DICOM Medical Image Security with DNA- Non-Uniform Cellular Automata and JSMP Map Based Encryption Technique

Ahmed Naguib[1], Walid El-Shafai[1,2], Mona Shokair[1,3]

Abstract: **With the global proliferation of the Internet and digitalization transforming how information is shared, there has been exponential growth in the transmission of multimedia content fueled by advancing communication technologies. In recent times, Digital Imaging and Communications in Medicine (DICOM) medical imaging has become critical for disease diagnosis. Given that these images are often transmitted across networks, ensuring their robust protection has become imperative. Unauthorized access or misuse of the data within these images could potentially result in serious consequences. Various approaches exist for safeguarding such images, with encryption emerging as a highly effective method. Encryption algorithms typically involve two key phases: confusion and diffusion. This paper suggested proposed encryption technique designed specifically for encrypting both gray-scale and color DICOM medical images. Several assessment criteria, including the Number of Changing Pixel Rate (NPCR), Unified Averaged Changed Intensity (UACI), average entropy, correlation coefficients, Structural Similarity (SSIM), Feature Similarity (FSIM), and Peak Signal-to-Noise Ratio (PSNR), are employed to evaluate the suggested cryptosystem. These evaluations vividly underscore the robust security performance exhibited by the proposed approach.**

***Keywords— DICOM, FSIM, SSIM,* PSNR, UACI, NPCR, Entropy.**

I. Introduction

The amount of data is exploding due to the development of various technologies such as cloud, artificial intelligence, and big data. Along with the rapid development of wireless network technology such as mobile communication and multimedia display device technology, a lot of multimedia information is transmitted and shared through the Internet. Therefore, it is very important to protect images from problems such as illegal copying and illegal distribution. In particular, a stable and strong security system is required to protect personal or confidential information in systems such as military, medical, and financial systems [1]. In fact, encryption can make important and sensitive original images such as military images, medical images, and images containing personal information into unrecognizable images to safely protect images from those who do not have permission for the images [2]. It is well known that existing encryption techniques, such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are not sufficient to encrypt images. This is because image data, unlike text data, has a large data capacity and has high redundancy and strong correlation between adjacent image pixels [3]. Actually, an image encryption algorithm that provides better performance than zoned encryption techniques is needed.

There has been an enormous increase in the distribution and archiving of Digital Imaging and Communications in Medicine (DICOM) medical images in recent years [4]. With the widespread adoption of digital formats for medical records and the growing utilization of telemedicine services, large volumes of radiological and clinical imaging data are now routinely transmitted electronically and retained digitally. This reflects the vast gains in connectivity of healthcare networks and transition from traditional film-based to computational medical imaging modalities across the industry. Secure exchange and long-term preservation of such sensitive patient information embodied in DICOMs has become mission critical as a result of the massive escalation in the digital dissemination and remote access to these important medical files [5].

There are generally three main approaches to secure digital images - steganography, watermarking, and encryption. Steganography involves hiding information within other media, while watermarking embeds identifying signatures directly into image content. Encryption, on the other hand, is considered the most direct and efficient method [6-8]. It ensures medical image security by converting the original, or plaintext, image into an unreadable form (cipher image) using a secret encryption key. Without possession of this secret key, no one is able to convert the cipher image back to the original plaintext version. Image encryption relies on two primary operations - confusion and diffusion. In fact, confusion aims to disguise relationships between encrypted image pixels and the plaintext whereas diffusion aims to spread out these relationships, making relationships between cipher pixels and the plaintext robust against attacks. From these three

Manuscript received [03 November 2023]; accepted [23November 2023]. Date of publication [17 January 2024].

[1]Ahmed Naguib is with Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, 32952 Menouf, Egypt (e-mail: ahmed.naguib.mohamed@gmail.com).

[2]Walid El-Shafai is with Department of Computer Science, Security Engineering Lab, Prince Sultan University, Riyadh 11586 Saudi Arabia.

[3]Mona Shokair is with Faculty of Electrical Engineering, 6 October University, Egypt(e-mail: shokair_1999@hotmail.com).

approaches, encryption provides the most straightforward level of security for medical images transmitted and stored using cryptographic techniques and a secret key [9].

Image encryption technology based on chaos function is being actively studied by researchers [10], [11]. Chaos theory is a complex field of nonlinear mechanics that is extensively studied in several scientific and technological fields. Its function is widely used in the field of image encryption because it has characteristics such as sensitivity to initial conditions and dense periodic trajectories. Encryption algorithms commonly leverage chaotic systems for their dynamic cryptographic properties. One-dimensional (1D) chaotic maps such as sine map, cosine map, logistic map, tent map, quadratic map, etc [12], in particular provide efficient implementation due to their single variable structure, making them an attractive option. However, 1D chaotic maps are limited by their relatively small key spaces as all the values exist within a one-dimensional range. This constrains the number of possible keys and weakens the system's resistance to brute force attacks. While computationally simple, 1D chaotic maps alone may not adequately satisfy modern security requirements that demand large key spaces to ensure the infeasibility of exhaustive searches. Therefore, when selecting an encryption scheme based on chaotic systems, alternative designs utilizing higher dimensional maps should be considered to strengthen the algorithm's overall cryptanalysis and better protect sensitive information in today's threat landscape. But in recent times, a proposed 1D chaotic map that has a large space key is devised. This 1D chaotic map is called JSMP map [13].

In fact, DNA encryption is an emerging cryptographic technique that utilizes the properties of DNA to securely encrypt and decrypt data. At the core of DNA, encryption is the mapping of binary numbers or characters to DNA base sequences. The four nucleotide bases in DNA - adenine (A), thymine (T), cytosine (C), and guanine (G) - can be used to represent the zeros and ones in binary representations of data. Moreover, well-defined rules are used to systematically assign each binary digit or character to a specific base or base pair [14]. Once the input plaintext is converted to a DNA sequence, it can be securely stored or transmitted. At the receiving end, the same mapping rules are applied in reverse to decrypt the ciphertext back to the original plaintext. Furthermore, DNA cryptography presents notable advantages, including robust supporting for strong capability for concurrent/simultaneous execution in DNA computing, resulting in accelerated computational processes. DNA molecules serve as effective storage media, offering a substantial capacity for data transmission. Additionally, DNA encryption is characterized by its low power consumption, aligning with energy-efficient computing solutions. DNA encryption techniques have proven effective in real use cases ranging from medical records to messaging to digital signatures and blockchain applications [15], [16].

Cellular automata (CA) are discrete dynamic systems that have attracted significant interest from researchers across many fields including physics, mathematics, theoretical computer science, and complexity science. A cellular automaton consists of a regular grid of cells, each in one of a finite number of possible states, such as on and off. The grid can be in any number of dimensions, but the most commonly studied is the one-dimensional line and two-dimensional plane [17]. The evolution of a CA is determined by its initial state, and a set of mathematical rules that dictate how the state of each cell changes in the next iteration based on the current state of its neighboring cells. This process is repeated over multiple generations, leading to emergent global patterns and dynamics from the bottom-up interactions between cells. Notable types of CA include elementary cellular automata like the famous Game of Life, which can simulate complex phenomena such as self-replicating structures. Due to their decentralized parallelism and ability to mimic physical, biological and chemical systems, cellular automata have found wide application in fields as diverse as physics, computational science, cryptography and artificial intelligence. They provide a simple yet powerful framework for modeling complex systems [18].

There are two main types for CA, one called uniform CA, while the other called non-uniform CA. In uniform cellular automata, the same ruleset is applied to all cells in the grid, it is a homogenous system. Where, in non-uniform cellular automata different rulesets are applied to different cells or regions of the grid, it is a homogeneous system. Both uniform and non-uniform cellular automata have the potential to serve as the basis for novel cryptosystems by leveraging their emergent computational properties. Uniform CA are well-suited for applications involving encryption schemes that rely on chaotic behavior and the difficulty of predicting long-term dynamics [19]. Encryption keys could be derived from initial CA configurations, with the emergent patterns forming the encryption/decryption mappings. However, the highly symmetrical nature of uniform CA may render them more susceptible to attacks. In contrast, purposefully designed non-uniform CA could introduce cryptographically valuable asymmetries. By using distinct rulesets in different spatial regions, non-uniform CA facilitate computations that are difficult to reverse-engineer without full knowledge of the localized transition logics [20], [21].

Hence, our research is driven by the intention to present a streamlined medical image encryption system, employing principles of chaos theory, DNA encoding, and non-uniform cellular automata, tailored to enhance the security of telemedicine services. In the envisioned cryptographic system, a 1D chaotic system that has a large space key is used to generate initial data and rules needed for non-uniform cellular automata, the key image that generated from the non-uniform cellular automata was used for DNA encryption operations to encrypt the medical image into an encrypted image for safely transmission over the network. The proposed medical image encryption system was rigorously tested and evaluated using multiple experiments, comparisons, and analyses. The results demonstrated that the suggested cryptosystem provides enhanced security and faster processing speeds. It also exhibited robust resilience against different types of attacks, such as known-plaintext attacks and chosen-plaintext attacks, outperforming conventional schemes. Therefore, the key contribution of this research was leveraging the synergistic benefits of integrating JSMP map, DNA, and non-uniform cellular automata techniques within a single cryptographic framework. This unified approach significantly strengthened the protection of medical images transmitted for telemedicine and healthcare services by capitalizing on the complementary advantages of the given techniques. Overall, the proposed cryptosystem was shown to fulfill the urgent need for robust and efficient safeguarding of sensitive patient medical data communicated over modern digital networks supporting remote healthcare applications and telemedicine.

The principal contribution of our paper lies in presenting a highly efficient cryptosystem incorporating the proposed mathematical concept of cellular automata, combined with the robust key space provided by a four-dimensional hyperchaotic system. This proposed system finds application in cloud services and the realm of the Internet of Medical Things (IoMT).

This paper is organized in the following manner: Section II presents a detailed description of the proposed medical image encryption framework. Section III then examines and reports the outcomes of simulations performed to test the cryptosystem model. A comparative evaluation against related studies in the field is featured in Section IV. Finally, Section V summarizes the main conclusions.

II. PRPOSED MEDICAL IMAGE CRYPTOSYSTEM

The encryption and decryption processes are shown in Figures 1 and 2, respectively. When encrypting color medical images, the image is first separated into its fundamental components - Red (R), Green (G), and Blue (B). Each individual color component then undergoes its own processing in the encryption scheme before being combined back together. The encryption steps are performed separately on the R, G, and B components before they are put back together. Finally, after undergoing individual encryption, the ciphered R, G, and B parts are reassembled to reconstruct the ciphered color medical image as the end result.

A. JSMP Map

The JoanS-MuraliP's (JSMP) map is a novel one-dimensional chaotic map introduced to address limitations in existing chaotic maps used for cryptographic applications. Specifically, most one-dimensional maps exhibit limited and discontinuous chaotic ranges that provide weak security. The JSMP map was constructed using function composition of the logistic map and a simple quadratic map. As shown in the following equation [13]

$$y_{n+1} = [\beta^2 (y_n^2 - 5)(1 - \beta(y_n^2 - 5))] \bmod 1 \quad (1)$$

Where $y \in [0,1]$ and $\beta \geq 0.5$

Studies of the dynamical behavior of the JSMP map revealed the presence of a wide discontinuity band within its bifurcation diagram as shown in Figure 3. When the map parameter was varied, the diagram showed extensive chaotic dynamics over a large region of the parameter space. This indicates that the system undergoes significant ergodic fluctuations across a broad range of conditions, suggestive of notable unpredictability and sensitive dependence on initial conditions - hallmarks of strong chaos according to nonlinear dynamics theory. Experimental results showed that the JSMP map passes stringent randomness tests, achieves high encryption entropy values, and produces cipher images with uniform histograms and low pixel correlations, confirming its suitability for cryptographic applications demanding strong secret keys. In summary, the JSMP map addresses limitations of existing one-dimensional chaotic maps through its demonstrated extensive chaotic properties and behavioral richness [22].

B. Fisher Yates Scrambler

The Fisher-Yates scrambler, also known as the Knuth shuffle, is a widely recognized algorithm used for randomizing the order of elements in a collection. Named after Ronald Fisher and Frank Yates, this algorithm provides an efficient and unbiased method of shuffling elements [23]. Its scrambler follows a simple yet powerful approach. It begins by iterating through the collection from the last element to the first, swapping each element with a randomly selected element from the remaining unshuffled portion. This process ensures that each element has an equal chance of occupying any position in the final shuffled sequence. By utilizing this algorithm, developers and statisticians can achieve truly random permutations, making it particularly valuable in applications such as simulations, cryptography, and statistical analysis. Its scrambler's elegance, reliability, and time complexity make it a go-to choice for generating random permutations and ensuring the desired level of randomness in various domains.

The Fisher-Yates shuffle is a proven technique for randomly permuting all elements within a finite list or array. Unlike simpler scrambling methods like row-column swapping, the Fisher-Yates algorithm provides maximally random, equiprobable permutations without any bias [24].

We opted to make use of the Fisher-Yates scrambling algorithm for reordering the pixels in the encrypted images. By adopting pseudorandom numbers generated from JSMP map rather than true random numbers, the scrambling process can be made fully reversible for decryption. This preserves the integrity of the encryption scheme while still achieving excellent randomness. By scrambling on the scale of individual pixels, the Fisher-Yates algorithm ensures any statistical patterns in the plaintext are completely dispersed after encryption. Figure 4 shows a detailed graphical explanation for a simplified Fisher-Yates scrambler based on pseudorandom numbers.

C. Non-uniform Cellular Automata

Cellular automata are discrete dynamical systems that have been widely studied and applied in cryptography due to their simple structure and ability to generate pseudo-random sequences. The change mechanism for 1D cellular automata is defined as [16]

$$x_i^{t+1} = f(x_{i-1}^t, x_i^t, x_{i+1}^t) \quad (2)$$

Where x_i^t represents the state of i^{th} cell at time t, x_i^{t+1} is the state of i^{th} cell at time t+1, and x_{i-1}^t, x_{i+1}^t are the neighbors of x_i^t . This is graphically represented in Figure 5.a.

Cellular automata that have cells restricted to only two feasible states (one or zero), and cells that communicate with two neighboring cells, are referred to as Elementary Cellular Automata (ECA) [21]. This is the most basic approach to CA, there are $2^8 = 256$ rule, and these rules are indexed by an integer number $\left[0, 256\right]$. Figure 5.b shows the boundary condition for selection of first and last cell's neighbors. Figure 5.c describes rule 150, rule 90, and rule 30, respectively, demonstrating the basic operation for cellular automata technique.

Traditional uniform CA has limitations such as a limited number of available rules and inability to generate long random sequences [17]. To address these limitations, we employ a non-uniform one-dimensional CA where each cell can follow different rules.

This increases the complexity and diversity of possible configurations compared to uniform CA. Specifically, we use eight CA rules that have been shown to pass randomness tests. There Boolean function is shown Table 1. The initial values of the CA cells are determined using the JSMP map, as chaotic function. This introduces randomness and sensitivity to initial conditions.

Crucially, the selection of the rule applied to each cell is also randomized using the JSMP map. This provides two layers of randomness - in both the initial cell values and the rules themselves. It ensures the generation of highly disordered and unpredictable sequences compared to a uniform CA with fixed rules. These chaotic properties strengthen the security of the generated key.

The non-uniform CA is implemented with periodic boundary conditions as shown in Figure 5.b, meaning the first and last cells are neighbors. This effectively wraps the CA into a ring structure [20]. The states of the CA cells are then sequentially updated according to the randomly assigned rules and neighboring cell values. The final output forms a binary key string that is converted into decimal values and used for image encryption.

The use of a non-uniform CA with randomized initial configurations and rules introduces complexity and disorder that would be difficult to analyze and predict. This enhances the security and robustness of the generated key compared to more regular uniform CA structures. It is an important component of the proposed encryption scheme that helps strengthen its cryptographic strength.

The proposed method first applies JSMP map 200 times to avoid transient effects from initial conditions. A cellular automata (CA) rule is then selected from Table 1 using the following equation

$$R_i = \lfloor y_i \times 7 \rfloor + 1 \qquad (3)$$

It based on the current JSMP map output y_i using Equation 1. This assigns one of the elementary CA rules listed in Table 1. The selected rule R_i is then applied to the first cell of the one-dimensional CA based on its state and that of its two neighbors.

This process iterates through each of the CA cells to compute the updated state. The binary values are then converted to decimal and stored as the encryption key. The previous CA state becomes the current state, and the process continues iteratively until a full key image is created.

To demonstrate the method, Figure 6 shows an example for key image generation assuming $y_0 = 0.55$, and β=10 as JSMP map parameters .This hybrid CA-JSMP map technique produces cryptographically strong pseudorandom numbers for use as encryption keys through a multi-step iterative process coupling a chaotic map with elementary cellular automata rules.

D. DNA

The proposed medical image cryptosystem utilizes DNA encoding rules to further enhance the security of encrypting medical images. DNA encoding takes advantage of the properties of deoxyribonucleic acid (DNA) and its nucleotide bases to perform encryption [14]. It is made up of four nucleotide bases namely adenine (A), thymine (T), cytosine (C) and guanine (G). These four bases form the building blocks of DNA and carry the genetic instructions of living organisms. An important property of these bases is their base pairing behavior following the Watson–Crick complement rule. Specifically, "A" and "T" are complementary base pairs that bond together, as well as "C" and "G". Since digital information in computers is represented using the binary digits "0" and "1", a mapping is required to encode the DNA bases for use in encryption/decryption algorithms. There are 24 possible ways to represent each DNA base using a 2-bit binary codon. However, only eight of these codons satisfy the Watson–Crick complement rule between the coded bases [15].

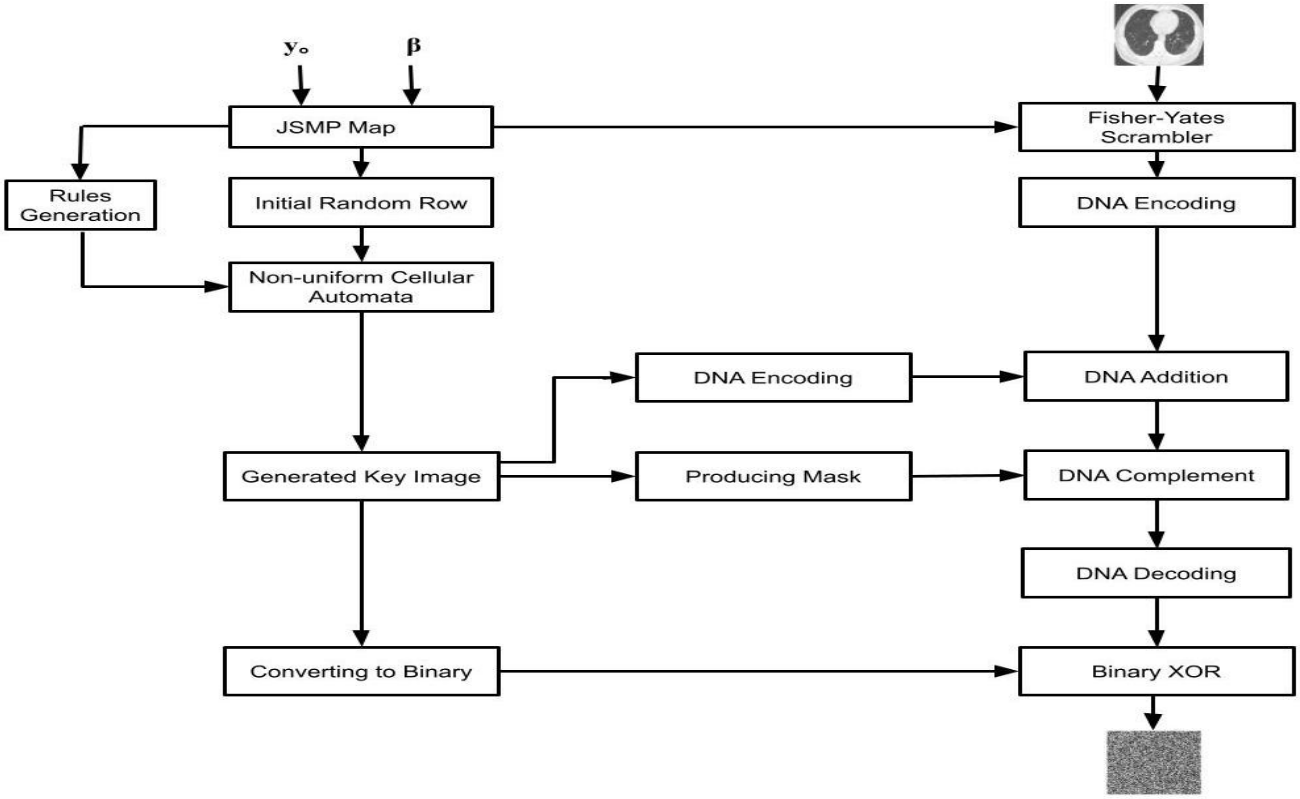


Fig. 1. Proposed DICOM medical image ciphering scheme.

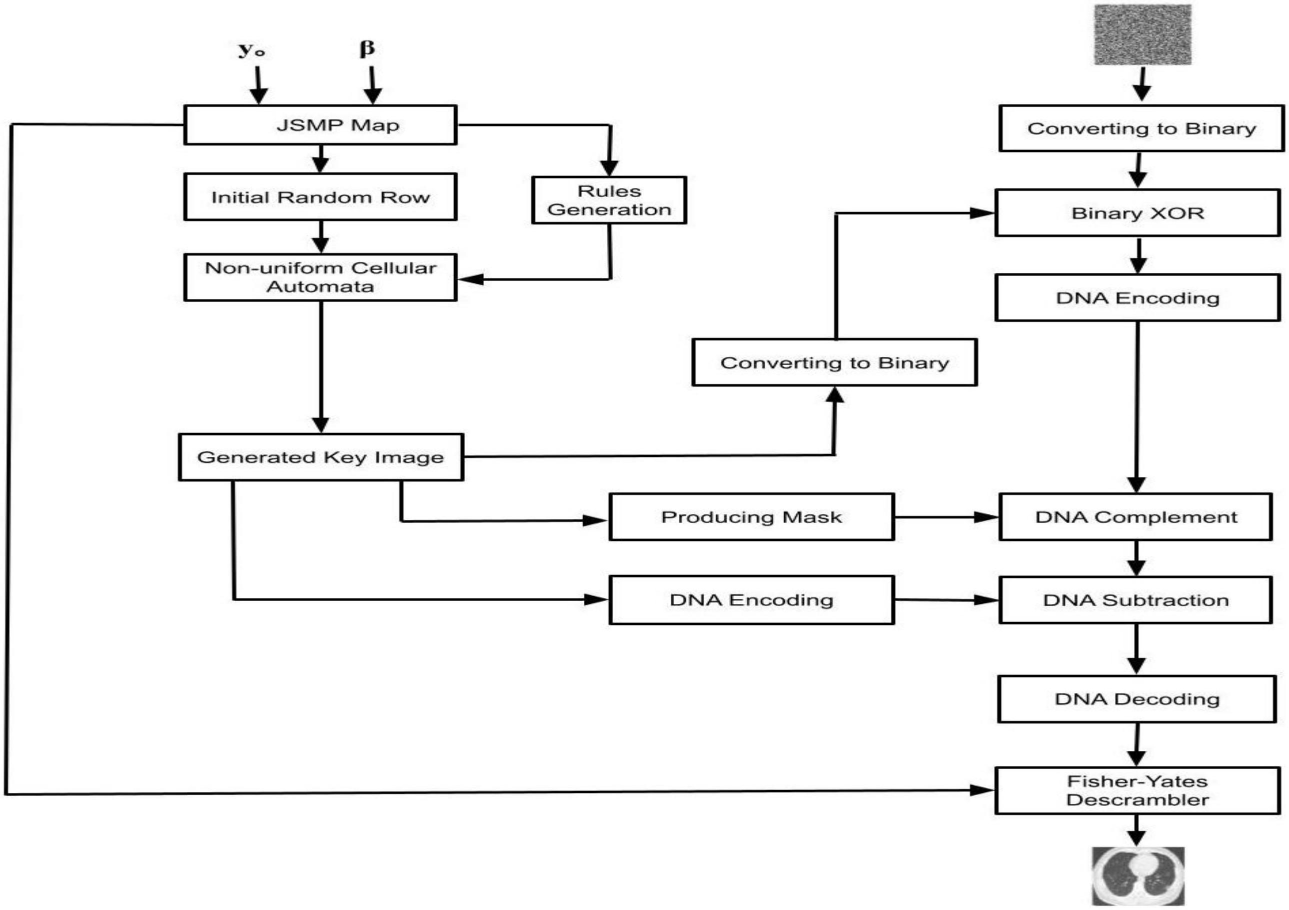


Fig. 2. Proposed DICOM medical image deciphering scheme.

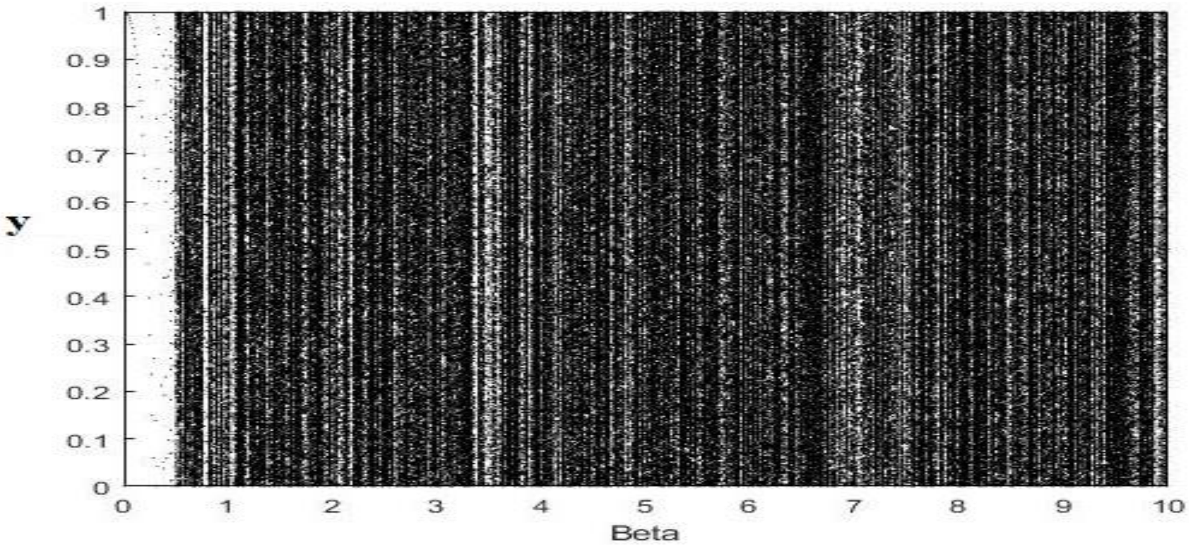
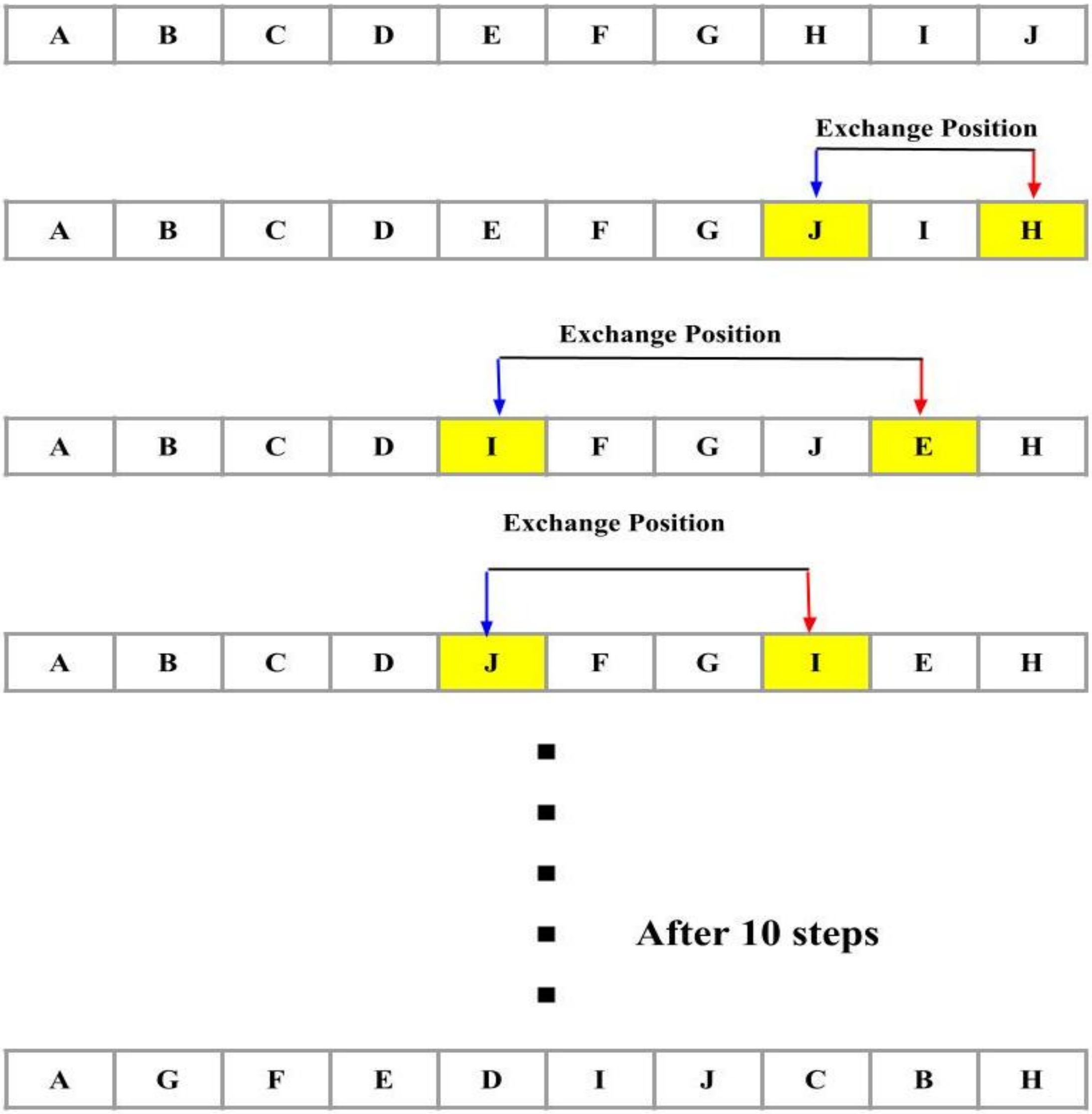


Fig. 3. Bifurcation diagram of the JSMP map.



A B C D E F G H I J

A B C D E F G J I H

A B C D I F G J E H

A B C D J F G I E H

A G F E D I J C B H

Fig. 4. Fisher-yates algorithm steps.

It is crucial for the encryption scheme that the mapping preserves the complementary relationships between bases. Otherwise, the encrypted data would not properly decrypt. These eight valid DNA coding rules are especially useful for cryptographic applications based on DNA's properties and are listed in Table 2 for reference. Adopting one of these rules ensures accurate encoding and decoding of information using the genetic language of DNA.

In fact, DNA algebraic operations like DNA addition and DNA subtraction rules are shown in Tables 3 and 4, respectively. Its addition involves combining two DNA code words base-by-base using modulo-2 addition. For example, to perform the addition of DNA code words 'AATC' and 'GCTA', we add their corresponding nucleotide bases using binary addition modulo-2. So 'A' + 'G' = 'C', 'A' + 'C' = 'T', 'T' + 'T' = 'G', and 'C' + 'A' = 'T', which gives the sum as 'CTGT'. Its subtraction is carried out in a similar manner by treating the DNA bases as binary numbers and performing regular binary subtraction. For 'AATC' - 'GCTA', we get 'A' - 'G' = 'T', 'A' - 'C' = 'A', 'T' - 'T' = 'A', and 'C' - 'A' = 'G', giving the difference as 'TAGG'. This method of encoding digital data as DNA code words allows for flexible binary arithmetic operations to be performed at the molecular level. DNA computing harnesses massively parallel biochemical processes and has potential applications in encryption, DNA-based data storage, and molecular computation. The ability to perform addition and subtraction on DNA code words forms the basis for more advanced DNA logic gates and algorithms.

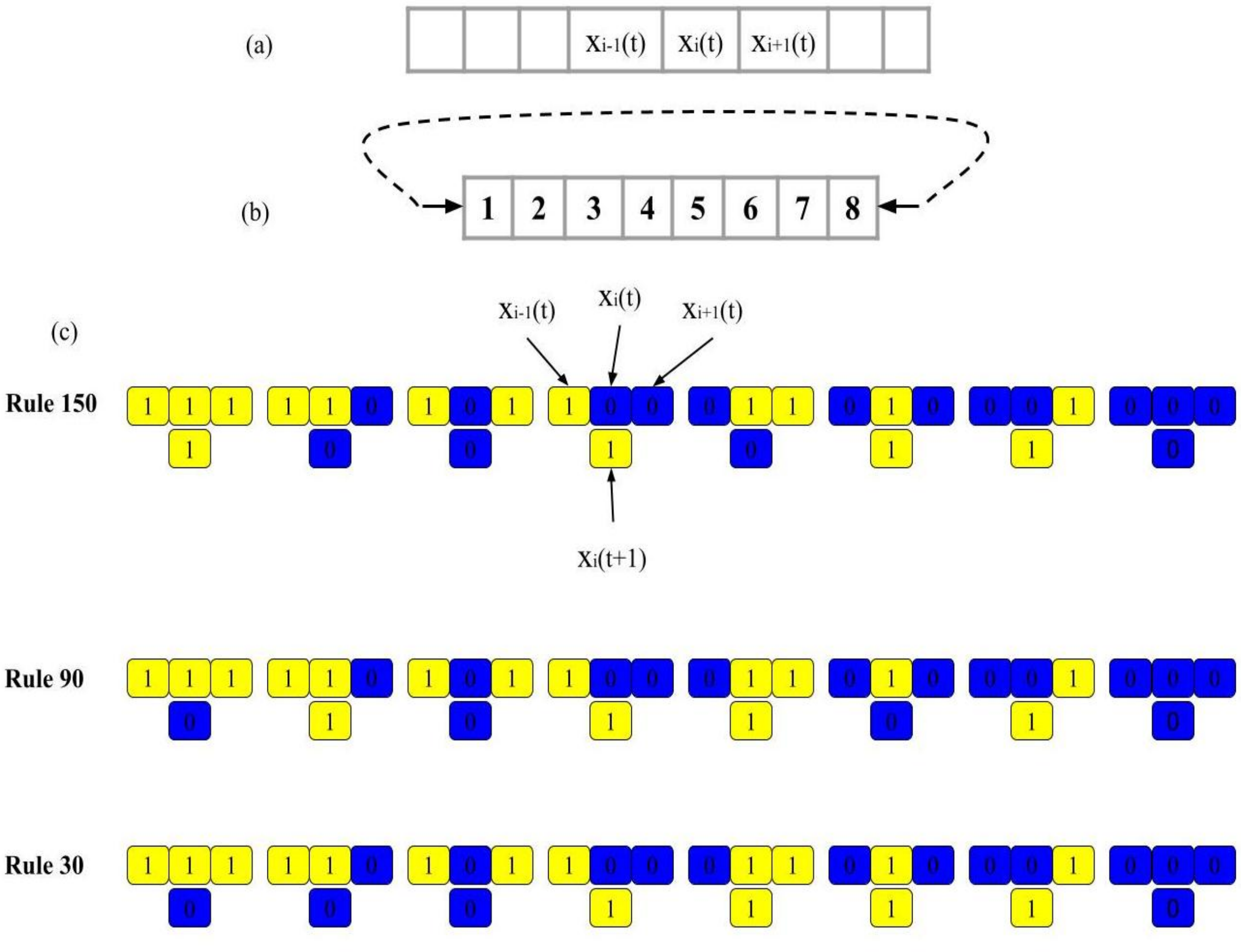


Fig. 5. (a) Three cells representation for cellular automata. (b) Boundary condition for selection of first and last cell’s neighbors. (c) Examples for cellular automata Rule 150, Rule 90, and Rule 30.

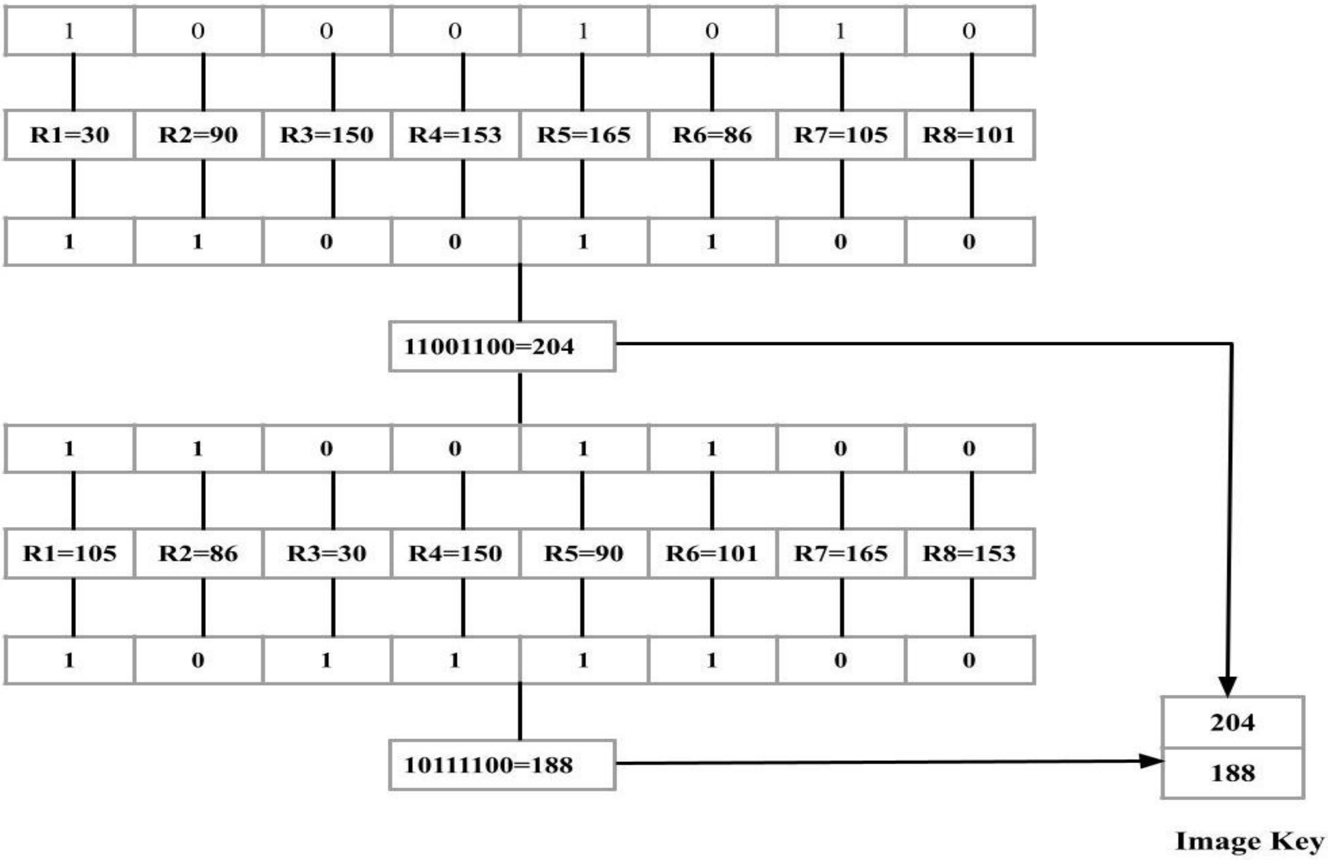

1 0 0 0 1 0 1 0
R1=30 R2=90 R3=150 R4=153 R5=165 R6=86 R7=105 R8=101
1 1 0 0 1 1 0 0
11001100=204
1 1 0 0 1 1 0 0
R1=105 R2=86 R3=30 R4=150 R5=90 R6=101 R7=165 R8=153
1 0 1 1 1 1 0 0
10111100=188
204
188
Image Key

Fig. 6. Key image generation example using JSMP map and non-uniform cellular automata.

Table 1. The Boolean representation of selected cellular automaton rules.

Rule index	Rule Number	Function
1	30	$x_i^{t+1} = x_{i-1}^t \text{ XOR } [x_i^t \text{ OR } x_{i+1}^t]$
2	90	$x_i^{t+1} = x_{i-1}^t \text{ XOR } x_{i+1}^t$
3	150	$x_i^{t+1} = x_{i-1}^t \text{ XOR } x_i^t \text{ XOR } x_{i+1}^t$
4	153	$x_i^{t+1} = x_i^t \text{ XNOR } x_{i+1}^t$
5	165	$x_i^{t+1} = x_{i-1}^t \text{ XNOR } x_{i+1}^t$
6	86	$x_i^{t+1} = [x_{i-1}^t \text{ NOR } x_i^t] \text{ XOR } [\text{NOT } (x_i^t)]$
7	105	$x_i^{t+1} = NOT[x_{i-1}^t \text{ XOR } x_i^t \text{ XOR } x_{i+1}^t]$
8	101	$x_i^{t+1} = [x_{i-1}^t \text{ NOR } x_{i+1}^t] \text{ OR}[\ (x_i^t \text{ XOR } x_{i+1}^t) \text{ AND } x_{i-1}^t]$

Table 2. Eight DNA Rules mapping.

DNA Rule **Bit Pattern**	**#1**	**#2**	**#3**	**#4**	**#5**	**#6**	**#7**	**#8**
00	A	A	C	C	G	G	T	T
01	C	G	A	T	A	T	C	G
10	G	C	T	A	T	A	G	C
11	T	T	G	G	C	C	A	A

Table 3. The DNA-based addition function in algebraic terms.

+	**A**	**C**	**T**	**G**
A	C	A	G	T
C	G	T	C	A
T	A	C	T	G
G	T	G	A	C

Table 4. The DNA-based subtraction function in algebraic terms.

-	**A**	**C**	**T**	**G**
A	C	G	A	T
C	G	T	C	A
T	A	C	T	G
G	T	A	G	C

III. Simulation Results

In the experiments, grayscale medical images with dimensions of 256 by 256 pixels and a bit depth of 8 bits per pixel was used to evaluate the results. A key advantage of the proposed encryption system is that it can process grayscale and color images of different sizes and properties. Whether the images are grayscale or color, small or large in resolution, the cryptosystem can encrypt them securely. This makes the system applicable for securing medical images during transmission and storage. The implementation is done using Intel(R) Core(TM) i3-5005U CPU @ 2.00GHz 2.00 GHz, Windows ten operating system, and 12.0 GB RAM with MATLAB 2019b.

A. Visual subjective analysis

Subjective visual analysis is an effective way to evaluate the quality of encryption. The distinct features of a medical image should be indistinguishable after encryption. Figure 7 presents the visual security results from encrypting different types of medical images. By examining the data, it is clear that all identifiable details within the original grayscale and color medical images are completely hidden, encrypted, and unrecognizable. This demonstrates the efficacy of the proposed cryptographic system [25].

Additionally, the decryption capability of the developed encryption method is notable. The encrypted medical images are accurately reconstructed back to their original form during decryption. Moreover, this shows that encrypted medical data can be securely transmitted and later decrypted correctly by authorized users. The distinct attributes that are essential for medical analysis and diagnosis are perfectly restored from the encrypted files. Therefore, the system thus achieves the goal of protecting confidential medical images during transmission while still allowing accurate analysis after decryption by appropriate parties.

B. Entropy analysis

It is important to perform entropy analysis as part of the security evaluation of the developed encryption algorithm. Entropy analysis provides a means to quantify and compare the level of randomness or information content in the encrypted images versus the original unencrypted images. By calculating the entropy of encrypted images, we can measure how well the encryption process concealed the underlying plaintext information and introduced uncertainty. A high entropy value for encrypted images implies that an attacker would obtain little useful knowledge from analyzing the encrypted content. This entropy evaluation thus serves as a gauge of how resistant the algorithm would be against attacks that exploit weaknesses in entropy or attempt to identify patterns in the encrypted data based on information theory assessments. Entropy analysis therefore forms a key part of rigorously verifying the security properties of the cryptographic scheme. Entropy of any image Z is calculated as [14]

$$H(Z) = -\sum_{i=1}^{n} p(z_i)\log_2 p(z_i) \tag{4}$$

Where z_i is the *ith* possible value in Z, and $p(z_i)$ is statistical probability of z_i in Z, the number of symbols is denoted as n. Table 5 displays the entropy results calculated for the original, encrypted, and decrypted images.

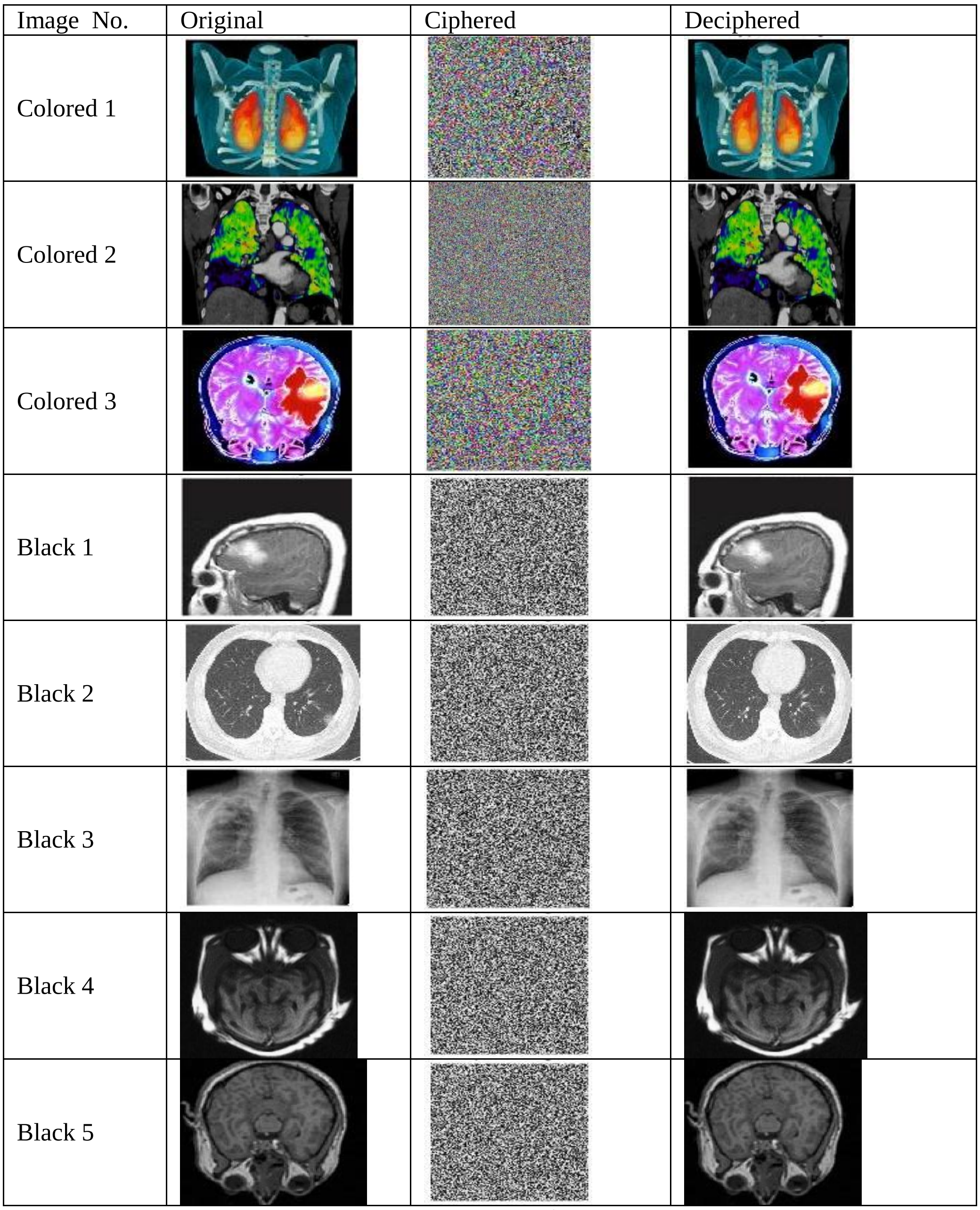


Fig 7. Visual security outcomes for color and gray medical images.

Table 5. Information entropy of original, encrypted, and decrypted images.

Image No.	Original Image	Encrypted Image	Decrypted Image
Colored 1	6.8234	7.9908	6.8234
Colored 2	6.8533	7.9985	6.8533
Colored 3	6.2595	7.9991	6.2595
Black 1	6.5097	7.9989	6.5097
Black 2	6.8689	7.9878	6.9689
Black 3	7.5967	7.9669	7.5967
Black 4	6.6231	7.9988	6.6231
Black 5	6.3724	7.9789	6.3724

For an 8-bit grayscale image with $2^8 = 256$ possible pixel values, the entropy would be ideally equal to 8 bits. As shown, the entropy values of the encrypted images are very close to 8 bits. This indicates that the proposed encryption algorithm successfully introduced a high level of randomness and uncertainty into the encrypted images, similar to random data. The entropy analyses confirm that the encrypted images have nearly uniform pixel value distributions. Therefore, an attacker would find it extremely difficult to extract useful information from these encrypted images using entropy-based analysis approaches. The closeness of the encrypted image entropies to the ideal value of 8 demonstrates that the proposed encryption technique provides strong security against entropy attacks aimed at identifying patterns in or determining information about the encrypted content.

C. Differential attack analysis

It is crucial for the encryption algorithm to produce highly differing encrypted outputs even if there is only a small difference between the original input images. This ensures that the algorithm is robust against differential cryptanalysis attacks. To evaluate the resilience of the proposed cryptosystem, two standard metrics - Unified Average Changing Intensity (UACI) and Number of Pixel Change Rate (NPCR) - are used to measure the effects of tiny changes in plain images on the corresponding encrypted images. A minor modification to the plaintext should lead to significant variations in the ciphertext. Calculating UACI and NPCR values quantifies the differential behavior of the encryption scheme. This analysis determines if the algorithm sufficiently obscures relationships between plaintext and ciphertext, thereby strengthening its security against differential attacks attempting to reveal vulnerabilities based on analyzing relationships between encrypted and original images. The following equation describes how to calculate both quantities [26]

$$NPCR = \frac{\sum_{m,n} F(m,n)}{M \times N} \times 100 \qquad (5)$$

$$UACI = \frac{1}{M \times N}\left(\sum_{m,n} \frac{\left|E_1(m,n) - E_2(m,n)\right|}{255}\right) \times 100 \qquad (6)$$

$$F(m,n) = \begin{cases} 0 & E_1(m,n)=E_2(m,n) \\ 1 & otherwise \end{cases} \qquad (7)$$

Where $E_1(m,n)$ is the encrypted version of the original image, $E_2(m,n)$ is the encrypted version of the modified plain image. Theoretical maximum values for NPCR and UACI metrics are 99.6% and 33.35%, respectively. Table 6 presents the calculated NPCR and UACI results for the proposed cryptosystem. The obtained values are very close to the theoretical optimum levels, confirming that even minor differences in plaintext images produces entirely different ciphertexts. This indicates that the algorithm achieves strong diffusion properties that make it highly sensitive to changes in the input. Based on the NPCR and UACI outcomes, it is clear that the cryptosystem demonstrates robustness against differential cryptanalysis by thoroughly masking relationships between encrypted and original versions of medical images. The metrics validate that the encryption scheme can withstand differential attacks attempting to compromise security by leveraging correlations between encrypted and original data.

D. Quantitative quality analysis

To accurately evaluate the security performance and quality of encryption and decryption provided by the proposed algorithm, quantitative image similarity metrics were computed and analyzed. Specifically, structural similarity index measure (SSIM), feature similarity index measure (FSIM), and peak signal-to-noise ratio (PSNR) metrics were computed to compare the encrypted/decrypted medical images with their corresponding original images. These similarity measures are commonly used in the literature to objectively assess the preservation of structural information and similarity to the original in encrypted images [27]. Table 7 presents the determined similarity index and PSNR values obtained through this analysis. Analyzing these quantitative results serves to effectively validate the encryption and decryption capabilities as well as security robustness afforded by the suggested cryptographic technique.

These outcomes show that the similarity index and PSNR values between the encrypted images and original images are extremely low. This confirms the encryption process successfully concealed all details and structural information from the original images. In contrast, the SSIM, FSIM and PSNR metric values computed by comparing the decrypted images to the original images were found to be very high.This validates the decryption capability of the algorithm in accurately recovering the pixel details and content of the original images from the encrypted images. Therefore, these quantitative measures demonstrate the effectiveness of both encryption and decryption performance of the proposed security algorithm. The encryption process adequately conceals data while the decryption process reliably retrieves the original details. Overall, the cryptosystem robustly performs its encryption and decryption functions as intended based on the similarity analysis results.

E. Correlation analysis

The correlation between neighboring pixels in the original versus encrypted images can be leveraged to evaluate the cryptosystem's strength. Both quantitative and visual correlation coefficients were determined for the color and grayscale medical images tested. Specifically, horizontal, vertical, and diagonal correlation values were computed using the provided equations. [28]

$$\begin{aligned} r_{p.c} &= \frac{cov(p,c)}{\sqrt{D(p)}\sqrt{D(c)}} \\ cov(p,c) &= E\left\{(p - E(p))(c - E(c))\right\} \\ E(p) &= \frac{1}{N}\sum_{i=1}^{N} p_i \\ D(p) &= \frac{1}{N}\sum_{i=1}^{N}(p_i - E(p))^2 \end{aligned} \qquad (8)$$

Where plain image is denoted as p, cipher image is denoted as c, and N represents the number of pixels.

Visual inspection for correlation coefficients are shown in Figure 8, it confirms that the proposed encryption algorithm successfully disrupts the pixel relationships present in the original images, indicating its robust diffusion capabilities and resistance to correlation-based attacks. Analyzing pixel correlations is meaningful because a strong encryption method should produce ciphertext in which adjacent pixels are essentially randomly distributed with little to no correlation, unlike the structural dependencies typically found between pixels in raw images [29].

The data in Table 8 indicates that the encrypted images exhibited exceptionally low correlation values between neighboring pixels when assessed in different orientations. This is an essential property for a robust encryption method. Additionally, the decrypted images demonstrate nearly perfect correlation (around 1) with their original counterparts in all pixel orientations. This confirms the algorithm's ability to accurately reconstruct the images from their encrypted form.

F. Histogram analysis

Histograms can provide a thorough evaluation of the statistical security of the proposed encryption algorithm. This analysis examines the algorithm's effectiveness in obscuring and rearranging information and its resilience against statistical attacks. Figure 9 shows the histogram results for the encrypted color and grayscale medical images. The histograms of the encrypted images are observed to be consistently flat, uniform, and noticeably different from the original plain images. This highlights the strength of the suggested security method. As a result, the encrypted images do not reveal any useful data vulnerable to statistical security analysis exploitation. Additionally, the histograms of the original and decrypted medical images are found to be almost identical, demonstrating the algorithm's excellent ability to reconstruct the images [30].

Table 6. NPCR and UACI findings for color and gray images.

Image No.	NPCR	UACI
Colored 1	0.99542	0.35751
Colored 2	0.99960	0.35460
Colored 3	0.99543	0.35281
Black 1	0.99715	0.34963
Black 2	0.99507	0.34446
Black 3	0.99689	0.33795
Black 4	0.99721	0.3265
Black 5	0.99576	0.3388

Table 7. PSNRs, SSIMs, and FSIMs for Color and gray medical images.

Image No.	Plain-Ciphered			Plain-Deciphered		
	Peak Signal-to-Noise Ratio	Structural Similarity	Feature Similarity	Peak Signal-to-Noise Ratio	Structural Similarity	Feature Similarity
Colored 1	6.4012	0.0066	0.3011	∞	1	1
Colored 2	5.2884	0.0065	0.2662	∞	1	1
Colored 3	5.0071	0.0024	0.1386	∞	1	1
Black 1	7.5184	0.0058	0.1795	∞	1	1
Black 2	5.9543	0.0049	0.4594	∞	1	1
Black 3	5.1007	0.0059	0.3713	∞	1	1
Black 4	6.9890	0.0027	0.2391	∞	1	1
Black 5	7.2785	0.0076	0.4281	∞	1	1

Table 8. Correlation coefficient calculated for medical images in both color and grayscale.

Image	Plain Image			Ciphered Image			Deciphered Image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Colored 1	0.9771	0.9861	0.9655	0.0040	-0.0001	0.0045	0.9771	0.9861	0.9655
Colored 2	0.8867	0.9772	0.8802	0.0059	0.0060	-0.0030	0.8867	0.9772	0.8802
Colored 3	0.9391	0.9473	0.8973	0.0010	-0.0001	0.0008	0.9391	0.9473	0.8973
Black 1	0.9700	0.9776	0.9565	0.0015	0.0019	-0.0009	0.9700	0.9776	0.9565
Black 2	0.9547	0.9665	0.9438	0.0013	0.0037	0.0005	0.9547	0.9665	0.9438
Black 3	0.9918	0.9843	0.9873	-0.0008	-0.0089	-0.0019	0.9918	0.9843	0.9873
Black 4	0.9809	0.9869	0.9686	-0.0090	-0.0006	0.0023	0.9809	0.9869	0.9686
Black 5	0.9626	0.9758	0.9416	0.0033	0.0003	-0.0016	0.9626	0.9758	0.9416

IV. Comparative Analysis

The findings from the comparative analysis are shown in Table 9. These results indicate that the proposed algorithm for securing medical data transmission in the Internet of Medical Things (IoMT) performs better than other recently developed encryption methods according to the security metrics evaluation. The analysis shows that the suggested algorithm outperforms related encryption techniques in securing medical images, whether color or grayscale. In other words, the proposed encryption method exhibits superior results on security testing compared to related encryption approaches that have been developed recently, demonstrating its effectiveness in protecting medical images for applications involving the Internet of Medical Things.

V. Conclusions

The proposed cryptosystem is well-suited for deployment in cloud computing environments and as part of the growing Internet of Medical Things (IoMT) domain. Specifically, the advanced security mechanisms employed by the encryption scheme make it particularly applicable for protecting sensitive medical data shared over cloud platforms and networks of interconnected medical devices, sensors and technologies that constitute the IoMT. The strong protection of patient information mandated for cloud services and evolving healthcare IoT ecosystems can be reliably enabled through the adoption of this robust and efficient encryption system. Overall, the approach offers a viable technological solution for the stringent security and privacy challenges of medical data transmission involved in modern cloud-based healthcare services and the proliferating realm of IoMT connectivity.

Table 9. Comparative analysis between proposed and other related work.

Algorithm	CPU time (s)	Entropy	NPCR	UACI	Correlation	PSNR (dB)	SSIM	FSIM
Proposed	1.721	7.9989	99.60	33.10	-0.0009	5.8910	0.0021	0.2067
Related work 1 [21]	1.69	7.9986	99.67	33.79	-0.0015	6.0151	0.0037	0.2773
Related work 2 [29]	1.735	7.9989	99.63	33.55	0.03097	9.33	0.0026	0.4105
Related work 3 [31]	3.5267	7.9372	99.55	34.08	0.09867	11.35	0.0967	0.4883
Related work 4 [32]	2.0893	7.9867	96.18	34.07	0.08672	10.08	0.012	0.4863
Related work 5 [33]	2.3675	7.9563	99.73	33.87	0.11308	10.14	0.1053	0.4485
Related work 6 [34]	2.8647	7.7362	99.17	32.93	0.11084	12.81	0.0834	0.4936

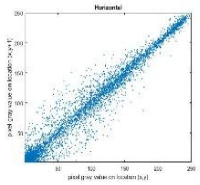
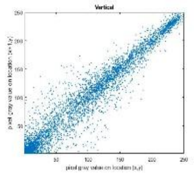
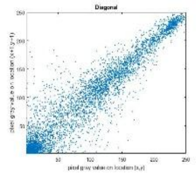
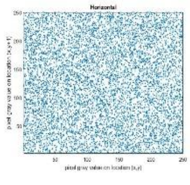
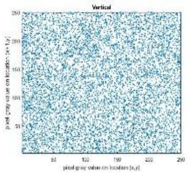
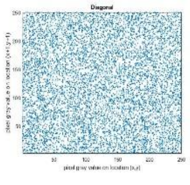
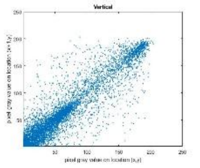
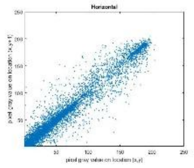
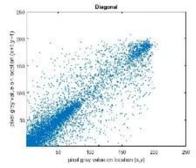
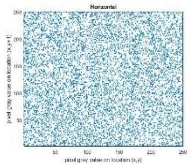
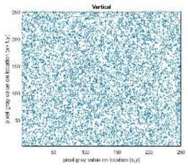
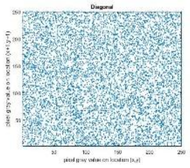
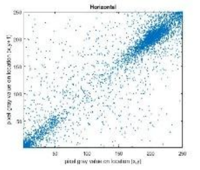
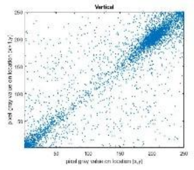
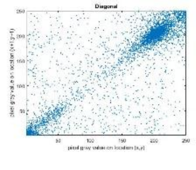
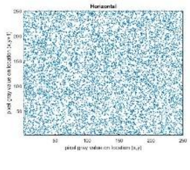
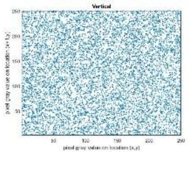
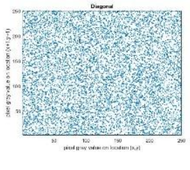
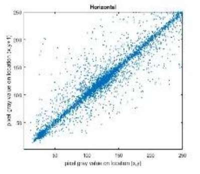
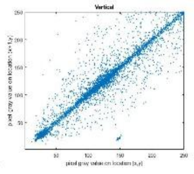
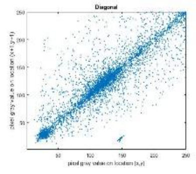
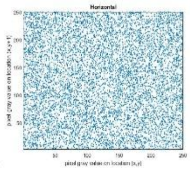
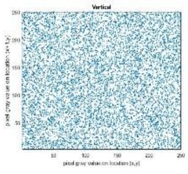
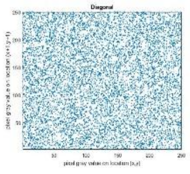
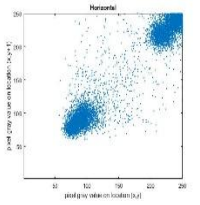
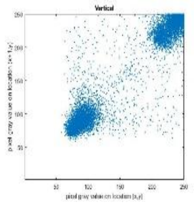
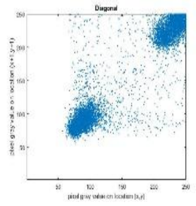
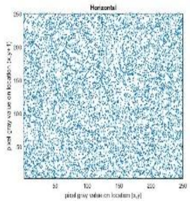
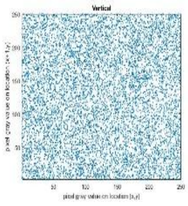
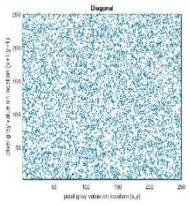
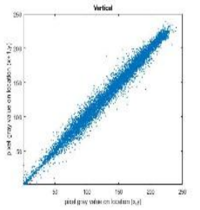
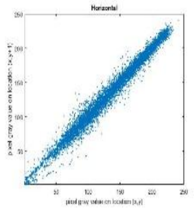
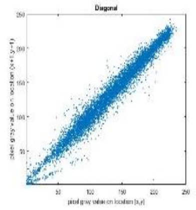
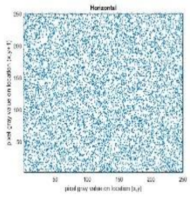
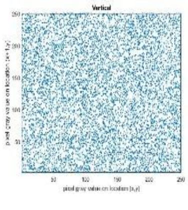
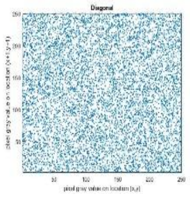
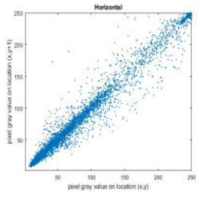
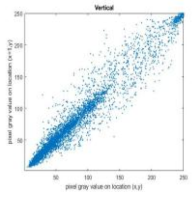
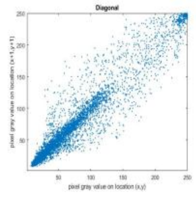
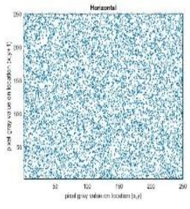
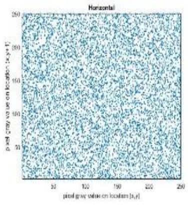
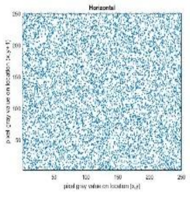
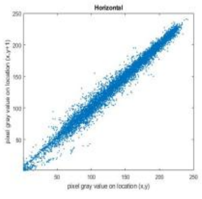
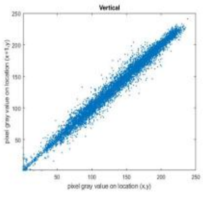
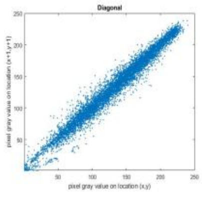
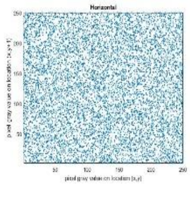
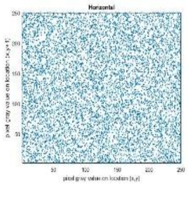
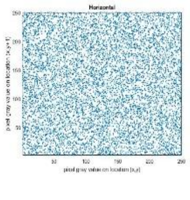
Image	Original Image			Encrypted Image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Colored **1**						
Colored **2**						
Colored **3**						
Black **1**						
Black **2**						
Black **3**						
Black **4**						
Black **5**						

Fig. 8. Visual correlation coefficients for color and gray medical images.

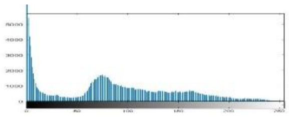
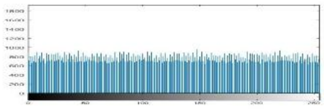
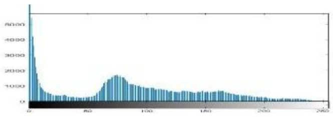
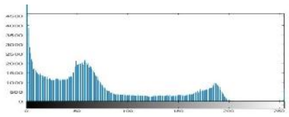
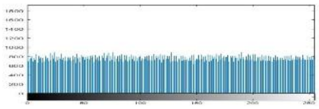
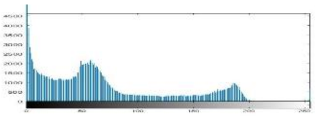
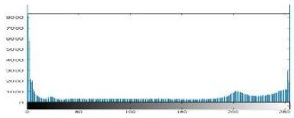
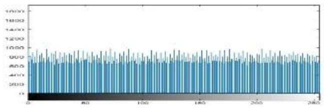
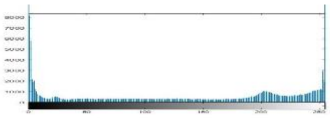
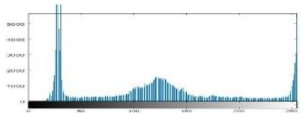
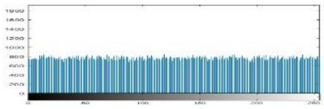
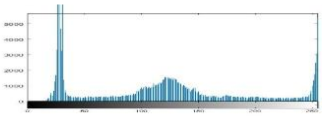
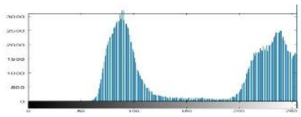
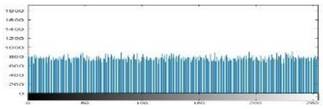
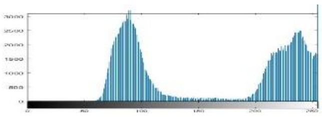
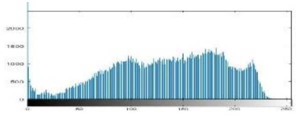
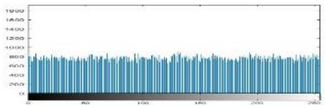
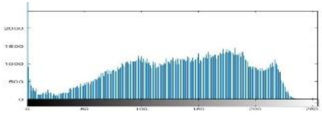
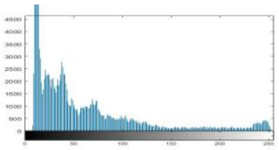
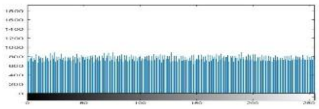
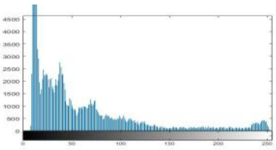
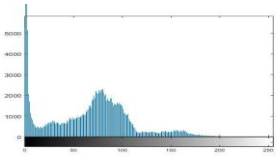
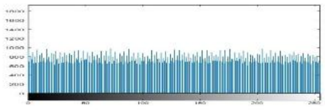
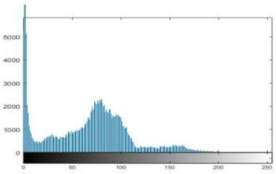
Image	Plain Image	Ciphered Image	Deciphered Image
Colored 1			
Colored 2			
Colored 3			
Black 1			
Black 2			
Black 3			
Black 4			
Black 5			

Fig. 9. Histogram analysis for medical images in both color and grayscale.

References

[1] R. Dwivedi, D. Mehrotra, and S. Chandra, “ Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review.” Journal of oral biology and craniofacial research, vol. 12, no. 2, pp.302-318, March 2022.

[2] S.T. Kamal, K.M. Hosny, T.M. Elgindy, M.M. Darwish, and M.M. Fouda, “A new image encryption algorithm for grey and color medical images.” IEEE Access, vol. 9, pp.37855-37865, March 2021.

[3] S. Shivani, S. Agarwal, and J. S. Suri, “Handbook of image-based security techniques,” 1 st ed,Chapman and Hall/CRC, May 2018.

[4] S. Mortajez, M. Tahmasbi, J. Zarei, and A. Jamshidnezhad, “A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images.” Informatics in Medicine Unlocked, vol. 20, p.100396, January 2020.

[5] D. Ravichandran, P. Praveenkumar, J.B.B. Rayappan, and R. Amirtharajan, “Chaos based crossover and mutation for securing DICOM image.” Computers in biology and medicine, vol. 72, pp.170-184, May 2016.

[6] M. Magdy, K. M. HosnY, N. I. Ghali,and S. Ghoniemy. “Security of medical images for telemedicine: a systematic review.” Multimedia Tools and Applications, vol. 81, no.18, pp.25101-2514, July 2022.

[7] K. J. Giri, S. A. Parah, R. Bashir, and K. Muhammad, “Multimedia security: algorithm development, analysis and applications,” Singapore: Springer, 2021.

[8] K. M. Hosny. “Multimedia security using chaotic maps: principles and methodologies,” New York: Springer ,vol. 884, 2020.

[9] V. Pavithra, and C. Jeyamala, “A survey on the techniques of medical image encryption.” In 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) , pp. 1-8, December 2018.

[10] L. Kocarev, and L. Shiguo, “Chaos-based cryptography: theory, algorithms and applications,” Springer Science & Business Media ,Vol. 354, 2011.

[11] A. Naguib, W. El-Shafai, M. Shokair, “Performance evaluation of an encrypted color image transmission over wireless network with different chaotic-based techniques”, Journal of Optics, pp. 1-10, January 2023

[12] R. Li, Q. Liu, and L. Liu, “Novel image encryption algorithm based on improved logistic map.” IET Image Processing, vol. 13, no. 1, pp.125-134, January 2019.

[13] J.S. Muthu, and P. Murali. "A new chaotic map with large chaotic band for a secured image cryptosystem." *Optik* 242, pp.167300, September 2021.

[14] W. El-Shafai, F. Khallaf, E. M. El-Rabaie, and F. E. Abd El-Samie, "Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 10, pp. 9007-9035, March 2021.

[15] K. Zhan, D. Wei, J. Shi, and J. Yu, “Cross-utilizing hyperchaotic and DNA sequences for image encryption,” Journal of Electronic Imaging, vol. 26, no. 1, pp. 13-21, Febraury 2017.

[16] L. Mariot, M. Saletta, A. Leporati, L. and Manzoni, “Heuristic search of (semi-) bent functions based on cellular automata.” Natural Computing, vol. 21, no.3 , pp.377-391, September 2022.

[17] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz,” Color image encryption based on hybrid hyper-chaotic system and cellular automata.” Optics and Lasers in Engineering, vol. 90, no. 1, pp. 225-237. March 2017.

[18] T. M. Gwizdałła, L. Manzoni, G. C. Sirakoulis, S. Bandini, and K. Podlaski, “ Cellular Automata: 14th International Conference on Cellular Automata for Research and Industry”, ACRI 2020, Lodz, Poland, December 2–4, 2020, Proceedings. Springer Nature, February 2021.

[19] X. Zhang, H. Zhang, and C. Xu. “Reverse Iterative Image Encryption Scheme Using 8-layer Cellular Automata.” KSII Transactions on Internet & Information Systems, vol. 10, no. 7, July 2016.

[20] X. Zhang, S. H. Seo, and C. Wang, “A lightweight encryption method for privacy protection in surveillance videos”, *IEEE Access*, vol. *6*, pp.18074-18087, April 2018.

[21] El-Shafai, W., Naguib, A. and Shokair, M., A Novel Hyper Chaotic-Cellular Automata Based Medical Image Encryption Technique.3^{rd} ICEEM, October 2023.

[22] J.S. Muthu, and P. Murali. “A novel DICOM image encryption with JSMP map.” *Optik* 251, pp. 168416, February 2022.

[23] M.K.L Teng, X. Wang, and J. Meng, “Color image encryption scheme based on the combination of the fisher-yates scrambling algorithm and chaos theory.” Multimedia Tools and Applications, vol. 80, pp.24737-24757, July 2021.

[24] F. Musanna, and S. Kumar, “A novel fractional order chaos-based image encryption using Fisher Yates algorithm and 3-D cat map.” Multimedia Tools and Applications, vol. 78, no.15, pp.14867-14895, June 2019.

[25] X. Wang, and Y. Wang, “Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points.” *Expert Systems with Applications*, vol. *213*, pp.118924. March 2023.

[26] S. S. Moafimadani, Y. Chen, and C. Tang, "A new algorithm for medical color images encryption using chaotic systems," Entropy,vol. 21, no. 6, pp. 577-601, June 2019

[27] P. Fang, H. Liu, C. Wu, and Liu. “A survey of image encryption algorithms based on chaotic system.” The Visual Computer, vol. 39, no. 5, pp. 1975–2003, April 2023**.**

[28] I. Almomani, W. El-Shafai, A. AlKhayer, A. Alsumayt , S. Aljameel, and K. Alissa, “Proposed biometric security system based on deep learning and chaos algorithms”, Computers Materials and Continua, vol. 74, no. 2, pp.3515-3537, January 2023.

[29] W. El-Shafai, I. Almomani, A. Ara, and A. Alkhayer,” An optical-based encryption and authentication algorithm for color and grayscale medical images” Multimedia Tools and Applications, vol. 82, no. 15, pp.23735-23770, June 2023.

[30] M. Li, S. Pan, W. Meng, W. Guoyong, Z. Ji, and L. Wang, “Medical image encryption algorithm based on hyper - chaotic system and DNA coding.” Cognitive Computation and Systems, vol. 4, no. 4, pp. 378-390. December 2022.

[31] W. El-Shafai, F. Khallaf, ES. El-Rabaie, and FE. El-Samie,” Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services”. Journal of Ambient Intelligence and Humanized Computing, pp. 1-28, July 2022.

[32] W. El-Shafai, I.M. Almomani, and A. Alkhayer, “Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication.” IEEE Access, 9, pp.35004-35026, February 2021.

[33] W. El-Shafai, M. H. Aly, A. D. Algarni, FE. El-Samie, and NF. Soliman. “Secure and Robust Optical Multi-Stage Medical Image Cryptosystem.” Computers, Materials & Continua, vol. 70, no. 1. January 2022.

[34] W. El-Shafai, AK. Mesrega, HE. Ahmed, NA. El-Bahnasawy, and FE. Abd El-Samie. “An efficient multimedia compression-encryption scheme using latin squares for securing internet-of-things networks.” Journal of Information Security and Applications, vol. 64, pp. 103039, February 2022.