China Petroleum Processing and Petrochemical Technology

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 763-781

SECURED HEALTHCARE ECOSYSTEM USING DNA CRYPTOGRAPHY IN 5G NETWORK

Animesh Kairi
*Institute of Engineering & Management, Kolkata, India Email: ani.kairi@gmail.com

Tapas Bhadra
Aliah University, Kolkata, India Email: tapas.bhadra@aliah.ac.in

Arindam Roy
Institute of Engineering & Management, Kolkata, India Email: arindamroy.coe@iem.edu.in

***Corresponding Author:** Animesh Kairi
*****Institute of Engineering & Management, Kolkata, India Email: ani.kairi@gmail.com

Abstract.
This abstract explores the concept of a secured healthcare ecosystem powered by DNA cryptography within a 5G network. It addresses the integration of cutting-edge technologies, such as DNA-based encryption within the context of high-speed and low-latency capabilities of 5G connectivity, offering a promising solution for safeguarding sensitive healthcare information. The focus of this study is on the secure transmission of digital medical images across open-source networks, which often contain private and confidential patient information. Ensuring the security and confidentiality of medical images is a paramount concern, especially in remote healthcare settings where these images are utilized for diagnoses. To address this concern, this research introduces a robust security approach for digital medical images, employing DNA cryptography and dual hyperchaotic maps. Given the substantial size of digital medical images, which can lead to extended computing times, we propose a targeted digital medical image encryption scheme designed to streamline the encryption process. This scheme involves the careful selection of digital medical photos, followed by randomization and diffusion operations within our proposed cryptosystem. To further enhance security, we employ DNA encoding and decoding algorithms based on the spatial position of pixels within the digital healthcare image. This spatial information is harnessed to create a unique DNA structure for each medical photograph. Subsequently, the cipher image is generated through a comprehensive DNA decryption process based on the values of individual pixels within the e-healthcare image. One notable challenge in securing digital medical images is their substantial size, which can result in prolonged computing times. To mitigate this, we present a targeted encryption scheme that streamlines the encryption process. Selected digital medical images undergo randomization and diffusion operations within our proposed cryptosystem. To bolster security further, we implement DNA encoding and decoding algorithms based on the pixel positions within the digital healthcare image. This spatial information is leveraged to construct a distinctive DNA structure for each medical photograph. Subsequently, the cipher image is generated through a comprehensive DNA decryption process that considers the values of individual pixels within the e-healthcare image. The cryptographic approach proposed in this research is designed to withstand various types of attacks, ensuring the integrity and confidentiality of medical data within an interconnected and data-centric healthcare landscape.

Keywords: DNA Computing, 5G, DNA Cryptography, Digital Healthcare image Cryptography, Hyper-chaos map

1. INTRODUCTION

In the realm of modern healthcare, the importance of medical imaging cannot be emphasized enough. Diagnoses, treatments, and groundbreaking research all depend heavily on the intricate visual data generated by medical imaging technologies. With the growing digitization and seamless exchange of these crucial medical images, safeguarding their security and privacy has risen to the forefront as an imperative concern [10].

The pivotal role of medical imaging in diagnosis, treatment, and research is underscored by its ever-increasing digitization and widespread dissemination [10]. However, as we march toward an era of seamless data exchange, the security and privacy of these sensitive visual assets have become paramount [12]. Traditional encryption techniques, while effective in many scenarios, often fall short of addressing the unique challenges posed by medical image encryption. This challenge calls for innovative solutions that can offer robust protection without compromising the efficiency and integrity of medical image data [12].

One such innovative approach that holds promise in addressing these concerns is the application of DNA cryptography to targeted medical image encryption. The principles of genetics and molecular biology serve as the foundation for DNA cryptography, which uses the extraordinary properties of DNA molecules to encrypt and decrypt sensitive information [9]. This emerging field combines the inherent data storage capacity and parallel processing capabilities of DNA with the complexities of cryptographic algorithms, birthing a novel encryption technique with immense potential for elevating the privacy and security of medical image data.

The proposed approach seeks to offer a reliable and effective mechanism for safeguarding medical imaging data throughout its lifecycle. This method can get beyond the constraints of traditional encryption methods by taking advantage of DNA molecules' unique properties, such as their enormous capacity for information storage and intrinsic parallelism [11]. Additionally, it introduces the concept of selectivity in encryption, allowing for the targeted protection of specific regions or characteristics within medical pictures while preserving data integrity and clinical value.

This innovative article directs its focus toward several key aspects mentioned as follows:

- **DNA Cryptography**: We delve into the principles behind encoding and decoding information using DNA sequences, taking advantage of leveraging four nucleotide bases as symbols for information representation.

- **Medical Image Security**: We address the unique challenges posed by medical image encryption, including the need for real-time access, efficient storage, and preservation of diagnostic information.

- **Enhanced Privacy**: We discuss the potential benefits of DNA cryptography in enhancing patient privacy by reducing the risk of unauthorized access to sensitive medical data.

- **Data Integrity and Accessibility**: We highlight how DNA cryptography can potentially contribute to ensuring the integrity and availability of medical images, a critical factor for accurate diagnosis and treatment.

- **Challenges and Future Directions**: We address the practical challenges, limitations, and future research avenues in the application of DNA cryptography to medical image encryption.

The subsequent sections of the article are structured as follows: Section 2 provides insights into digital medical image encryption techniques. Section 3 delves into the proposed image cryptography techniques tailored for healthcare (ICTH) in the 5G network. Section 4 presents the experimental findings and conducts a comprehensive security study. Section 5 explores the utilization of the proposed model within the 5G Network. Finally, Section 6 offers a conclusion that synthesizes the key findings and implications of this research.

2. DIGITAL MEDICAL IMAGE ENCRYPTION TECHNIQUES

For the security and privacy of sensitive medical image data, digital medical image encryption solutions unquestionably play a pivotal role. This section explores some common digital medical image encryption techniques, along with their respective advantages and disadvantages. Table 1 provides an overview of these cryptographic techniques along with their advantages and disadvantages.

Table 1. Different Image Cryptography Techniques

Technique	Research Paper	Advantages	Disadvantages
Homomorphic Encryption	"Privacy-Preserving Deep Learning for Medical Image Analysis" by Shou et al. (2018)	Preserves data privacy during computation	Computational overhead
Visual Cryptography	"Visual Cryptography for Biometric Privacy" by Barni et al. (2005)	No decryption is required for visualization	Image quality loss
Steganography	"Medical Image Steganography: Study and Implementation" by Cheddad et al. (2010)	Hides data within the image	Vulnerable to detection
Watermarking	"Digital Watermarking of Medical Images: A Review" by Azeem et al. (2014)	Provides authentication and integrity	Susceptible to attacks
Chaos-Based Cryptography	"Medical Image Encryption Using Chaos-Based Compression" by Chang et al. (2009)	Chaotic systems offer randomness	Sensitivity to initial conditions
DNA-Based Cryptography	"DNA-Based Cryptography for Secure Data Storage" by Kozareva et al. (2012)	Unique and biological encryption medium	Complexity in DNA manipulation
Blockchain for Medical Images	"Blockchain-Based Secure	Immutable and tamper-resistant	Scalability and energy consump-

	Sharing of Medical Imaging Data" by Azaria et al. (2016)	ledger	tion
Visual Secret Sharing	"Efficient Visual Secret Sharing Scheme for Medical Images" by Thien et al. (2019)	Distributes the secret visually	Limited to a small number of participants
Quantum Cryptography	"Quantum Cryptography and Secure Communication" by Gisin et al. (2002)	Provides unconditional security	Limited practical implementation in healthcare
Elliptic Curve Cryptography	"Elliptic Curve Cryptography for Medical Image Security in IoT-Based Healthcare Systems" by Al-Riyami et al. (2020)	Strong security with smaller key sizes	Requires efficient key management and computation

2.1. Dual Hyper-chaos Map

The term "Hyper-chaos" denotes a state of extremely chaotic behavior within a dynamic system where multiple variables exhibit complex, unpredictable, and highly sensitive behaviors [1]. In the context of chaos theory and cryptography, hyperchaotic systems are often employed to enhance the security of encryption processes due to their increased complexity compared to regular chaotic systems [15].

A "Dual Hyper Chaotic Map" combines the effects of two hyper-chaotic maps to produce chaotic sequences. These sequences can be applied to crypto-graphic tasks like data encryption and secure transmission. The purpose of adopting dual hyper-chaos is to introduce an additional level of complexity and unpredictability, making it significantly more challenging for attackers to decipher the encrypted data without a comprehensive understanding of the initial conditions and parameters governing both chaotic maps. The dual hyper-chaos map is mathematically represented as equations (1–3):

$$x_{n+1} = a(y_n - x_n) + y_n - \frac{a}{2\pi}\sin(2\pi x_n) \quad (1)$$

$$y_{n+1} = bx_n - x_n z_n + cy_n - \frac{a}{2\pi}\sin(2\pi x_n) \quad (2)$$

$$z_{n+1} = x_n y_n - dz_n \quad (3)$$

In digital image encryption, the fusion of DNA Cryptography and Dual Hyper Chaos Map presents a unique and effective approach to safeguard sensitive image data [2]. This hybrid approach tackles the information-storage capabilities of DNA sequences and the chaotic behavior of dual hyper-chaotic maps to enhance encryption security. The following example illustrates how these two techniques may be combined:

I. **Generation of Dual Hyper Chaos Sequence:** As mentioned earlier, two chaotic maps are selected to generate the dual hyper-chaos sequence. These chaotic sequences will serve as one component of the encryption process.
II. **DNA Encoding of Chaotic Sequence:** Convert the binary representation of the dual hyper-chaos sequence into a DNA sequence. This encoding process typically involves mapping binary values to specific nucleotide bases (A, T, C, G) in DNA.
III. **DNA Encryption:** Apply DNA cryptography techniques to further encrypt the DNA sequence derived from the chaotic sequence. This may involve various methods such as DNA sequence shuffling, substitution, or other DNA-based cryptographic operations.
IV. **DNA Key Generation:** The initial conditions and parameters used to generate the chaotic sequence can also serve as the basis for generating a DNA encryption key. This key is essential for the DNA cryptography step.
V. **Pixel-wise XOR Operation:** Similar to the Dual hyper-chaos Map encryption process, perform pixel-wise XOR operation between the DNA-encrypted sequence and the pixel values of the original image. This step introduces confusion and combines the advantages of both techniques.
VI. **Repetitive Encryption Rounds:** Similar to the Dual hyper-chaos Map encryption process, the DNA-encrypted image undergoes multiple rounds of pixel-wise XOR operation with the chaotic sequence, enhancing the encryption strength.
VII. **Decryption Process:** The decryption process involves the reverse steps. Initially, the chaotic sequence is regenerated using the same initial conditions and parameters. Subsequently, the DNA cryptography decryption process is applied to recover the original dual hyper-chaos sequence. Finally, the pixel-wise XOR operation with the recovered sequence is conducted to retrieve the original image.

The integration of DNA Cryptography and the Dual hyper-chaos Map in digital image encryption offers several advantages:

- **Enhanced Security:** Dual-layer encryption employing chaotic sequences and DNA cryptography raises the complexity of attacks required to breach the encryption.
- **Multiple Key Sources:** The initial conditions for chaotic sequence generation and DNA encryption keys provide dual security layers, making the encryption process more resilient.
- **Inherent Parallelism:** DNA cryptography leverages the inherent parallelism of DNA sequences, potentially leading to faster encryption and decryption processes.

However, the integration of these two complicated techniques necessitates careful consideration of various parameters, key management, and potential computational overhead. Rigorous analysis and experimentation are necessary to assess the actual security strength and performance of this hybrid encryption approach in diverse scenarios [9].

The creation of the DNA structure of the digital medical image using these encoding principles results in a unique DNA structure for each image. This approach is employed in a proposed image cryptography technique tailored for healthcare to provide exceptional safety for digitized medical images.

3. PROPOSED IMAGE CRYPTOGRAPHY TECHNIQUES FOR HEALTHCARE (ICTH) IN 5G NETWORK

In this section, we present the Proposed Image Cryptography Techniques for Healthcare (ICTH) tailored for the 5G network environment. This innovative approach combines the power of DNA-based cryptography, Dual Hyper-chaos Maps, pixel selection, permutation, diffusion, and DNA decoding rules to create a robust and secure framework for the encryption

and decryption of sensitive medical images. The objective is to address the unique challenges posed by the digitization and transmission of medical images in modern healthcare, ensuring both data security and diagnostic integrity.

3.1. Pixel Selection Algorithm

The foundation of the ICTH method lies in the precise selection of pixels from the original digital medical image. This pixel selection algorithm ensures that only the most relevant and diagnostically significant pixels are included in the encryption process, reducing computational overhead while maintaining the integrity of the medical image. Figure 1 shows how the dual hyper-chaos map and DNA sequence processes are used in the suggested selective digitized medical image cryptosystem to secure medical images. The Pixel selection algorithm, which is used to choose the pixels for the proposed model from the original digital medical image, is shown in Algorithm 1.

Algorithm 1: Pixel Selection Algorithm:

- **Input:**
- Image (matrix of pixel values)
- Criteria for pixel selection (e.g., colour range, intensity threshold)
- **Output**
- Selected pixels (list of coordinates)

I.**Initialization:**

- Initialize an empty list to store the coordinates of selected pixels.

II. **Iterating Through Pixels in the Image:**

- Iterate through each row and column of the image matrix.

III. **Apply Selection Criteria:**

- For each pixel, verify if it satisfies the selection criteria. This might involve comparing pixel values to a certain threshold or ensuring that the pixel falls within a predefined colour range.

IV. **Meeting Criteria:**

- If the pixel meets the criteria, add its coordinates to the list of selected pixels.

V. **Continuing Loop:**

- Continue looping through all pixels in the image.

VI. **Returning Selected Pixels:**

- After iterating through all pixels, return the list of selected pixel coordinates.

Example Use Case:

Suppose there is a grayscale image, and one wants to select pixels with intensity values greater than a certain threshold (e.g., intensity > 150). The algorithm performs the following steps:

a) Iterates through each pixel in the image.
b) Check the intensity value of the pixel.
c) If intensity > 150, it adds the pixel coordinates to the list of selected pixels.
d) After processing all pixels, it returns the list of selected pixel coordinates.

This process ensures that only pertinent pixels are considered for subsequent encryption steps, enhancing both efficiency and security.

Matrix M1 has the chosen pixels, whereas matrix M2 holds the remaining pixels. They are both transformed into an 8-bit binary picture. To create the 4-bit DNA-encoded matrices C1

and C2, all eight DNA base patterns are applied to an 8-bit binary picture [3]. The binary image's pixel index determines which DNA encoding rules are used.

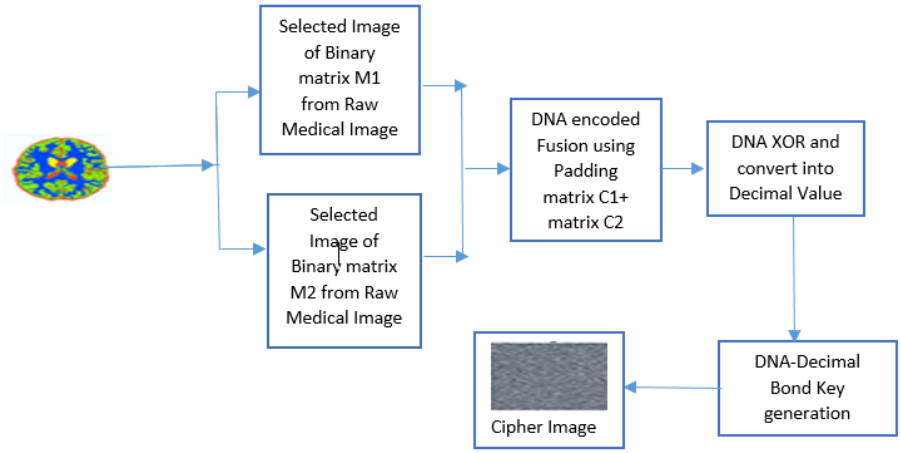


Figure 1. Proposed ICTH Method

3.2 Selection of DNA Rules

Selecting appropriate DNA rules for encoding chaotic data is a critical step in the ICTH framework. This process involves defining a mapping scheme that transforms chaotic values into DNA sequences. To guide this process, we present a straightforward algorithm as shown in Algorithm 2:

Algorithm 2: Selection of DNA Rules in Chaos Method:

Input:

- Chaotic sequence (a sequence of numerical values)
- Desired DNA base encoding (e.g., mapping to A, T, C, G)
- Encoding parameters (e.g., grouping values, sequence length)

Output:

- DNA sequence representing encoded chaotic data

I.Define Mapping Scheme:

- Decide how to map chaotic values onto DNA bases. This could be direct (one value per base) or involve grouping values.

II.Initialize DNA Sequence:

- Initialize an empty DNA sequence to hold the encoded data.

III.Encoding Process:

- Iterate through each chaotic value in the sequence:

i. Map the chaotic value to a DNA base according to the chosen encoding scheme.

ii. Append the mapped DNA base to the DNA sequence.

IV.Grouping (Optional):

- If grouping chaotic values, specify a group size (e.g., every 3 chaotic values form a group).
- Map each group of chaotic values to a corresponding DNA sequence (e.g., ATC).

V.DNA Sequence Generation:

- As you iterate through the chaotic sequence, construct the DNA sequence by appending the DNA bases or sequences.

VI.Outputting the DNA Sequence:

- Return the generated DNA sequence representing the encoded chaotic data.

VII. Security Considerations:

- Ensure that the mapping scheme doesn't introduce patterns or vulnerabilities that could be exploited by attackers.
- Analyze the collision resistance, randomness, and potential weaknesses of the chosen DNA rules.

VIII. Integration with Encryption:

- Integrate the generated DNA sequence with your chaos-based encryption process, using it as an encryption key or for additional encoding steps.

Example:

Suppose you have a chaotic sequence [0.734, -0.612, 0.921,] and you want to map it to DNA bases using a simple direct mapping:

- Positive values map to A or T
- Negative values map to C or G

The algorithm would then iterate through the chaotic values, map each value to a DNA base, and construct the DNA sequence accordingly.

3.3 Permutation Process

The permutation process within chaotic systems involves rearranging elements or data points according to the chaotic behavior of the system. This process enhances data security by introducing randomness, making it more challenging for attackers to predict or decipher the original data. Permutation is commonly used as part of cryptographic algorithms and data scrambling techniques to ensure data confidentiality and integrity [3].

Here's a general outline of how the permutation process can be integrated into a chaotic system:

I. **Selecting a Chaotic System:** Choose a chaotic system with well-defined equations exhibiting sensitive dependence on initial conditions. Common chaotic systems include the Logistic map, Henon map, and Lorenz system.

II. **Initialization:** Set the initial conditions and parameters of the chaotic system. These initial conditions act as the "seed" for the chaotic behavior.

III. **Generating Chaotic Sequence:** Iterate the chaotic system using its equations and the specified initial conditions to generate a sequence of chaotic values.

IV. **Mapingp Chaotic Values to Permutation Indexes:** Map each chaotic value to an index within the range of the data intended for permutation. This mapping can be done using a suitable mathematical function that transforms chaotic values into indexes.

V. **Applying Permutation:** Rearrange the elements of the data based on the mapped permutation indexes. This rearrangement process may involve swapping, position shifting, or other techniques.

VI. **Repeating the Process:** If necessary, repeat the process for a specified number of rounds or iterations to enhance the level of permutation and complexity.

VII. **Decryption (if applicable):** Implement a corresponding decryption process to reverse the permutation and recover the original data if this process is part of a cryptographic algorithm.

The benefits of integrating the permutation process into a chaotic system are as follows:

- **Increased Security:** Chaotic behavior enhances unpredictability, making the permutation process more effective in obscuring the original data.
- **Data Confidentiality:** Permutation can be used to protect sensitive information in data by making it more challenging to interpret.

As shown in Figure 1, the pixels of C1 are randomly shuffled using this index. The DNA-encoded matrix pixels are therefore subjected to random decoding rules.

3.4. Diffusion Process

Diffusion, a fundamental concept across various scientific domains, including physics, chemistry, biology, and computer science, plays a critical role in cryptography and data security. It refers to the gradual spreading or mixing of particles, molecules, or information due to random motion. In the context of cryptography and data security, diffusion enhances encryption algorithms' security by spreading the influence of one piece of data across a larger set of data [4].

In cryptography, the diffusion process is a crucial element of many encryption algorithms, particularly symmetric-key algorithms. It seeks to make the link between the plaintext and cipher text more complex and challenging to interpret by spreading the effect of certain plaintext bits or symbols across the cipher text. Diffusion makes sure that even modest input changes have a big impact on the output, making it harder for attackers to take advantage of trends. The Advanced Encryption Standard (AES), which uses a mix of substitution and permutation techniques to generate strong diffusion features, is a well-known example of diffusion in cryptography. Through a series of modifications, each byte of the plaintext is dispersed and blended with other bytes, guaranteeing that changes to one byte have a cascade impact on successive rounds of encryption. In summary, diffusion is a key concept in cryptography that focuses on spreading the influence of input data to achieve confusion and enhance security. It's an essential aspect of encryption algorithms that aims to make the relationship between plaintext and cipher text highly non-linear and resistant to various attacks. The shifting of pixel values is the chaotic system's diffusion process. The DNA XOR operation modifies the DNA-encoded matrix's pixel values. For instance, the Genetic-encoded matrix C1 contains the DNA sequence A T G C, whereas the Genetic-encoded matrix C2 has the DNA sequence G A C T. When these two nucleotides are joined using XOR, a new, distinct sequence called "G T T G" is produced.

3.5. DNA Decoding Rules

The Integration of DNA decoding rules with a dual hyper-chaos algorithm results in a sophisticated encryption method that offers enhanced security for digitized medical images. Here is an overview of how this combination might work:

I.DNA Decoding Rules:

- **Encoding**: DNA sequences are mapped to numerical values or binary strings using specific encoding rules. This process involves translating the four nucleotide bases (A, T, C, G) into a format suitable for mathematical operations.
- **Key Generation**: Specific segments or patterns within the DNA sequence can serve as encryption keys. DNA decoding rules determine how these segments are extracted and transformed into encryption parameters.

II.Dual Hyper-chaos Algorithm:

- **Key Initialization**: The DNA-derived encryption keys are used to initialize the parameters of the dual hyper-chaos algorithm. These keys modify the initial conditions or control parameters of the chaotic maps.
- **Encryption Process**: The dual hyper-chaos algorithm processes the plaintext medical image data using the modified chaotic maps. The resulting cipher text is highly sensitive to both chaotic behavior and DNA-encoded keys.

III.Integration:

- **Parameter Modification**: The selected segments of the DNA sequence are decoded using the predefined rules. The decoded values are then used to adjust the parameters of the chaotic maps, introducing variability and complexity into the encryption process.
- **Nonlinear Mixing**: DNA-derived parameters are combined with parameters from the Dual Hyper-chaos algorithm in a nonlinear and unpredictable manner. This mixing ensures that even slight changes in the DNA sequence result in significantly different encryption results [5].

IV.Decryption:

- **DNA Decoding**: Recipients of the encrypted data follow the same DNA decoding rules to extract relevant segments from the DNA sequence.
- **Parameter Adjustment**: These decoded segments adjust the chaotic map parameters during decryption.
- **Dual Hyper-Chaos Decryption**: Adjusted chaotic maps are employed to reverse the encryption process, revealing the original medical image data.

By combining DNA decoding rules with a dual hyper-chaos algorithm, ICTH establishes a multi-layered encryption method relying on both the inherent uniqueness of DNA sequences and the chaotic nature of the algorithm. This approach enhances security by introducing an additional layer of complexity, making it more challenging for potential attackers to decipher encrypted medical images. Moreover, the biological nature of DNA sequences adds an extra layer of security due to the biological nature of DNA and its potential resistance to certain types of attacks.

4. INVESTIGATIONAL OUTCOMES AND SECURITY STUDY

The experimentation was conducted on a computing system equipped with an Intel core process running at 3.60GHz, backed by 8 GB of RAM. A diverse set of digital healthcare images, including MRI, CT, Nuclear Medicine, X-ray, and Ultrasound images, were used for testing and analysis. The implementation of the proposed ICTH method was carried out using the Python programming language. Figure 2 displays the sample's original digitized medical image. In the proposed model, a new technique is introduced.

Steps in Suggested Image for the Healthcare Cryptosystem (ICTH)

I. **Background:** The depiction of a hospital scene featuring medical professionals, patients, and medical equipment sets the context for healthcare.
II. **Data Flow:** A visual representation of data flow, which could represent patient information, medical images, or electronic health records within the hospital environment. Data can be portrayed as streams of digital particles or as data packets.
III. **Encryption Techniques:** To signify the involvement of the cryptosystem, the encryption process can be represented using mathematical symbols (like +, -, ×, ÷) or encryption algorithms' like DNA Cryptography.
IV. **Key Exchange:** The key is to be transferred via the secure path of the network.
V. **Shield or Vault:** An illustration of a protective shield or vault enveloping the entire scene, emphasizing the cryptosystem's role in defense against unauthorized access and breaches.
VI. **Secure Connectivity:** Depict interconnected nodes or devices, such as computers, smartphones, and medical devices, within the hospital setting, representing secure communication channels enabled by the cryptosystem.

VII. **Privacy Icons:** Integration of privacy-related icons like a shield, lock, or puzzle piece, further emphasizing the importance of data security and confidentiality in healthcare.

The image should prioritize visual appeal, clarity, and ease of understanding to effectively convey the concept of healthcare data security achieved through a cryptosystem.

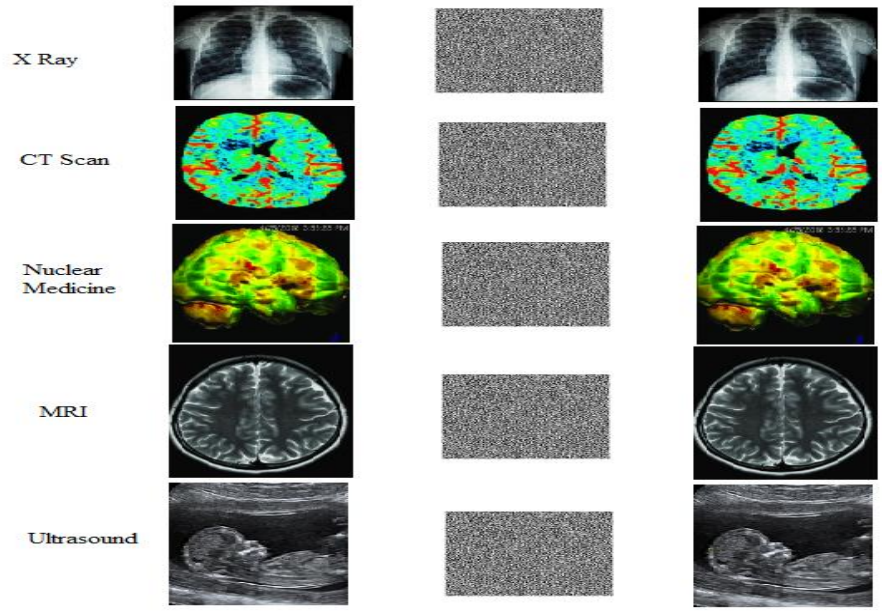


Figure 2. (a) Original image, (b) Encrypted Health image, and (c) Decrypted Health image

Table 2. DNA XOR Operation

XOR	A	T	C	G
A	A	T	C	G
T	T	A	G	T
C	C	G	A	C
G	G	C	T	A

Utilizing algorithm 1, the original digitalized medical picture is divided into two matrices: M1 contains the selected pixels, while M2 holds the remaining pixels. Both matrices are then transformed into 8-bit binary images [6]. To evaluate the effectiveness of the recommended ICTH approach, a series of cryptographic investigations were conducted, including differential attacks, exhaustive assaults, and statistical attacks, are conducted. An error rate is utilized to assess the peak signal-to-noise ratio (PSNR), mean square error (MSE), and entropy.

4.1. Statistical Attack

A statistical attack is a cryptographic attack method that analyzes data patterns, frequencies, or statistical properties to uncover hidden information. These attacks exploit vulnerabilities in data distribution or randomness to reveal hidden information, such as encryption keys or confidential messages. Statistical attacks leverage statistical tools and techniques to detect vulnerabilities in the encryption process, potentially compromising the security of the system [7].

4.1.1. Correlation Coefficient Analysis

Correlation coefficient analysis is a statistical technique used to quantify the strength and direction of the relationship between two variables. It measures how closely the values of two variables are related, with values ranging from -1 to 1, where -1 indicates a perfect negative correlation, 1 indicates a perfect positive correlation, and 0 indicates no correlation. Correlation coefficient analysis helps in how changes in one variable are associated with changes in another, aiding in data analysis, decision-making, and pattern identification [8].

The correlation coefficient analysis formula is as follows:

$$r = \frac{S\sum I_O \overline{I_O} - (\sum I_O)(\sum \overline{I_O})}{\sqrt{S(\sum I_O^2) + (\sum I_O)^2}\sqrt{N\left(\sum \overline{I_O^2}\right) + \left(\sum \overline{I_O}\right)^2}} \quad (5)$$

where Io and Io are, respectively, the gray-level frequencies of the actual digitalized medical image and its surrounding pixels.

4.1.2. Histogram Analysis

Histogram analysis is a visual and numerical technique used to understand the distribution of data values within a dataset. It involves organizing data into "bins" or intervals and counting how many data points fall into each bin. The resulting histogram graphically represents the occurrence or occurrence density of data values across different ranges [8]. Histograms offer an understanding of the figure, central tendency, spread, and outliers of a dataset, helping to identify shapes, trends, and characteristics that might not be immediately apparent from the raw data. The pictorial distribution of pixels is the histogram analysis shown in Figure 3.

4.2. Differential Attack

A differential attack is a type of cryptanalytic attack that exploits the differences between pairs of plaintexts and their corresponding cipher texts. It is a cryptanalytic technique that exploits differences between pairs of plaintext and ciphertext to deduce information about the inner workings of a cryptographic algorithm and potentially compromise its security. Utilizing the unified average changed intensity (UACI) and various varying pixel rate (NPCR) approaches, differential attacks are verified.

4.2.1 NPCR and UACI

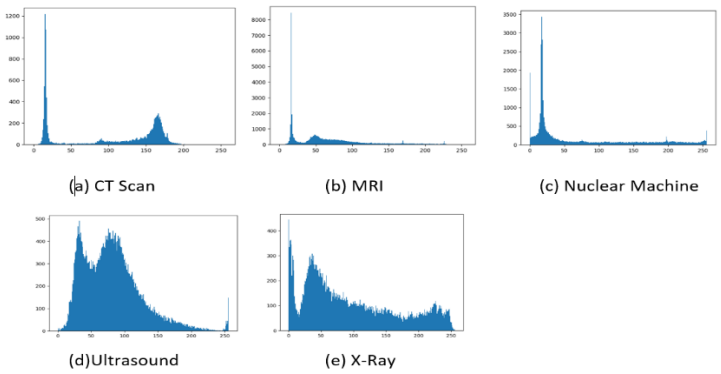
UACI measures the average intensity change between corresponding pixels of two encrypted images resulting from changes in the original images. It evaluates the algorithm's confusion property, aiming for uniform and unpredictable changes in pixel values. Lower UACI values indicate better confusion.

This pixel change rate is calculated using NPCR, as defined in (6).

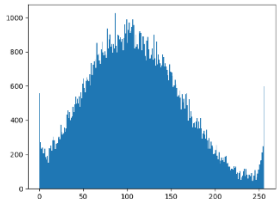
$$NPCR = \frac{\sum_{m,n} D_1(m,n)}{W_1 \times H_1} \times 100\% \quad (6)$$

Where W_1 and H_1 are the width and height of the digital medical image and D1(m, n) is defined as

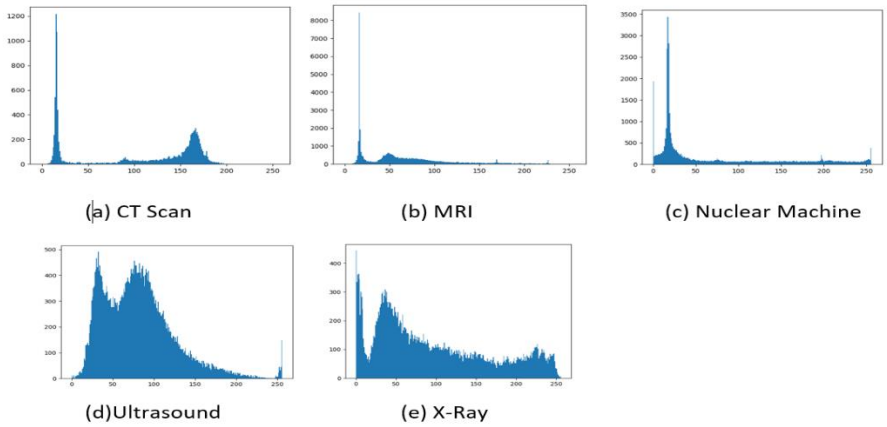
$$D_1(m,\ n) = \begin{cases} 0, & if\ I_{ee}(m,\ n) = I_e(m,\ n) \\ 1, & if\ I_{ee}(m\ \ n) \neq I_e(m,\ n) \end{cases} \quad (7)$$



(i)



(ii)



(iii)

Figure3. Histogram of (i) Original, (ii)Cipher & (iii) Decrypted image

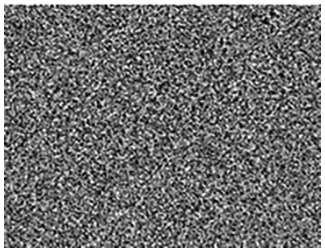


Figure4.Decrypted digitized image

The UACI is well-defined in Eq.(8)

$$UACI = \frac{1}{W_1 + H_1}\left[\sum_{m,n}\frac{|I_{ee}(m,\ n) - I_e(m,\ n)|}{255}\right] \times 100\,\% \quad (8)$$

where I_e and I_{ee} are original digitized medical pictures and a ten-pixel frequency altered original digitized image was used to create two ciphered images, respectively. Both NPCR and UACI are used to quantitatively evaluate the changes in encrypted images caused by changes in the original images. These metrics are often applied in pairs to provide a comprehensive assessment of an encryption algorithm's performance in terms of diffusion and confusion. It's important to note that while these metrics provide insights, they are not exhaustive and should be used alongside other security analyses to evaluate the overall security of an encryption scheme.

4.3. MSE and PSNR

Using PSNR and MSE measurements, the level of detail of the digital clinical picture is evaluated. Measures how well the encrypted digitalized medical picture resembles the original digitalized medical image. More similarity is represented by a number near zero, while less similarity is shown by larger values. The MSE estimates the average squared errors between the original digitally encoded medical picture (Io) and the encoded digitalized medical image (I_e). The MSE is defined in Eq. (9).

$$MSE = \frac{\sum_S [I_O(m,\ n) - I_e(m,\ n)]^2}{S} \quad (9)$$

The PSNR is used to determine if the relevance of the digitalized medical picture is impacted by the inclusion of noise during transmission. A superior encryption method is indicated by the lowest PSNR value. Eq. (10), which defines the PSNR.

$$PSNR = 10\log_{10}\frac{(256-1)}{MSE} \quad (10)$$

The PSNR is used where S represents the size (m × n) of the digitized medical image.

4.4. Entropy

A statistic for assessing the efficacy of encryption techniques is entropy value. Entropy measures the probability distribution of the grey levels throughout the whole picture. The more evenly distributed grey levels are indicated by a higher entropy score. The uniform distribution of grey levels suggests that the pixels are jumbled in a way that makes it very challenging for outsiders to predict even a tiny section of the straightforward medical image. As a result, a higher entropy value denotes superior con-fusion quality. Eq. (11) defines entropy.

$$\mathrm{H(U)} = \sum_{i=0}^{255} \mathrm{p}(u_i) log_2 \mathrm{p}(u_i) \quad (11)$$

where $p(U_i)$ represents the probability of distribution of the grey level of the encrypted digitized medical image.

4.5. Exhaustive attack

An exhaustive attack, also known as a brute-force attack, is a cyber-security technique in which an attacker systematically tries all possible combinations of characters, keys, or passwords until the correct one is found. This method is characterized by its thoroughness, as it leaves no stone unturned, trying every conceivable option to gain unauthorized access to a system, file, or encrypted data. While exhaustive attacks can be effective on weak or short passwords, they can be time-consuming and resource-intensive, especially when dealing with longer and more complex keys or passwords. Defenders often implement measures such as account lockouts and strong authentication methods to mitigate the effectiveness of exhaustive attacks.

4.6. Performance Analysis

Figure 5 displays the results of the ICTH method's performance analysis. Figure 5 shows that the NPCR value is close to 99.78% and the UACI value is close to 34.55%. The values are nearly identical to the optimal value of NPCR > 99% and UACI 33% [8]. The MSE and PSNR values in the proposed ICTH approach are close to 740.132 and 5.92 dB, respectively, indicating high encryption quality. The entropy value, which measures the uniformity of grey levels in the encrypted images, is approximately 7.8866 for ciphered images, close to the optimum entropy value of 8.0.

The ICTH approach that has been suggested offers effective security. According to our calculations, the encryption and decryption processes take 0.226 and 0.238 seconds, respectively, to complete. To check the relationship coefficient of nearby pixels, three thousand pixels of a digitalized medical picture are chosen in the horizontal, vertical, and diagonal directions. The mean correlation coefficient is displayed in Table 3. According to Table 3, neighboring pixels in a decrypted digital medical picture are strongly connected, but they are not as closely related in an encoded medical image. A decrypted digital image's average correlation coefficient is 0.9986, whereas a medical image's is 0.00164. Therefore, the proposed ICTH method is suitable for transmitting the digital medical picture across unassuming channels.

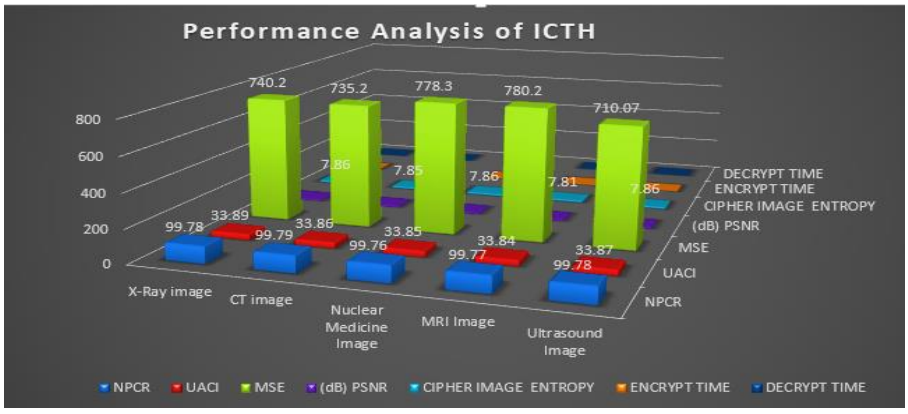


Figure5. ICTH method's Performance Analysis

Table 3. The correlation coefficient for the ICTH Method

Health Image	Side	Correlation Coefficient	
		Encrypted image	Decrypted image
X-Ray image	Horizontal	0.0196	0.992
	Vertical	0.0197	0.993
	Diagonal	0.0197	0.995

CT image	Horizontal	0.0192	0.996
	Vertical	0.0178	0.994
	Diagonal	0.0169	0.995
Nuclear Medicine Image	Horizontal	0.0189	0.989
	Vertical	0.0189	0.988
	Diagonal	0.0189	0.999
MRI Image	Horizontal	0.0159	0.992
	Vertical	0.0162	0.995
	Diagonal	0.0168	0.996
Ultrasound Image	Horizontal	0.0153	0.992
	Vertical	0.0152	0.993
	Diagonal	0.0146	0.994

Table 4 shows the comparison of times with different image size files and it is observed that the time complexity is quite efficient with increases of image size. Table 5 shows the different size images and key sizes. It is a general observation of image size and key size.

Table 4. Comparison of Time

Image size	Encryption time (s)	Decryption time (s)
128 * 128	4.01	0.285
256 * 256	18.8	0.478
512 * 512	25.5	1.236
1024 * 1024	35	3.366

Table 5. Image Size and Key Size Comparison

Image size	Raw File Size	Key Size
128 * 128	483 Kb	1kb
256 * 256	1.6MB	1kb
512 * 512	5.8MB	1kb
1024 * 1024	25.6MB	1kb

5. PROPOSED MODEL UTILIZATION IN 5G NETWORK

Establishing a secured healthcare ecosystem through DNA cryptography within a 5G network involves the integration of cutting-edge technologies to ensure the confidentiality, integrity, and availability of sensitive healthcare data while harnessing the capabilities of 5G connectivity. This section provides a comprehensive overview of how such a system might function effectively:

I. **DNA Cryptography**:

- DNA cryptography involves encoding and decoding data using the genetic information stored in DNA molecules. DNA sequences serve as encryption keys or carriers of information.
- DNA encryption offers an extremely high level of data security, as decoding without the correct DNA sequence is virtually impossible.

II. **Healthcare Data Security**:

- Electronic health records (EHRs), patient data, and medical research information are highly sensitive and demand robust protection.
- DNA cryptography can be employed to encrypt and secure these critical healthcare data sets.

III. **Integration with 5G Network**:

- 5G networks deliver high speed, low latency, and reliable connectivity, making them ideal for securely transmitting substantial volumes of healthcare data [13].

- The low latency of 5G ensures that encrypted data can be transmitted and processed in real time, which is essential for healthcare applications [14].

IV. **Authentication and Access Control**:
- Implement strong authentication mechanisms to guarantee that only authorized healthcare professionals and systems can access the data.
- Multi-factor authentication, biometrics, and DNA-based authentication can be integrated to enhance security.

V. **Data Storage and Transmission**:
- Encrypted healthcare data can be securely stored in cloud-based servers or distributed databases with stringent access controls.
- When transmitted over the 5G network, data should be further protected using encryption protocols such as TLS/SSL.

VI. **End-to-End Encryption**:
- Ensure that data remains encrypted from the point of origin to the destination, preventing unauthorized interception or tampering.
- The combination of end-to-end encryption and DNA cryptography adds multiple layers of security.

VII. **Security Auditing and Monitoring**:
- Continuous monitoring and audit of the system to detect and respond to security threats or breaches promptly.
- Implement intrusion detection systems and security information and event management (SIEM) solutions.

VIII. **Regulatory Compliance**:
- Adhere to healthcare data protection regulations such as HIPAA in the United States or GDPR in Europe.
- Ensure that the DNA cryptography and data handling practices comply with these regulations.

IX. **Disaster Recovery and Redundancy**:
- Develop robust disaster recovery plans to ensure data availability even in the event of network failures or natural disasters.
- Utilize redundant data centers and backup systems.

X. **User Education and Training**:
- Provides comprehensive training to healthcare staff and users on best practices for data security and privacy to minimize human errors.

XI. **Ethical Considerations**:
- Address ethical concerns related to DNA data usage, including consent, data ownership, and privacy rights of individuals.

  Creating a secured healthcare ecosystem using DNA cryptography in a 5G network is a complex endeavor that requires collaboration among experts in genetics, cyber security, networking, and healthcare. This approach should prioritize both data security and patient privacy while meeting regulatory requirements [13].

6. Conclusion

The fusion of DNA cryptography and medical image encryption presents a groundbreaking opportunity to transform the security landscape of sensitive medical data. The establishment of a secured healthcare ecosystem through DNA cryptography within a 5G network represents a visionary approach to meeting the complex security demands of the healthcare industry. It introduces the potential for a paradigm shift in how healthcare data is protected, shared, and utilized, all while prioritizing patient privacy and regulatory compliance. As tech-

nology progress continues, sustained research and development in this field will be essential to refining and expanding the capabilities of this innovative solution. DNA cryptography in the realm of healthcare holds the promise of becoming increasingly feasible and widely adopted. This could revolutionize data security in the healthcare industry, facilitating secure data exchange among medical professionals and ultimately enhancing patient care.

The proposed approach of selective medical image encryption using DNA cryptography (ICTH) represents a forward-looking solution with the potential to significantly enhance data security and privacy, ushering in a new era of secure medical information exchange. A secured healthcare ecosystem powered by DNA cryptography holds immense potential for the protection of sensitive medical data, the preservation of patient privacy, and the enhancement of data integrity. While there are challenges and ethical considerations that must be addressed, ongoing research and interdisciplinary collaboration can unlock the full potential of this innovative approach to healthcare data security.

Authors' contributions

The work's idea and design benefited greatly from the enormous contributions made by each contributor. AK and TB have analyzed and designed the work and created a new method presented in the work. AK and TB have performed the data duration formal analysis and interpretation of the data. AK has utilized the software. AK and TB have attained manuscript review and editing. AR has substantively revised it. The authors read and approved the final manuscript.

Funding

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Availability of data and materials

All data generated or analyzed during this study are included in the article (and in its supplementary materials).

Acknowledgments

Not applicable.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

References

1. Anusudha, K., Venkateswaran, N., & Valarmathi, J. (2017). Secured medical image watermarking with DNA codec. Multimedia Tools and Applications, 76(2), 2911–2932. doi:10.1007/s11042-015-3213-1

2. Fu, C., Li, W. J., Meng, Z. Y., Wang, T., & Li, P. X., (2013, December). A symmetric image encryption scheme using chaotic baker map and Lorenz system. In 2013 Ninth International Conference on Computational Intelligence and Security (pp.724–728). Leshan, China: IEEE. doi:10.1109/CIS.2013.158
3. Gehani, A., LaBean, T., & Reif, J. (2003). DNA-based cryptography. In Natasa, Jonoska Gheorghe, Paun Grzegorz, Rozenberg (Eds.), Aspects of Molecular Computing (pp. 167–188). Berlin, Heidelberg: Springer. doi:10.1007/978-3-540-24635-0_12
4. Hamza, R., & Titouna, F. (2016). A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Information Security Journal: A Global Perspective, 25(4–6), 162–179. doi:10.1080/19393555.2016.1212954
5. Kanso, A., & Ghebleh,M. (2015). An efficient and robust image encryption scheme for medical applications. Communications in Nonlinear Science and Numerical Simulation, 24(1–3), 98–116. doi:10.1016/j.cnsns.2014.12.005
6. Kester, Q. A., Nana, L., Pascu, A. C., Gire, S., Eghan, J. M., & Quaynor, N. N. (2015). A cryptographic technique for the security of medical images in health information systems. Procedia Computer Science, 58, 538–543. doi:10.1016/j.procs.2015.08.070
7. Krishnamoorthi, R., & Murali, P. (2014, February). Chaos-based image encryption with orthogonal polynomials model and bit shuffling. In 2014 International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 107–112). Noida, India: IEEE. doi:10.1109/SPIN.2014.6776931
8. Prema T. Akkasaligar and Sumangala Biradar (2020). Selective medical image encryption using DNA cryptography Information Security Journal: A Global Perspective (pp. 91-101) doi: 10.1080/19393555.2020.1718248
9. A. Kairi, T. Bhadra, “Decoding The Future Using A Novel Dna-Based Cryptosystem”, in Journal of European Chemical Bulletin, Volume -12, Special Issue-10: Page: 3597 –3609 2023.
10. H. Montenegro, W. Silva, and J. S. Cardoso, "Privacy-Preserving Generative Adversarial Network for Case-Based Explainability in Medical Image Analysis," in IEEE Access, vol. 9, pp. 148037-148047, 2021, doi: 10.1109/ACCESS.2021.3124844.
11. Q. -X. Huang, W. L. Yap, M. -Y. Chiu and H. -M. Sun, "Privacy-Preserving Deep Learning With Learnable Image Encryption on Medical Images," in IEEE Access, vol. 10, pp. 66345-66355, 2022, doi: 10.1109/ACCESS.2022.3185206.
12. A. Cheddad et al, Digital image steganography: Survey and analysis of current methods, Signal Processing, Volume 90, Issue 3 2010, Pages 727-752, ISSN 0165-1684,https://doi.org/10.1016/j.sigpro.2009.08.010
13. P. Pirinen, "A brief overview of 5G research activities," 1st International Conference on 5G for Ubiquitous Connectivity, Akaslompolo, Finland, 2014, pp. 17-22, doi: 10.4108/icst.5gu.2014.258061
14. A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," in IEEE Access, vol. 3, pp. 1206-1232, 2015, doi: 10.1109/ACCESS.2015.2461602
15. Ravichandran, D., Praveenkumar, P., Rayappan, J. B. B., & Amirtharajan, R. (2017). DNA chaos blends to secure medical privacy. IEEE Transactions on Nanobioscience, 16(8),850–858. doi:10.1109/TNB.2017.2780881