Journal of Theoretical and Applied Information Technology
31st December 2024. Vol.102. No. 24
© Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURE AND EFFICIENT MEDICAL IMAGE ENCRYPTION FOR MEDICAL CYBER PHYSICAL SYSTEM USING CHAOTIC WITH DNA SEQUENCE

KAILASAM SELVARAJ[1], KARTHEEBAN KAMATCHI[2]

[1]Research Scholar, Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, India

[2]Associate Professor, Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, India

E-mail: [1]kailashsrivi@gmail.com, [2]k.kartheeban73@gmail.com

ABSTRACT

In contrast to the conventional healthcare industry, Medical Cyber-Physical Systems increasingly utilize smart sensor technology and health app to ensure enhanced healthcare. Medical imaging has become essential in recent years for disease diagnosis. These images include X-rays, ultrasound, and the brain which contains private and delicate information. There are many difficulties with the protected sharing and storing of medical images. The protection of medical information is increased through the use of encryption. The research recommends protected and lightweight medical image encryption using chaotic with DNA sequences for a medical cyber-physical system. First, the image is divided into blocks, rotated based on local pixel intensity variance, and shuffled using random permutation. The shuffled blocks are then reassembled, and a bitwise XOR operation completes the encryption, with a key generated from chaotic logistic maps and DNA symbols. Analytical evaluations show the proposed method outperforms earlier techniques, offering stronger security for medical data.

Keywords: *MCPS, Medical Image, Encryption, Chaotic, DNA, Xor operation, image blocks, image rotation, imaging, Measure and Integration*

1. INTRODUCTION

The notion of a "cyber-physical system" (CPS) describes the fusion of computation, the online and offline physical environments, and computer networks. Connected networks and computers are also used to oversee and control the physical operations through feedback loops. Sensors collect an enormous amount of data from the outside world. After that, these data are transferred to the digital realm for analysis and processing. The objective of the CPS is to perform essential functions by integrating intelligence into standard goods and services [1].

A special kind of CPS in smart healthcare that combines cyber and physical space is called a medical cyber-physical system (MCPS) [2]. The physical environment serves as the MCPS's structural base. It consists of a variety of real-time significant health sensing devices and diagnosis devices as well as a user space made up of various users. It sends sensing data to the internet via sensing devices and gets control data from it to operate physical equipment. The key element of MCPS is cyber space, which is in charge of handling user and health data analysis, storage, and access data security. As the MCPS's neurological center, the cyber space recognizes, collects, processes, and stores the detecting data from the physical space via network communication systems creates the feedback control data, and then sends it back to the physical environment via network transmission systems [3].

The typical MCPS architecture contains four layers [4]: Data Acquisition, Data Pre-processing, data storage, and action Figure 1 shows the four-layer architecture. Different constraints are used to describe each layer. Various cryptographic methods must be used to secure communication between the layers. An MCPS must offer certain characteristics at every level, including data privacy. Medical data access is restricted to those with the proper authorization owing to unique encryption techniques. This paper provides security for medical images.

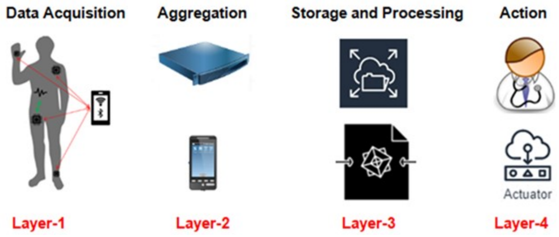


Figure 1: MCPS Layer architecture

Digital images can generally be secured via image steganography [5], watermarking [6], and encryption [7]. Encryption, which uses a secret key to turn a picture into an unintelligible form, is the simplest and most efficient method of securing medical image security. Nobody can retrieve the original image if they don't have the secret key. The conventional techniques RSA [8] and AES [9] have been used to encrypt medical imaging data. These methods are not very effective because of the intrinsic qualities of images, such as more connection among nearby pixels, substantial duplication, and vast data storage. As a result, numerous studies have made substantial use of chaos-based systems [10] [11] [12] to encrypt medical images.

The innovative field of chaos-based cryptography uses different chaotic maps to produce arbitrary sequences for digital medical image encryption [13] [14]. These low-level chaotic maps exhibit strange properties including entropy, unusual attractors with different beginning keys, susceptibility to initial states, and non-linearity. These features can be used to build a robust cryptosystem [15] [16]. Chaos-based cryptography doesn't necessarily offer high-level protection [17], as a result of some chaos maps' subpar statistical features [18], poor dissemination functions, and vulnerability to known and deliberate plaintext assaults. To create more reliable image cryptosystems, chaos maps have been combined with various algorithms, including DNA coding [19], cellular automata [20], and other combinations [21] [22].

Many researcher [19] [32] [35] [37] suggests chaos and DNA coding for image encryption. Chaos-based DNA image encryption has some drawbacks, including Single DNA operation rules resulted in easy cracking, poor security performance because of the low correlation, vulnerability to plaintext attack, and high computation time and complexity. This research increases security performance (high correlation), reduces the computation time and complexity through lightweight medical image encryption. This paper use DNA sequences (only symbols) without DNA operation (addition, subtraction) and encoding rules.

With high resolution, significant correlation, and big storage capacity, the present image encryption techniques have several drawbacks for medical image encryption, and it is challenging to generate trustworthy clinically usable medical images. The above said challenges have been overcome through the proposed algorithm. This research suggests a secure and lightweight medical image encryption using chaotic with DNA sequence for a medical cyber-physical system. First, the image is divided into an equal number of blocks, and the rotation of the blocks is done according to the local variance of the intensity of the pixels. After that, random permutation is used to shuffle the rotated picture blocks, and finally, one image is generated for encryption by reassembling the shuffled blocks. With the help of bitwise XOR operation, the encryption of the medical image is completed, and the key is created by combining chaotic logistic and DNA symbols.

The paper's outline structure is as follows: The related fields of medical image encryption and cyber-physical space are covered in Section 2. The suggested medical picture encryption is explained in Section 3, and the empirical results are explained in Section 4. The conclusion and next steps are covered in Section 5.

2. RELATED WORK

2.1 Medical CPS

The development of technology to safeguard patient safety is essential given major cybercrime. A selective encryption technique along with segmentation and dissemination are the fundamental components of the secure data storage and distribution approach proposed by Qiu et al., [23], which ensures data security and privacy even when the transmission medium and credentials are exposed. It is an extension of a user-centric system that grants access permissions to the end user for information exchange while safeguarding data on dependable devices, such the user's smartphone. The blockchain-based certificate-less collective signature technique is presented by Shu et al., [24] that can be utilized for the safe exchange and archiving of medical information in MCPS. In this method, health records are exchanged on the blockchain and maintained off the blockchain in a two-layer system model. It offers identity confidentiality and message authentication that fulfills MCPS's security criteria.

To train disease detection models using distributed medical imaging data, Guo et al. [25] offer a scheme based on federated learning in MCPS. This plan can not only successfully address the issue of protecting confidentiality, but it can also address the issue of choosing the right model for doctors and reducing storage requirements. It can guarantee that customers receive a continuously enhanced diagnostic system. Udayakumar et al. [26] present a blockchain-based safe image transfer and diagnosis system for the MCPS environment. This method includes an image capture strategy that allows wearable technology to take medical information. This model implements an intrusion detection system that looks for intruders inside the MCPS using a recurrent neural network.

Tyagi et al., [27] present a decentralized e-healthcare application model. To safeguard Medical Cyber-Physical Systems, an intelligent access-control technique is proposed. A simple specification-based method for managing misbehavior identification is proposed by Choudhary et al. [28]. It uses automatic model inspection and formal verification to find misbehavior in an IoT device that is integrated into a medical cyber-physical system.

2.2 Medical Image Encryption

Kamal et al. [29] suggest a method for encrypting both grayscale and color medical photos. The image is partitioned into numerous chunks. The zigzag sequence, rotation, and arbitrary shuffling were used to jumble the blocks. A key is then generated via a disorganized logistic map to decode the scrambled image. By applying the modification approach, Masood et al. [30] offer a strong multi-stage cryptographic scheme for medical image encryption. This complex cryptographic approach minimizes correlation between the pixels in digitized medical images by using random integers derived from chaos maps.

Khashan et al. [31] provide a straightforward cryptographic technique for encoding the boundary maps of medical pictures. To obtain a boundary map, a boundary-finding scheme is first applied. A large key is created using a chaotic map. The significant discovered picture blocks are suggested to be encrypted using a one-time pad technique. Ravichandran et al. propose a two-stage approach for encrypting medical images in [32]. In the very first stage of the shuffling process, block confusion gives way to row and column pixel scrambling. At the first step of distribution, the pixels of the jumbled image are bitwise and coaxially warped to strengthen the system's defense against differential assault. The basis of the second step of the dissemination operation is DNA coding and xor operations.

For the purpose of creating a block cipher that can be used to encrypt and decrypt medical images, a model deep learning-based method [33] is recommended. The learning model used to create the key is the generative adversarial network. The objective is to find out the mapping connection between the original image and the secret key. Javan et al. [34] describe a technique for encrypting medical images based on multi-mode synchronization of hyper-chaotic systems. In the first instance, there are certain response systems attached to the main system, while in the second instance, there is circular synchronization. This paper suggests a lightweight medical image encryption technique for MCPS.

The paper by K. Shankar et al. [40] focuses on enhancing medical image security using a chaos-based encryption technique. Traditional encryption methods are not always effective for images due to their size and pixel correlation, leading to the adoption of chaos theory, known for its randomness and sensitivity to initial conditions. The authors propose an optimal key generation technique using a chaotic map that ensures high security and resistance to various attacks like brute-force and statistical analysis. Their method improves image scrambling for better diffusion and confusion while preserving medical image quality, making it suitable for secure transmission and storage in healthcare applications.

3. PROPOSED APPROACH

This section introduces the proposed method to encrypt medical images by using DNA sequences and chaotic systems. This figure represents a structural design illustration. Figure 2 The encryption process involves several key steps to ensure the secure transmission and storage of medical images. It splits the original image into smaller components to make it harder to decode the original image. Rotating these components, the structure of the image is further distorted. Next the image is shuffled, meaning that it loops through and rearranges the pixel position so there are no identifiable patterns left. This being creates an image that looks disturbing at first and seems illegible without the correct key. Meanwhile, using chaotic sequences of DNA coding technologies generates a secure key with extremely high randomness. It encrypts this in an image using a key that it also generates and later returns the encrypted scrambled image. It ensures that the encrypted medical image is highly resistant to different types of attacks, even with little or no information, while preserving good integrity and privacy.

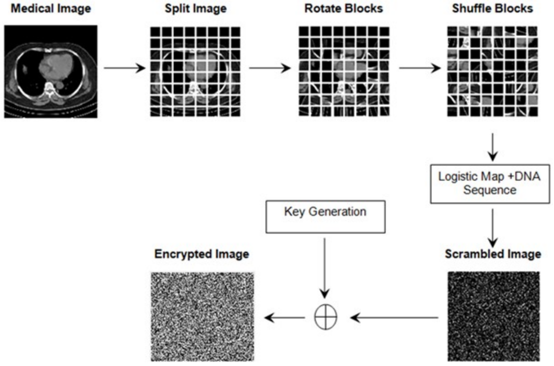


Figure 2: Medical Image Encryption Block Diagram

3.1. Split Image

MI is the grayscale medical image, with dimensions of xxx rows by yyy columns. The image is first cropped to the fixed resolution of 128 x 128 for standardize the encryption process The MI is split into multiple evenly sized blocks after resizing it to enable operations behind. The block size can be 8, 16 or 32 pixels according user requirements which is also generating more choices for the level of detail and processing complexity in visual imaging. Figure 3 shows how different block sizes impact the medical image structure and its encryption process, as in the partitioning of an input image. Figure 3 Input Extraction Block Size Fig. 3: Various Block Sizes + Medical Image Training /Transient Encryption → Along with a medical image for training purposes or transiently encrypted segments. With every block size, distinct structures can be encrypted during the training or transient stage.

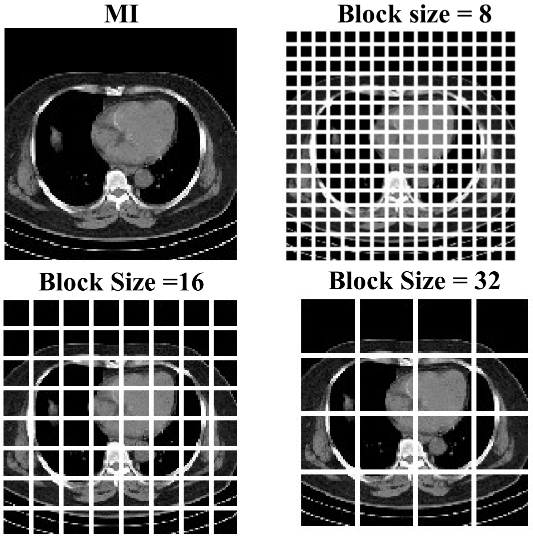


Figure 3: Image Splitting with different block sizes.

3.2. Rotate Image

Based on the pixel value's mean and variance, block of the image is rotated. The pixel mean value is computed as,

$$\mu = \frac{1}{xy}\sum_{i=1}^{x}\sum_{j=1}^{y} MI_{ij} \qquad (1)$$

The variance of pixel intensity is computed as,

$$\sigma^2 = \frac{1}{xy}\sum_{i=1}^{x}\sum_{j=1}^{y}\left(MI_{ij} - \mu\right)^2 \qquad (2)$$

The image blocks can be rotated by 90°,180°, and 270° based on the local variance of pixel intensity. The rotation angle (90°,180°,270°) can be identified as,

$$ang = \begin{cases} 0°, & if\ mod(\mu,2) = 0\ and\ mod(\sigma^2,2) = 0 \\ 90°, & if\ mod(\mu,2) = 0\ and\ mod(\sigma^2,2) \neq 0 \\ 180°, & if\ mod(\mu,2) \neq 0\ and\ mod(\sigma^2,2) = 0 \\ 270°, & if\ mod(\mu,2) \neq 0\ and\ mod(\sigma^2,2) \neq 0 \end{cases} \qquad (3)$$

The image rotation for different angles is shown in Figure 4.

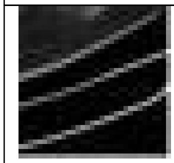
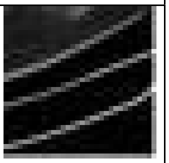
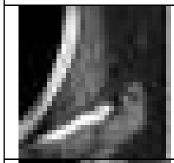
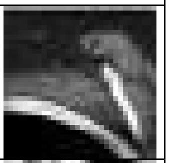
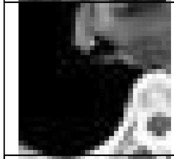
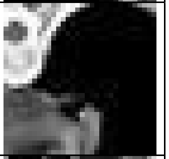
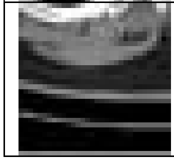
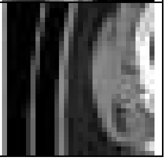
Image Blocks	Mean and Variance	Angle	Rotated Blocks
	32, 124	0°	
	70, 229	90°	
	61, 398	180°	
	69, 251	270°	

*Figure 4: Image R*otation for different angles

3.3. Shuffle Image

This function will randomly shuffle the rotated image blocks using permutation. The method of taking n elements randomly from a pre-defined set and arranging them in some order is referred to this technique. As an example, if that image is decomposed into 8 blocks identified as {1, 2, 3, 4, 5, 6, 7} and {8}, then this random shuffling could switch those blocks to a new progression of

{3, 6, 8, 2, 1, 4, 7, 5}. This random shuffling process improves the security by complicating and making the image more unpredictable. Visual randomness in the shuffled image blocks is illustrated in figure 5.

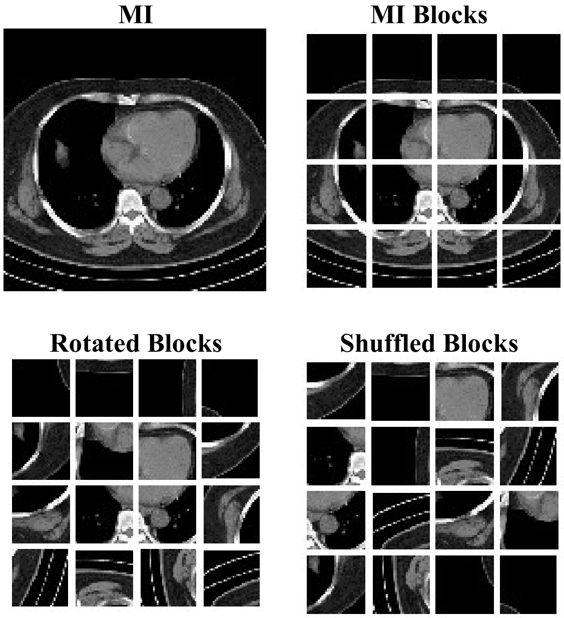


Figure 5: Shuffled blocks

3.4. Scramble Image

The DNA symbols and logistic map are used to create the jumbled image. We apply the logistic map to map a degree two polynomial. It is frequently used as a representative illustration of how extremely straightforward nonlinear dynamical methods may produce intricate chaotic phenomena [35]. It is one of the straightforward methods that display the shift from order to chaos and possesses many of the characteristics necessary for a pseudorandom number generator (PRNG) [36]. The quality of randomness is frequently the primary factor that separates various PRNGs. Additionally, throughput, implementation costs, and randomness quality are crucial considerations when assessing the efficacy of PRNGs in applications. The logistic map can produce an infinitely long chaotic sequence of numbers for the greatest significance of its process parameter. The logistic random number generator is limitless, irregular, and uncorrelated in contrast to the common congruential arbitrary number producer, which is cyclic. It is specified formally as:

$$map_{i+1} = r * map_i(1 - map_i) \tag{4}$$

Where and i is the iteration. When the control parameter is between [3.57, 4.0], the logistic map is chaotic.

Except for computer science, DNA sequencing has become very valuable for basic biological research and in many applied domains, including medical, forensic, and biological systematics [37]. The gene order is composed of four nucleotides: adenine (A), thymine (T), guanine (G), and cytosine (C).

The logistic map is used in this paper to create the DNA sequence.

$$dna = \begin{cases} 'A', & if\ map_i < 0.25 \\ 'C', & if\ map_i \geq 0.25\ and\ map_i < 0.5 \\ 'G', & if\ map_i \geq 0.5\ and\ map_i < 0.75 \\ 'T', & Otherwise \end{cases} \tag{5}$$

The scrambled image is generated based on the DNA symbols. The symbols A, C, G, and T are combined. For example, if DNA = ACTCTGTCTCTG then combine similar symbols. ACCCCGGTTTTT.

3.5. key Generation

The following formula is used to generate the key:

$$key_{i+1} = cos(q * acos(key_i)) \tag{6}$$

Where q and i is the iteration.

3.6. Encrypt Image

In this stage, the image pixels are altered, leading to the generation of a noisy, unintelligible image. To achieve this, the encryption process utilizes a secure key K and the jumbled image's vector, applying a bit-wise XOR function to scramble the pixel values further. The resulting output is the encrypted image, which is highly resistant to unauthorized access. The step-by-step encryption process is outlined in Algorithm 1. To retrieve the original image, the decryption process is simply the reverse of encryption, where the same key K is applied to reverse the transformations and recover the input image.

Algorithm-1 Encryption Process

```
Input: Medical Image MI with x rows and y columns, blocksize
Output: Encrypted Image encImg
Step01: Split MI into the number of blocks with equal blocksize.
Step02: For each block
Step03: Compute mean value using (1)
Step04: Compute variance using (2)
Step05: Find angle (θ) using (3)
Step06: Rotate the block based on the angle (θ)
Step07: End For
Step08: RN = generate random vector with $\frac{xy}{blocksize^2}$
Step09: Shuffle blocks based on RN
Step10: Generate a logistic map using (4)
```

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

```
Step11: Generate DNA sequence using (5)
Step12: To combine similar symbols to get the scrambled image scr.
Step13: Generate key using (6)
Step14: Convert scr into pixel vector imgV
Step15: $e1 = imgV \oplus key$
Step16: Convert e1 vector into image encImg
```

4. EXPERIMENTAL RESULTS

This section highlights the effectiveness of the proposed encryption method. The medical image encryption system was implemented using MATLAB on a system with an Intel Pentium® processor (2.30 GHz), 4GB of memory, and running Windows 10. To thoroughly evaluate the cryptographic technique, a variety of benchmarks and medical images were selected. The set of images used for testing includes not only standard benchmark images but also actual medical images, such as CT scans and X-rays. This diverse range ensures that the encryption method is tested across different types of images, allowing for a robust analysis of its performance.

Each image, whether a benchmark or a medical one, was resized to 128 x 128 pixels for consistency in the encryption process. This uniform size ensures that all images are processed under the same conditions, providing reliable and comparable results. Figures 6 and 7 present sample standard and medical images used in the experiments, offering a visual reference for the types of images encrypted during the study.

The use of both standard and medical images in testing allows for a comprehensive evaluation of the proposed method’s ability to secure sensitive medical data while ensuring that it performs well across different image types.

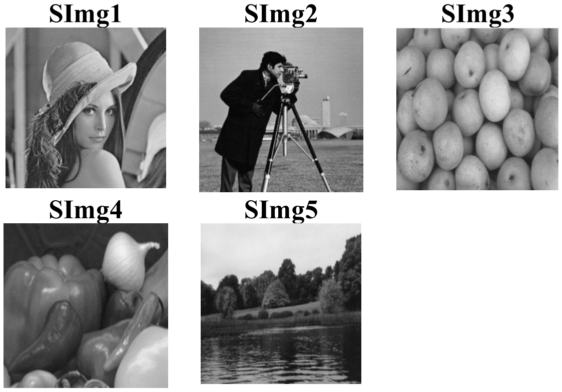


Figure 6: Standard Test Images

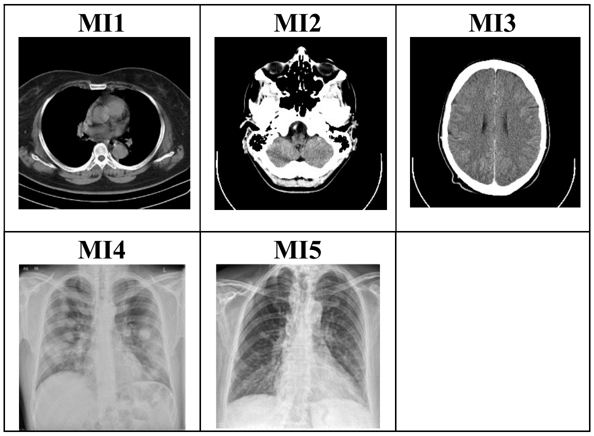


Figure 7: Medical Test Image

The efficacy of the suggested encryption method is assessed via the metrics listed below.

Information Entropy is a measurement of the image's unpredictability. It is defined as:

$$H(c) = \sum_{i=1}^{w} P(c_i)\, log_2 \frac{1}{P(c_i)}$$

where P(c) is the chance that c will appear, and the highest value of entropy for greyscale images is 8. The pixels in the image are more randomly dispersed if the entropy is near 8.

When analyzing encrypted images, correlation distributions and correlation coefficients are of utmost importance.

$$\begin{cases} E(x) - \frac{1}{N}\sum_{a-1}^{N} x_a \\ D(x) - \frac{1}{N}\sum_{a=1}^{N} (x_a - E(x))^2 \\ Cov(x,y) = \frac{1}{N}\sum_{a=1}^{N} (x_a - E(x))(y_a - E(y)) \\ \gamma_{x,y} = \frac{Cov(x,y)}{\sqrt{D(x)D(y)}} \end{cases}$$

The algorithm's efficiency was evaluated using both the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). It premeditated as,

$$NPCR = \frac{1}{xy}\sum_{a=1}^{x}\sum_{b=1}^{y} D(a,b) * 100$$

$$D(a,b) = \begin{cases} 0 \; if \; E_1(a,b) = E_2(a,b) \\ 1 \; if \; E_1(a,b) \neq E_2(a,b) \end{cases}$$

$$UACI = \frac{1}{xy}\sum_{a=1}^{x}\sum_{b=1}^{y} \frac{|E_1(a,b) - E_2(a,b)|}{255} * 100$$

The original and encrypted images' difference is measured using the peak signal-to-noise ratio (PSNR). It can be computed by,

$$PSNR = 10 * log_{10}(\frac{255^2}{MSE})$$

$$MSE = \frac{1}{xy}\sum_{a=1}^{x}\sum_{b=1}^{y}|OI(a,b) - EI(a,b)|^2$$

The original image is referred to as OI and the encrypted image as EI. A considerable divergence between the input and the encrypted image is indicated by lower PSNR values.

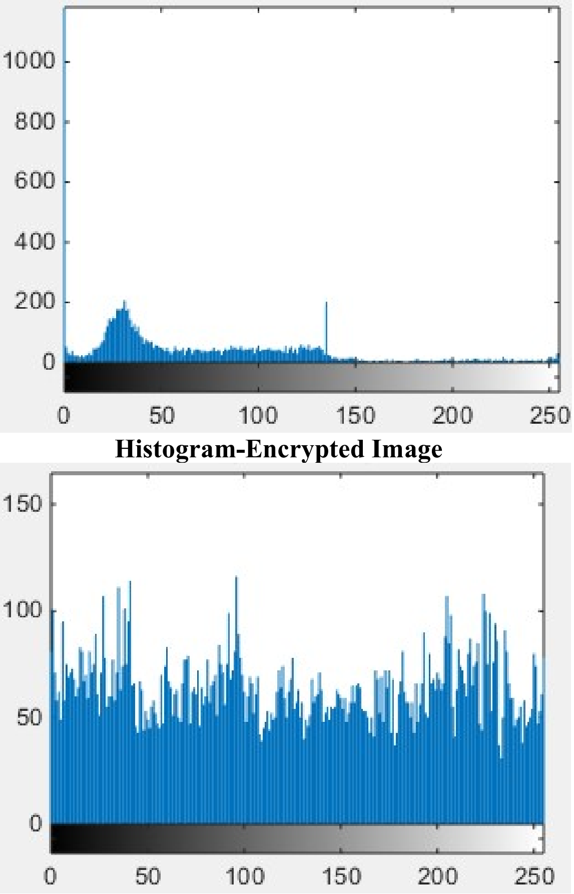
The metrics for standard and medical images are shown in Table 1.

Table 1: Metrics for standard and Medical Images

S.No	Entropy	Correl-ation	NPCR	UACI	PSNR
SImg1	7.9851	1.0	99.53	14.86	9.474
SImg2	7.9839	1.0	99.65	17.48	8.6012
SImg3	7.9839	1.0	99.56	10.85	9.7718
SImg4	7.9858	1.0	99.62	20.45	8.6740
SImg5	7.9820	1.0	99.53	20.78	7.3151
MI1	7.9596	1.0	99.59	37.00	6.1189
MI2	7.9306	1.0	99.47	35.12	5.23
MI3	7.9426	1.0	99.49	33.39	6.0364
MI4	7.9761	1.0	99.57	7.32	9.724
MI5	7.987	1.0	99.65	8.23	8.398

The histogram of an image shows the number times each pixel value occurs which will provide us with some intuition about the overall structure of the image. The histogram of an encrypted image needs to be flat, meaning there is equal probability of any pixel value around a uniform distribution. This flatness makes difficult for a hacker to extract some useful data or patterns from the image. Similarly the histograms of original(input) and encrypted image should be more random as well. When its values are too close to each other it could mean that we are exposing information about how the encryption process works. Although not optimized for the proposed use case, this contrast is effectively demonstrated in Fig. 8 by comparing the histograms of medical images to that of its corresponding encrypted version (MI1).

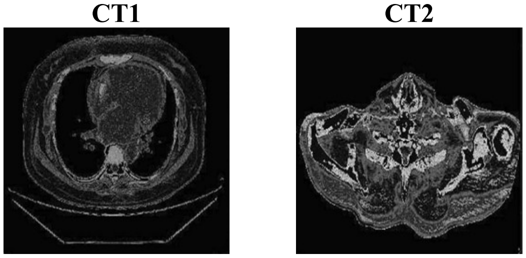
Histogram- Input Image



Histogram-Encrypted Image

Figure 8: Histogram for Image-MI1

The suggested medical image encryption approach is compared with the scheme Chaos-MIE [30], EM-DNA [35], HC-DNA [38] and S-HC-DNA [39]. Figure 9 shows the sample images for comparison.



CT1 **CT2**

Figure 9: CT Images for Comparison

Entropy, NPCR and UACI comparison for CT Images are shown in Table2.

Table 2: Entropy, NPCR and UACI Comparison

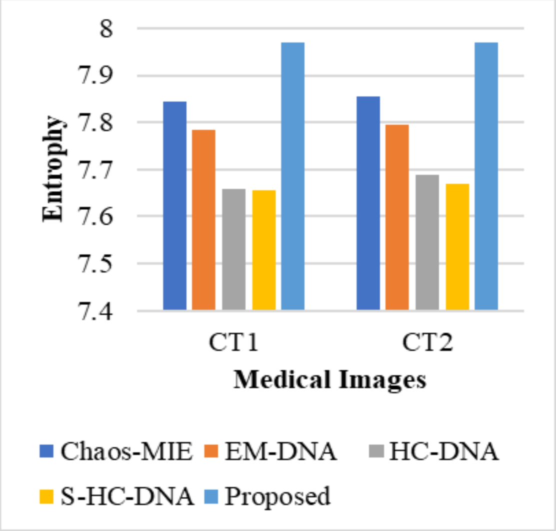
Methods	CT1		
	Entropy	NPCR	UACI
Chaos-MIE	7.8447	99.62	33.65
EM-DNA	7.7842	99.5	37.22
HC-DNA	7.6596	48.67	18.58
S-HC-DNA	7.6554	53.39	19.93
Proposed	7.9694	99.71	39.59

Methods	CT2		
	Entropy	NPCR	UACI
Chaos-MIE	7.8539	99.60	33.65
EM-DNA	7.7955	99.31	38.34
HC-DNA	7.6895	50.57	19.25
S-HC-DNA	7.6684	50.21	19.35
Proposed	7.9686	99.74	39.96

Figure 10 shows the CT image entropy NPCR and UACI comparison. The proposed approach has high entropy. NPCR and UACI compared to Chaos-MIE, EM-DNA, S-HC-DNA and HC-DNA methods.

Furthermore, the image encryption methods should also fulfill it of real-life timing for preprocessing the patients sensitive information. The speed of an encryption algorithm affects if it can be implemented on various medical and engineering applications. While there are complex encryption methodologies that provide heightened levels of security, they tend to be notoriously long to compute, hence inefficient for real time applications. Such methods tend to be slow when lossy and can have impractical execution times in contexts where data is processed quickly.

The proposed encryption approach addresses this issue by offering significantly faster execution times compared to the S-HC-DNA method. Despite maintaining a high level of security, the proposed method is more efficient and better suited for real-world applications where time is a critical factor. Table 3 presents a comparison of the execution times between the S-HC-DNA method and the proposed approach, highlighting the substantial reduction in computation time, making it more practical for everyday use in securing medical images.



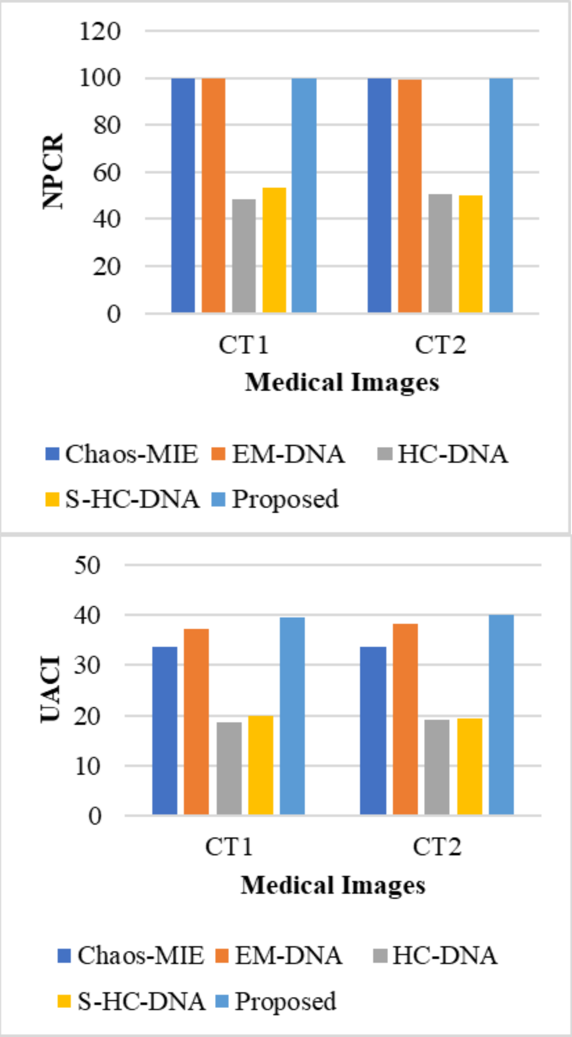


Figure 10: Comparison of Entropy, NPCR and UACI

In addition to safeguarding patients' confidential details, effective image encryption techniques must also adhere to time constraints. Typically, the algorithm's running time has a significant impact on whether it can be applied in practise. Even though a complicated encryption technique works well, the high computation time makes it impractical for engineering. The proposed approach take very less execution time compared to S-HC-DNA method. Table 3 shows the execution time of S-CH-DNA and proposed approach.

Table 3: Execution Time Comparison

Image	S-HC-DNA	Proposed
CT1	281.8	174.5
CT2	181.9	169.3

5. CONCLUSION AND FUTURE WORK

A CPS used in medical fields is called MCPS. Expanding the research and application of MCPS is essential to improving the global healthcare service system and elevating the grade of medical care. The requirement for a safe encryption method to safeguard private data in medical images is emphasized in this research. This paper presents a health cryptography approach based on image blocks, disordered with gene sequence. Experiments with both ordinary and medical pictures are used to evaluate the usefulness of the proposed technique. The metrics entropy, correlation, and histogram are analyzed. The result shows that the proposed encryption method is more effective than other prior encryption techniques. In the future, the proposed encryption approach is enhanced with the hybrid chaotic map with QR code-based encryption.

REFERENCES:

[1] Duo, W., Zhou, M., & Abusorrah, A, "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges", IEEE/CAA Journal of Automatica Sinica, 9(5), 2022, 784-800.

[2] Priyadarshini, I., Kumar, R., Tuan, L. M., Son, L. H., Long, H. V., Sharma, R., & Rai, S, "A new enhanced cyber security framework for medical cyber physical systems", SICS Software-Intensive Cyber-Physical Systems, 35(3), 2021, 159-183.

[3] Chen, F., Tang, Y., Wang, C., Huang, J., Huang, C., Xie, D., et al, "Medical cyber-physical systems: A solution to smart health and the state of the art", IEEE Transactions on Computational Social Systems, 9(5), 2021, 1359-1386.

[4] Kocabas, O., Soyata, T., & Aktas, M. K, "Emerging security mechanisms for medical cyber physical systems", IEEE/ACM transactions on computational biology and bioinformatics, 13(3), 2016, 401-416.

[5] Biradar, R. L, "Secure medical image steganography through optimal pixel selection by EH-MB pipelined optimization technique", Health and Technology, 10(1), 2020, 231-247.

[6] Kahlessenane, F., Khaldi, A., Kafi, R., & Euschi, S, "A robust blind medical image watermarking approach for telemedicine applications", Cluster computing, 24(3), 2021 2069-2082.

[7] Abdulbaqi, A. S., Obaid, A. J., & Mohammed, A. H, "ECG signals recruitment to implement a new technique for medical image encryption", Journal of Discrete Mathematical Sciences and Cryptography, 24(6), 2021, 1663-1673.

[8] Jain, M., & Kumar, A, "RGB channel based decision tree grey-alpha medical image steganography with RSA cryptosystem", International Journal of Machine Learning and Cybernetics, 8(5), 2017, 1695-1705.

[9] Hafsa, A., Sghaier, A., Malek, J., & Machhout, M, "Image encryption method based on improved ECC and modified AES algorithm", Multimedia Tools and Applications, 80(13), 2021, 19769-19801.

[10] Liu, J., Ma, Y., Li, S., Lian, J., & Zhang, X, "A new simple chaotic system and its application in medical image encryption", Multimedia Tools and Applications, 77(17), 2018, 22787-22808.

[11] Vaseghi, B., Mobayen, S., Hashemi, S. S., & Fekih, A, "Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption", IEEE Access, 9, 2021, 25911-25925.

[12] Gafsi, M., Abbassi, N., Hajjaji, M. A., Malek, J., & Mtibaa, A, "Improved chaos-based cryptosystem for medical image encryption and decryption", Scientific Programming, 2020.

[13] Ahmad, J., Masood, F., Shah, S. A., Jamal, S. S., & Hussain, I, "A novel secure occupancy monitoring scheme based on multi-chaos mapping", Symmetry, 12(3), 2020.

[14] Wang, S., Wang, C., & Xu, C, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm", Optics and Lasers in Engineering, 128, 2020.

[15] Qayyum, A., Ahmad, J., Boulila, W., Rubaiee, S., Masood, F., Khan, F., & Buchanan, W. J. et al, "Chaos-based confusion and diffusion of image pixels using dynamic substitution", IEEE Access, 2020.

[16] Masood, F., Ahmad, J., Shah, S. A., Jamal, S. S., & Hussain, I, "A novel hybrid secure image encryption based on Julia set of fractals and 3D Lorenz chaotic map", Entropy, 22(3), 2020, 274

[17] Norouzi, B., Mirzakuchaki, S., & Norouzi, P, "Breaking an image encryption technique based on neural chaotic generator", Optik, 140, 2017, 946-952.

[18] Parvin, Z., Seyedarabi, H., & Shamsi, M, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function", Multimedia Tools and Applications, 75(17), 2016, 10631-10648.

[19] Belazi, A., Talha, M., Kharbech, S., & Xiang, W, "Novel medical image encryption scheme based on chaos and DNA encoding", IEEE access, 7, 2019, 36667-36681.

[20] Wang, X., & Guan, N, "Chaotic image encryption algorithm based on block theory and reversible mixed cellular automata", Optics & Laser Technology, 132, 2020, 106501.

[21] Tang, Z., Yang, Y., Xu, S., Yu, C., & Zhang, X, "Image encryption with double spiral scans and

chaotic maps", Security and Communication Networks, 2019.

[22] Zhou, N., Yan, X., Liang, H., Tao, X., & Li, G, "Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system", Quantum Information Processing, 17(12), 2018, 1-36.

[23] Qiu, H., Qiu, M., Liu, M., & Memmi, G, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0", IEEE journal of biomedical and health informatics, 24(9), 2020, 2499-2505.

[24] Shu, H., Qi, P., Huang, Y., Chen, F., Xie, D., & Sun, L, "An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems", Sensors, 20(5), 2020, 1521.

[25] Guo, K., Li, N., Kang, J., & Zhang, J, "Towards efficient federated learning based scheme in medical cyber-physical systems for distributed data", Software: Practice and Experience, 51(11), 2021, 2274-2289.

[26] Udayakumar, P., & Rajagopalan, N, "Blockchain enabled secure image transmission and diagnosis scheme in medical cyber-physical systems", Journal of Electronic Imaging, 31(6), 2022.

[27] Tyagi, A. K., Aswathy, S. U., Aghila, G., & Sreenath, N, "AARIN: Affordable, accurate, reliable and innovative mechanism to protect a medical cyber-physical system using blockchain technology", International Journal of Intelligent Networks, 2, 2021, 175-183.

[28] Choudhary, G., Astillo, P. V., You, I., Yim, K., Chen, R., & Cho, J. H, "Lightweight misbehavior detection management of embedded IoT devices in medical cyber physical systems", IEEE Transactions on Network and Service Management, 17(4), 2020, 2496-2510.

[29] Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M., & Fouda, M. M, "A new image encryption algorithm for grey and color medical images", IEEE Access, 9, 2021, 37855-37865.

[30] Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S. U., Jan, S. U., et al., "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations", Wireless Personal Communications, 127(2), 2022, 1405-1432.

[31] Khashan, O. A., & AlShaikh, M, "Edge-based lightweight selective encryption scheme for digital medical images", Multimedia Tools and Applications, 79(35), 2020, 26369-26388.

[32] Ravichandran, D., Banu S, A., Murthy, B. K., Balasubramanian, V., Fathima, S., & Amirtharajan, R, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain", Medical & Biological Engineering & Computing, 59(3), 2021, 589-605.

[33] Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K. K. R., & Qin, Z, "DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption", IEEE Transactions on Neural Networks and Learning Systems. 33(9), 2021, 4915-4929.

[34] Javan, A. A. K., Jafari, M., Shoeibi, A., Zare, A., Khodatars, M., Ghassemi, N., et al., "Medical images encryption based on adaptive-robust multi-mode synchronization of chen hyper-chaotic systems", Sensors, 21(11), 2021, 3925.

[35] Chakraborty, S., Seal, A., Roy, M., & Mali, K, "A novel lossless image encryption method using DNA substitution and chaotic logistic map", International Journal of Security and Its Applications, 10(2), 2016, 205-216.

[36] Murillo-Escobar, M. A., Cruz-Hernández, C., Cardoza-Avendaño, L., & Méndez-Ramírez, R, "A novel pseudorandom number generator based on pseudorandomly enhanced logistic map", Nonlinear Dynamics, 87(1), 2017, 407-425.

[37] Enayatifar, R., Abdullah, A. H., & Isnin, I. F, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence", Optics and Lasers in Engineering, 56, 2014, 83-93.

[38] Zhan, K., Wei, D., Shi, J., & Yu, J, "Cross-utilizing hyperchaotic and DNA sequences for image encryption", Journal of Electronic Imaging, 26(1), 2017, 013021-013021.

[39] Li, M., Pan, S., Meng, W., Guoyong, W., Ji, Z., & Wang, L, "Medical image encryption algorithm based on hyper-chaotic system and DNA coding", Cognitive Computation and Systems, 4(4), 2022, 378-390.

[40] K, Shankar., Mohamed, Elhoseny., E, Dhiravida Chelvi., S, K, Lakshmanaprabu., & Wanqing, Wu, "An Efficient Optimal Key Based Chaos Function for Medical Image Security", IEEE Access, (6), 2018, 77145 – 77154.