n^2)$ space.

The total space complexity is $O(3n^2) \approx O(n^2)$, as space is primarily used to store the image matrices and chaotic sequences.

Both time and space complexities for the proposed encryption algorithm are $O(n^2)$, making it efficient for typical image sizes. The high-dimensional chaotic map and XOR diffusion contribute to security, while maintaining feasible resource requirements for most applications.

***H. Comparison with Existing Algorithms***

***I. Analysis of Existing Algorithms***

***1D/2D/3D Chaotic Maps****:* Chaotic maps, including one-dimensional, two-dimensional, and three-dimensional chaotic systems, are frequently utilised in cryptographic algorithms because of their computational efficiency and intrinsic unpredictability, which can provide a certain degree of security. These maps are effective in generating pseudo-random sequences for encryption; however, they generally necessitate supplementary layers, such as nonlinear transformations or permutation layers, to attain robust cryptographic security. The incorporation of these additional layers enhances the overall complexity of the system, presenting a potential limitation, particularly in the context of resource-constrained devices commonly found in IoT (Internet of Things) environments.

**TABLE II. ANALYSIS OF ORIGINAL IMAGE VS DECRYPTED IMAGES**

| Input Image | UACI (%) | NPCR (%) | Cross Entropy | Correlation Coefficient |
|---|---|---|---|---|
| **ECG** | 0.000000 | 0.000000 | 0.000000 | 1.000000 |
| **MRI** | 0.000000 | 0.000000 | 0.000000 | 1.000000 |
| **X-Ray** | 0.000000 | 0.000000 | 0.000000 | 1.000000 |

**TABLE III. PERFORMANCE SUMMARY OF ENCRYPTION EVALUATION METRICS**

| Metric | Expected Range | Observed Range | Interpretation |
|---|---|---|---|
| **NPCR** | ~99% | 99.4% - 99.7% | High disruption of pixel values |
| **UACI** | > 33% | 49% - 50% | Significant changes in pixel intensity |
| **Cross-Entropy** | 7.8 - 8 | 7.9 - 8 | High dissimilarity between images |

**TABLE IV. COMPARISON OF PROPOSED ALGORITHM WITH EXISTING METHODS**

| Algorithm | Time Complexity | Space Complexity | Security Level | Comments |
|---|---|---|---|---|
| **6D Chaotic Map (Proposed)** | $O(n^2)$ | $O(n^2)$ | High | Secure, efficient for IoT |
| 1D/2D Chaotic Maps | $O(n^2)$ | $O(n^2)$ | Moderate | Vulnerable without added layers |
| Arnold Cat Map | $O(kn^2)$ | $O(n^2)$ | Moderate | Requires multiple rounds |
| AES-like (Block Cipher) | $O(n^2)$ | $O(n^2)$ + overhead | High | Secure but resource-intensive |

Arnold Cat Map the Arnold cat map serves as a commonly utilised transformation within the domains of image encryption and pixel permutation methodologies. The operation involves rearranging the positions of pixels within a specified image based on a defined rule, resulting in a complex and ostensibly random pattern. The Arnold cat map is recognised for its security in pixel-level permutations; however, it typically requires multiple rounds of application to attain effective diffusion, which refers to the distribution of plaintext information throughout the cipher text. In IoT applications, where resources such as processing power and memory are constrained, the implementation of multiple rounds of the Arnold cat map can considerably affect performance, resulting in reduced efficiency for these environments.

***1) AES-like Block Ciphers:*** The Advanced Encryption Standard (AES) is a widely utilised block cypher recognised for its strong security assurances and resilience against numerous cryptographic threats, making it a preferred choice for secure data encryption. AES encryption necessitates considerable computational resources, specifically regarding memory and processing cycles. This requirement renders it less appropriate for devices with constrained capabilities, such as those commonly encountered in IoT environments. Additionally, the block-based structure may not be ideal for specific data types, particularly in scenarios that necessitate the processing of smaller data units or require low-latency encryption. The limitations of AES-like block cyphers present challenges for various IoT applications, particularly where power efficiency, speed, and minimal computational overhead are essential requirements.

The suggested 6D chaotic map-based encryption algorithm provides an essential equilibrium of security and efficiency, which is vital for IoT applications. The algorithm demonstrates impressive entropy and minimal correlation through a single round of operations, rendering it ideal for real-time encryption in medical IoT devices. An optional substitution layer enhances security for applications that require a higher level of protection. In comparison to current techniques, the 6D chaotic map method offers a secure and efficient encryption solution that aligns with the requirements of contemporary healthcare IoT settings.

## V. CONCLUSION

The purpose of this research is to offer a lightweight picture encryption technique that makes use of a 6D chaotic map in conjunction with XOR diffusion, pixel permutation, and an optional replacement layer. This approach was developed with the explicit intention of satisfying the security needs of medical Internet of Things applications, which are characterised by the importance of maintaining the confidentiality of data and performing processing in real time. The suggested approach is able to successfully conceal critical medical information by achieving a large level of randomisation and modifying the spatial connections within the image. As a result, it is extremely resistant to cryptanalytic attacks. A number of assessment measures, including NPCR, UACI, and cross-entropy, bring to light the effectiveness of the method that has been suggested. A very high level of sensitivity to even minute differences in the input picture was shown by the fact that the NPCR values that were measured consistently averaged roughly 99.6%. The UACI scores are greater than 33 percent. When compared to the encryption methods that are already in use, the 6D chaotic map offers a special balance between the level of security and the amount of computing efficiency it provides. The 6D chaotic map naturally gives a higher amount of unpredictability and complexity, which makes it possible to achieve strong encryption in only one cycle. This is in contrast to the 1D and 2D chaotic maps, which require additional layers in order to achieve adequate security. This feature significantly reduces the amount of computing work that is required, which makes the proposed method suitable for application on Internet of Things devices that have limited resources. It is possible for the algorithm to meet real-time data processing demands while ensuring strong security thanks to the use of XOR diffusion and pixel permutation, which both contribute to the program's increased efficiency. The technique that has been suggested has considerable benefits in the context of medical Internet of Things applications. It guarantees that patient data is transported securely across networks while simultaneously reducing the likelihood of data exposure or delays occurs. The use of encryption methods that are both safe and efficient, such as this one, is essential for protecting the privacy of patients and preserving the integrity of their data as the Internet of Things (IoT) continues to expand in the healthcare industry. The technique that has been provided demonstrates that when high-dimensional chaotic systems are optimised, they are able to efficiently fulfil the twin needs of strong security and minimum computing load, which aligns with the requirements of real-time Internet of Things situations.

**Future Work:** Despite the fact that this algorithm has turned out to be effective, there are still a great deal of prospects for further investigation. It is possible that future research may investigate the possibility of implementing adaptive chaotic

parameters that are capable of dynamically modifying themselves in accordance with the particular characteristics of each medical picture. To add insult to injury, the combination of machine learning techniques with chaotic encryption may make it easier to pick parameters, which in turn increases the effectiveness of encryption and strengthens defences against new attacking strategies. The expansion of the algorithm's functions to support a variety of Internet of Things devices and networks, in particular edge computing frameworks, provides a huge potential to improve the algorithm's significance in the field of healthcare. To summarise, the introduction of a 6D chaotic map-based picture encryption method represents a significant step forward in the process of assuring safe, real-time image processing for applications related to the Internet of Things in the medical field. This approach strikes a balance between robust security features and computing efficiency, therefore offering a feasible and scalable solution to the growing demand for secure medical data transfer via Internet of Things (IoT) networks.

## ACKNOWLEDGMENT

The authors like to convey their profound appreciation to the Department of Information Technology at Noorul Islam Centre for Higher Education, Tamil Nadu, India, for their steadfast support and encouragement during this project. Gratitude is expressed to the team members and colleagues whose thoughts and constructive criticism have greatly enhanced the creation and refining of this work.The authors thank the support of OpenAI's ChatGPT in improving the manuscript's clarity and consistency. The cooperative atmosphere cultivated by the scientific community has been essential in realising this work.The authors express their sincere gratitude to all individuals who have directly or indirectly contributed to the successful completion of this research.

## REFERENCES

[1] Wang, X., et al. (2021). 4D Chaotic Map-based Image Encryption. *Entropy*, 23(8), 835.
[2] Zhou, Y., et al. (2023). 3D Chaotic Encryption for Secure Image Transmission. *IEEE Transactions on Information Forensics and Security*.
[3] Liu, C., & Chen, G. (2021). Chaotic Encryption Using 6D Systems. *Nonlinear Dynamics*, 106(2), 187-199.
[4] Patidar, V., et al. (2022). Pixel Permutation in Chaotic Image Encryption. *IEEE Access*, 10, 102964-103025.
[5] Zhang, T., et al. (2022). Image Encryption Techniques for Wireless Networks. *IEEE Wireless Communications*, 29(6), 94-102.
[6] Huang, J., et al. (2020). XOR Diffusion for Robust Image Encryption. *Information Sciences*, 512, 1200-1215.
[7] Al-Otum, H., & Shehab, A. (2022). Survey on Chaotic Encryption for Image Security. *IEEE Access*, 9, 1534-1555.
[8] Xiao, D., et al. (2021). Substitution Techniques in Image Encryption. *Entropy*, 23(5), 511.
[9] Ahmad, S., et al. (2022). Comparative Analysis of Highdimensional Chaotic Maps. *IEEE Transactions on Multimedia*, 24, 2225-2235.
[10] Li, S., et al. (2021). Key Sensitivity in Chaotic Image Encryption. *Entropy*, 23(3), 321.
[11] Sun, Q., et al. (2023). High-dimensional Chaos in Image Encryption: A Review. *Chaos, Solitons & Fractals*, 159, 112071.
[12] Khan, M. S., et al. (2022). Lightweight Image Encryption for IoT: Chaotic Maps and XOR Techniques. *Journal of Information Security and Applications*, 66, 103091.
[13] Javed, A., & Masood, F. (2021). Performance Analysis of Chaotic Map-based Image Encryption for IoT Devices. *IEEE Access*, 9, 147346-147355.
[14] Huang, Y., et al. (2020). Review on Chaotic-based Lightweight Cryptographic Techniques for IoT Security. *IEEE Internet of Things Journal*, 7(10), 9271-9281.
[15] Rahman, H., et al. (2021). 6D Hyperchaotic Maps in Lightweight Cryptography. *International Journal of Electronics and Communications*, 129, 153510.
[16] Lee, D., et al. (2023). Advanced Image Encryption for IoT Applications Using Chaotic Sequences and Permutation. *Computers & Security*, 127, 102983.
[17] Deng, L., & Xu, W. (2022). XOR Diffusion and Permutation in Chaotic Map Encryption for Real-time IoT. *Journal of Real-Time Image Processing*, 19, 647-656.
[18] Chen, F., et al. (2021). Survey of Lightweight Image Encryption Algorithms Using High-dimensional Chaos. *Electronics*, 10(5), 573.
[19] Ali, S., et al. (2020). Chaotic Maps and Image Scrambling Techniques for Secure Medical Data Transmission in IoT. *Wireless Personal Communications*, 114, 3031-3050.
[20] Zhao, Y., et al. (2024). Lightweight Encryption for Edgebased IoT Applications: A Chaotic Map Approach. *IEEE Transactions on Industrial Informatics*.