International Research Journal of Multidisciplinary Scope (IRJMS), 2024; 5(4):1084-1094 IRJMS

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2024.v05i04.01653

Homomorphic DNA Security in IoT Edge Data

Lakshmanan S [1]*, Kokilavani T[2], Joseph Charles P[1]

[1]Department of Computer Science, St. Joseph's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu-620005, India, [2]Department of Computer Science, Christ University, Nagasandra, Bangalore, Karnataka-560073, India. *Corresponding Author's Email: lakshmansjc1@outlook.com

Abstract

The Internet of Things (IoT) based intelligent medical system possesses sensitive and private patient data. Most data relates to the patient's medical records and highly sensitive information. For this reason, safety and confidentiality of information are crucial. The preservation of patient privacy when sharing medical data is the primary concern of this study. Due to their excellent performance, biological notations based on deoxyribonucleic acid (DNA) are becoming increasingly admired for guaranteeing encryption and image protection. This paper proposes lightweight homomorphic with DNA-based medical image encryption (HDNA_MIE) for heterogeneous IoT in edge computing. The proposed approach contains two steps: In the first step, the secure DNA keys are generated using lightweight operations such as shifting and Josephus ring-based permutation (JRP). In the second step, the lightweight homomorphic cryptographic algorithm with DNA sequence-based encryption algorithm is suggested for secure encryption. The suggested strategy is evaluated using computational time and statistical analysis with several measures to determine its efficacy. The experimental findings of the proposed strategy exhibited a high level of security and a noticeable enhancement in the Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI) and encryption processing time. The experiment outcomes demonstrate that our technique may be applied to highly confidential image encryption.

Keywords: DNA Sequence, Homomorphic Encryption, Image Encryption, Lightweight Cryptography, Medical Data Security.

Introduction

The Internet of Things (IoT) integrates the physical and digital realms to create a unified communication network of connected objects (1). The transmission of medical data has become commonplace with the introduction of distant computerized healthcare oriented IoT solutions. An effective model must be developed to guarantee the secrecy and reliability of the patient's clinical information communicated from the Internet of Things (2). One of the security precautions for safe communications is cryptography. The most popular method for reducing the security gap is to encrypt data stored remotely. The encryption and decryption technologies are offered in three types: symmetric, asymmetric, and hybrid algorithms, which may be applied to encrypt and decode data (3). Numerous lightweight architectures are made for contexts with limited resources. For randomization, most of them employed elliptic curves (4), AES, and chaotic maps (5). Lightweight block ciphers are often implemented to enable bulk data encryption and are significant building blocks in creating many cryptographic protocols. Compared to traditional cryptographic methods, Paillier homomorphic encryption allows encrypted data to be computed while maintaining functionality and privacy (6).

Medical image encryption is one of the expanding fields in which cryptographic systems are being used; effective methods with minimal time and cost requirements should be used. Symmetric or asymmetric cryptographic techniques must be used when encrypting an image to change the original picture into a cipher picture. This procedure is called image encryption (7). Numerous methods and settings are available for encrypting medical photos. The idea of biological DNA operations is currently being used in many ways to ensure image security. Here, the researchers map DNA using alternative rules based on binary (8) or hexadecimal (9) numbers. Additional operations are also performed on DNA,

(Received 16th July 2024; Accepted 25th October 2024; Published 30th October 2024)

such as XOR, addition, subtraction, and so on. These methods are utilized to the encryption and decryption of the whole picture.

Numerous researchers have indicated that DNA-based techniques (10, 11) have shown to be the most effective method for encrypting images due to their huge parallelism and reduced time complexity.

A lightweight, effective encryption system by Hasan *et al.,* (12) secures healthcare image data. Medical photos are protected by lightweight encryption using two permutation techniques. The image is encrypted in three phases using a 256-bit key value for logic. Rajendran *et al.,* (13) recommend a chaotic security design for medicinal picture transmission and storage. Model construction involves three main steps. To construct the Lorenz chaotic map seed key, the plain picture is processed using message digest five ways. In the second stage, row and column wise

Disorders are applied to the picture. Finally, binary reverse and complement procedures are used to dual diffusion.

To secure medical photos, Li *et al.* use DNA coding, Secure Hash Algorithm 3 (SHA-3), and a chaotic system (14). A SHA-3 hash value is computed from the originalpicture and used as the hyper-chaotic system's starting value. Second, image intensity forms a consecutive binary digital sequence. Third, a 4-dimensional hyper-chaotic pseudo-arbitraryseries globally perturbs the bit stream to hide the input image's effective information.Yin *et al..* (15) show how to improve elliptic curve cryptography (ECC) by adding homomorphic encryption. The author employed the enhanced ECC to make the addition and multiplication homomorphisms. John *et al.,*'s medical picture encryption uses a linear feedback shift register (LFSR, 16). Pixel location is shuffled by the LFSR to generate pseudo-random integers. The receiver side node can decipher the encrypted picture provided via a cloud platform to restore the original image. DICOM computed tomography pictures are used to evaluate.

Aditya *et al.,* (17) presents a new cryptosystem that encrypts sensitive medical images using affinity transformation, Knight's trip map, DNA sequencing, and chaotic maps. Two kinds of matrices and chaotic sequences are generated from the medical pictures. This work enhances the security and reduces the attacks. Xie *et al.,* introduced DNA encoding and hyperchaos (18). It had four phases: scrambling, diffusing, producing key streams, and forming chaotic system beginning values. Wu *et al.,* (19) suggests a content-aware DNA computing method to protect medical pictures. A transmitter and receiver engage in encryption and decryption using an identical structure but with distinct operations. Thabit *et al.,* describe a lightweight, efficient homomorphic cryptographic scheme with two encryption levels (20). The initial level uses a unique, efficient, simple cryptographic technique and the next level examines homomorphic schemes to increase cloud computing security data.

An innovative and effective climbing method for picture encryption is proposed byUddin *et al.,* (21). Complex operations on encrypted data can be carried out utilizing homomorphic encryptions without decrypting individual data using homomorphic properties.Two homomorphic qualities employed for sophisticated computation without disclosing information are additive and multiplicative (22). There are three types of homomorphic encryption: Partial, Somewhat and Full homomorphic encryption (23). Many researchers used the Josephus ring (24) for encrypting images. Wang *et al.,* (25) suggests a new scheme which integrates chaotic systems and Josephus movement. The algorithm employed the Josephus traversal for pixel jumblingandthe chaotic system to manipulate pixels. Hua *et al.,* (26) suggests new techniques based on the Josephus dilemma and filter dispersion.A new and enhanced Josephus ring-based permutation technique is proposed by Guan *et al.,* (27). Iqbal *et al.,* (28) introduces a novel RGB (colour picture) encryption approach that improves security by combining DNA computing, 5D multi-wing hyperchaotic systems, and Dynamic 3D scrambled images (D3DSI). A colour image is transformed into a 1D array when its three parts are supplied.In order to secure images, this paper presented a new approach (29) that uses a DNAsequence of variable size. The programme accomplished picture encryption by DNA dynamic coding, generated a DNA dynamic chain, and dynamically operated the row and column chains.

This proposed approach presents lightweight homomorphicwith DNA-based medical image

encryption (HDNA_MIE). The suggested method consists of two steps: First, lightweight procedures like shifting and Josephus ring-based permutation (JRP) are used to construct the secure DNA keys. For secure encryption, a lightweight homomorphic cryptographic technique with DNA sequences is suggested in the second stage.

Methodology

This section explains the proposed lightweight homomorphic with DNA-based medical image encryption (HDNA_MIE) for heterogeneous IoT in edge computing. The proposed approach contains two steps: In the first step, the secure DNA keys are generated using lightweight operations such as shifting and Josephus ring-based permutation (JRP). In the second step, the lightweight homomorphic cryptographic algorithm with DNA sequence-based encryption algorithm is suggested for secure encryption. Figure 1 depicts the workflow of the suggested HDNA_MIE design.

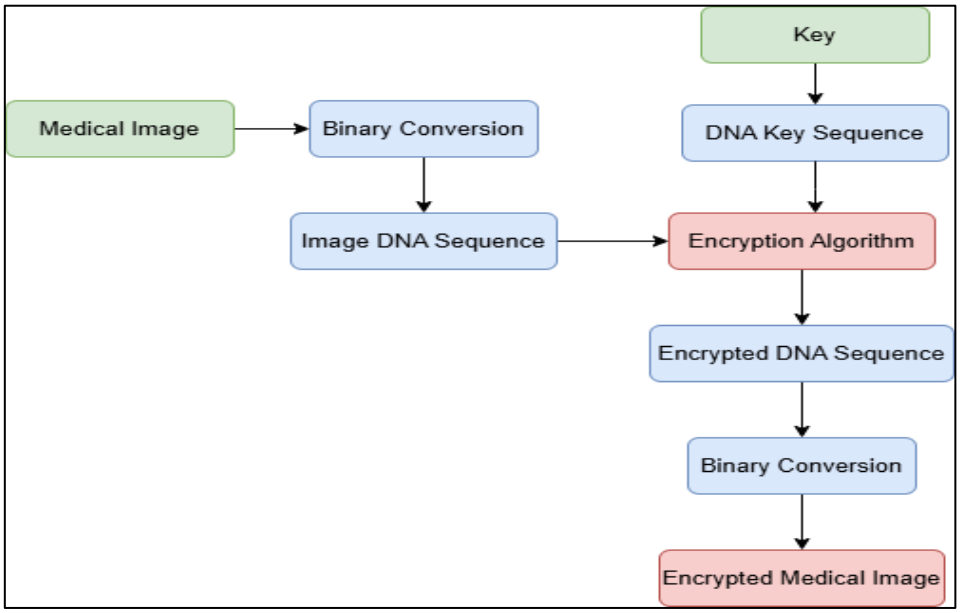

Figure 1: Proposed Architecture

Key Generation

The key is essential in facilitating the encryption and decryption procedure. The proposed algorithm is derived from DNA sequences and logical operations, strengthening the key. The stronger the key generated, the more secure the encryption becomes, the more complex the encryption is, and the fewer attackers will know the key. The 8-bit string key generates six sub-keys (K1, K2, K3, K4, K5, and S.K.).The proposed key generation algorithm (Algorithm-1) is shown below. Figure 2 illustrates the procedure of generating the key.

The input (8-bit key string) is 'mysecret'. Table 1 shows the binary and corresponding DNA sequences.

Algorithm-1: Key Generation
Input: 8-bit string key
Output: DNA keys (K1, K2, K3, K4, K5, SK)

Step01: Convert 8-bit string key to binary value
Step02: Generate 32-bit DNA Sequences from binary value
Step03: Divide 32-bit sequences into 16-bit S1 and 16-bit S2
Step04: Divide S1 into 8 bit DNA sequences (R1 and R2)
Step05: Divide S2 into 8 bit DNA sequences (L1 and L2)
Step06: RP1 = shift R1 by 4 bit
Step07: RP2 = Apply JRP function
Step08: LP1 = shift L1 by 4 bit
Step09: LP2= Apply JRP function

Step10: $K1 = RP1 \oplus RP2$
Step11: $K2 = RP2 \oplus LP1$
Step12: $K3 = LP1 \oplus LP2$
Step13: $K4 = K1 \oplus K2$
Step14: $K5 = K2 \oplus K3$
Step15: SK = Combine K4 and K5
Return K1, K2, K3, K4, K5 and SK

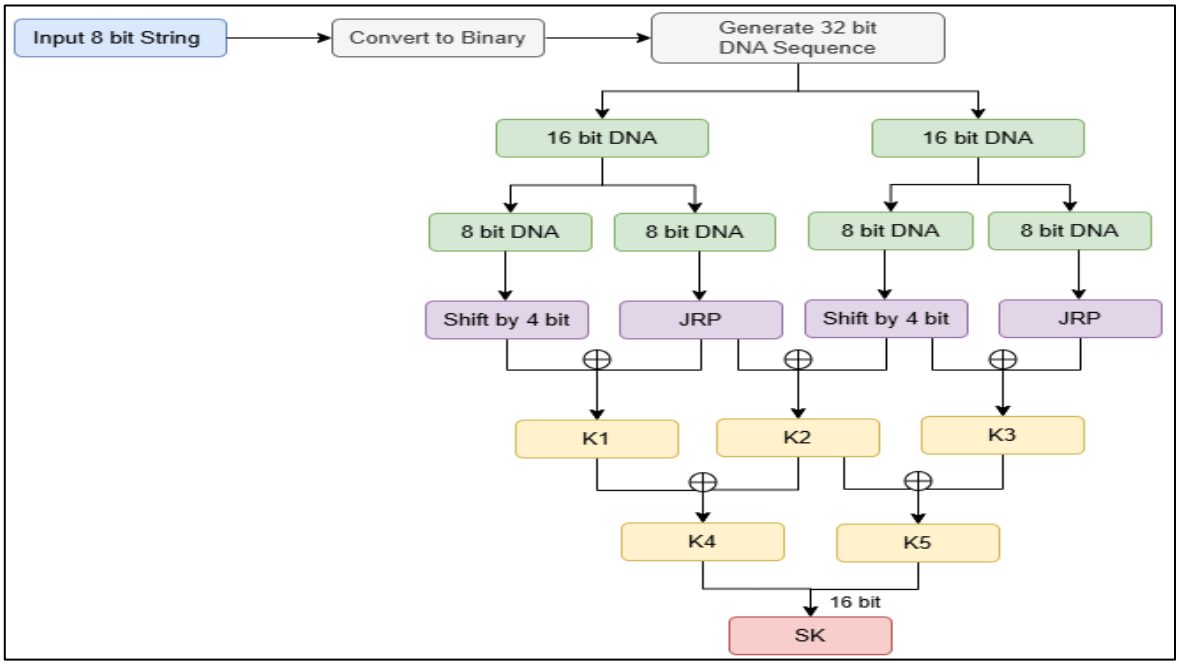

Figure 2: Key Creation Process

Table 1: DNA Sequences

Input	Binary Value	DNA Sequences
m	01101101	CGTC
y	01111001	CTGC
s	01110011	CTAT
e	01100101	CGCC
c	01100011	CGAT
r	01110010	CTAG
e	01100101	CGCC
t	01110100	CTCA

The 32-bit DNA sequence 'CGTCCTGCCTATCGCCCGATCTAGCGCCCTCA'
S1 = CGTCCTGCCTATCGCC
S2 = CGATCTAGCGCCCTCA
R1 = CGTCCTGC
R2 = CTATCGCC
L1 = CGATCTAG
L2 = CGCCCTCA
RP1 = shift R1 by 4 bit = CTGCCGTC
RP2 = Apply JPR for R2 by 4 step= TCCTCACG
LP1 = shift L1 by 4 bit = CTAGCGAT
LP2 = Apply JPR for L2 by 4 step= CACGCCCT

$$K1 = RP1 \oplus RP2 = CTGCCGTC \oplus TCCTCACG = GGTGAGGT$$
$$K2 = RP2 \oplus LP1 = TCCTCACG \oplus CTAGCGAT = GGCCAGCC$$

$$K3 = LP1 \oplus LP2 = CTAGCGAT \oplus CACGCCCT = ATCAATCA$$
$$K4 = K1 \oplus K2 = GGTGAGGT \oplus GGCCAGCC = AAGTAATG$$
$$K5 = K2 \oplus K3 = GGCCAGCC \oplus ATCAATCA = GCACACAC$$
$$SK = Combine\ K4\ and\ K5 = AAGTAATGGCACACAC$$

Encryption Process

This section explains the algorithm for encrypted medical pictures. The image is encrypted using multiple rounds with simple, lightweight operations like, shifting, XoR and addition of DNA sequences. Algorithm-2 explains the proposed medical picture encryption process.

The paillier encryption algorithm is initially used to encrypt the medical picture. The DNA sequences are generated for encrypted pixels. These DNA sequences are encrypted using keys generated from algorithm-1 with lightweight operations. Figure 3 shows the working procedure of the encryption technique.

Algorithm-2: Medical Image Encryption
Input: Medical Image (MI), DNA keys
Output: Encrypted Medical Image (EMI)

```
01: GetMIHeight and Width
02: For i = 1 to MI_Width
03:    For j = 1 to MI_Height
04: pix = getMI_Pixel()
05: encPix = Apply Paillier Encryption (pix)
06: binPix = Convert encPix to binary format
07: DNAPix = Generate DNA sequences of binPix
08:    End For
09: End For
10: For each seq in DNAPix
11:    S1 = K1 + K2 // Combine keys
12:    A1 = XoR (seq, S1) // apply xor between sequence and combined keys
13:    R1 =  Left_Shift (A1, 4) // apply left shift
14:    S2 = K2 + K3
15:    A2 = XoR (R1, S2)
16:    R2 = Right_Shift (A2,4)
17:    S3 = K3 + K4
18:    A3 = XoR (R2, S3)
19:    R3 = Left_Shift (A3, 4)
20:    S4 = K4+K5
21:    A4 = XoR (R3, S4)
22:    R4 = Right_Shift (A4, 4)
23:    R5 = DNA_Add (R4, SK)
24: encDNAPix = R5
25:    encBin = Generate binary value for encDNAPix
26:    encImgPix = Convert binary into an integer value
27:    Set encImgPix to EMI
28: End For
29: Return EMI
```

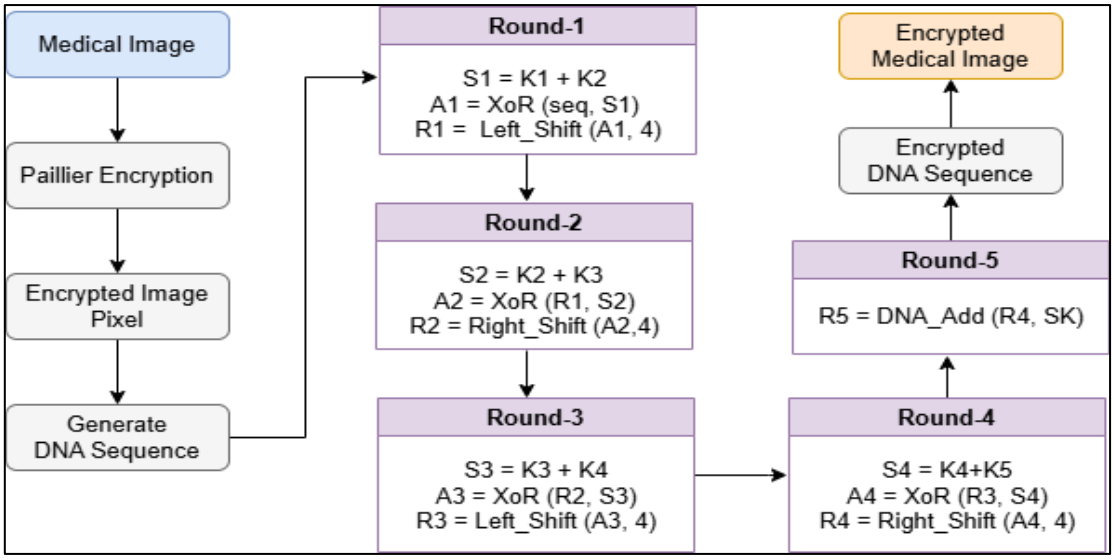

Figure 3: Encryption Process

Decryption Process

The original plain image is intended to be produced by an image decryption method. When a suitable decryption technique is used, the image is completely recreated, meaning it is 100% identical to the original. It is the computational inverse of the encryption process.

Results

This section analyses the performance of the proposed HDNA_MIE using different evaluation metrics. Figure 4 shows the sample images from OPENi database (30) to validate the proposed approach.

The efficacy of the suggested technique is analysed using the following metrics: Execution Time, histogram analysis, information entropy, NPCR, UACI, PSNR and MSE.

Execution time is one of the most important factors when developing cryptography. Cryptographic execution time for encryption refers to the overall duration required to perform both the encryption and decryption processes on unique data. Table 2 shows the duration required for both the encryption and decryption processes. The decryption time for the image is less than the encryption time.

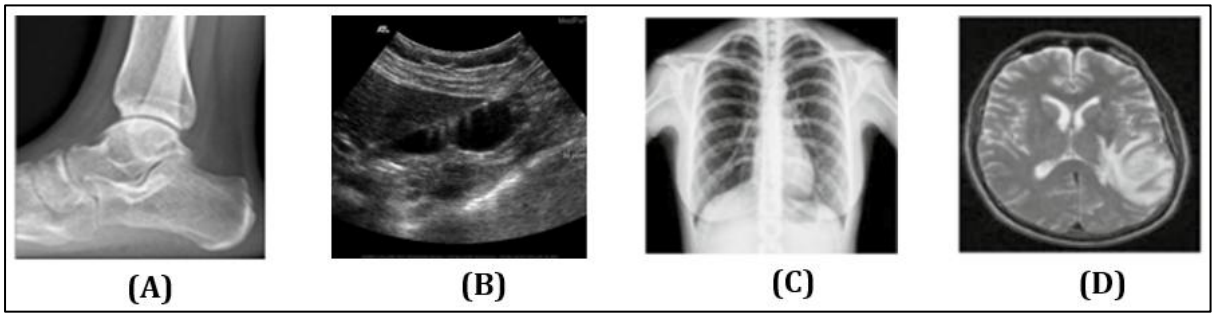

Figure 4: Sample Input Medical Pictures (A) CT Scan (B) Ultrasound (C) X-Ray (D) MRI

Table 2: Encryption and Decryption Time

Image	Encryption Time (ms)	Decryption Time (ms)
CT Scan	43767	17232
Ultrasound	32124	12812
X-Ray	37620	12523
MRI	34513	15313

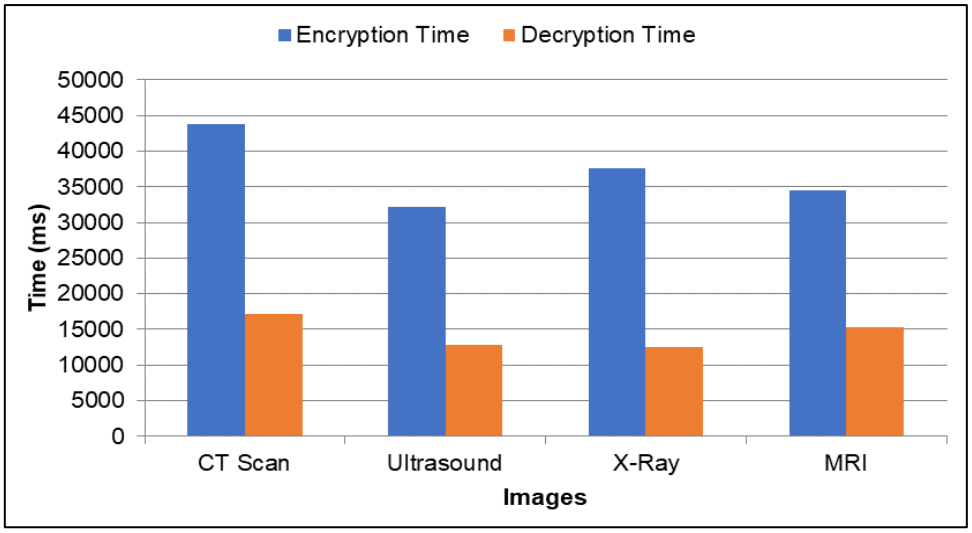

Figure 5: Execution Time

The performance of execution time for different images is shown in Figure 5. The histogram illustrates the distribution of pixel frequencies in the image. To ensure that an attacker cannot predict any picture data, it is important for an encrypted image to have a histogram that is evenly distributed. Furthermore, it is necessary to distinguish among the histograms of the original and encrypted images. Figure 6 displays the histograms and encrypted versions of medical pictures.

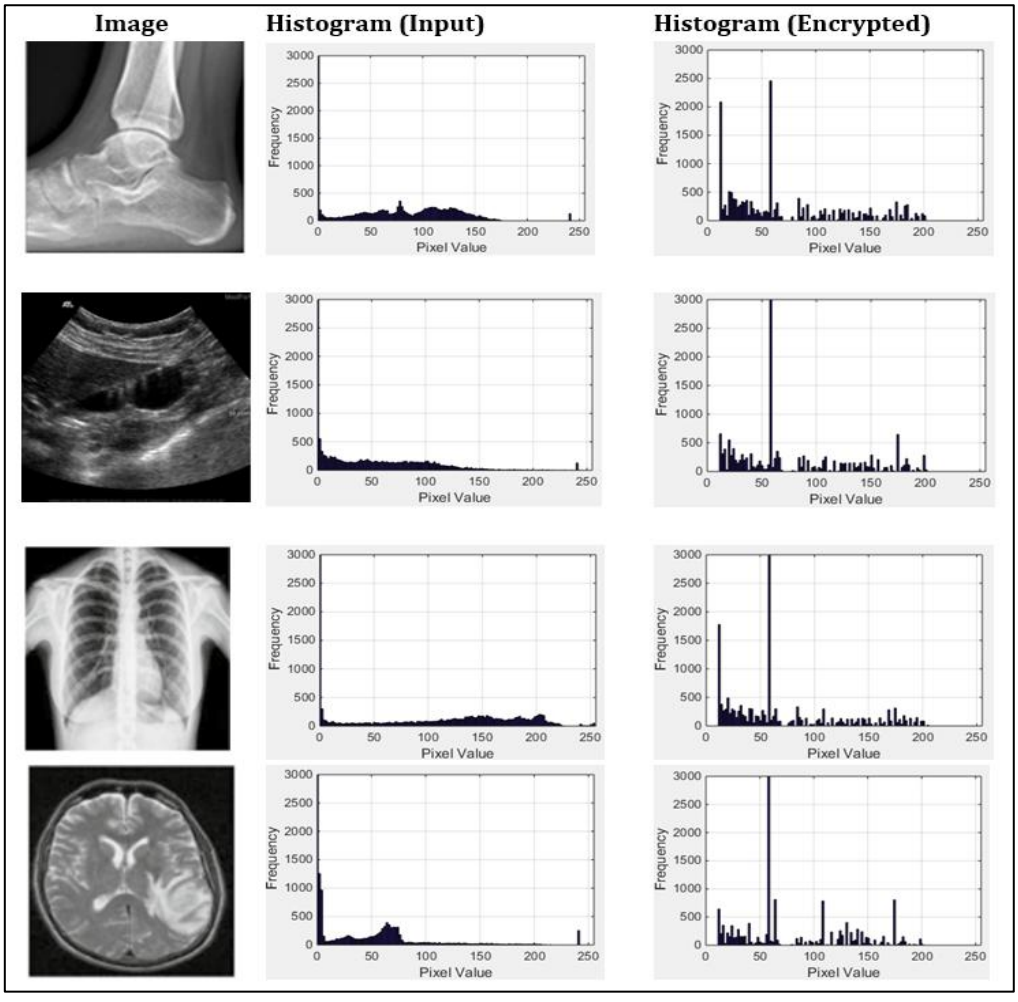

Figure 6: Histogram of Input and Encrypted Image

Experimental Setup

The proposed algorithm is implemented using python and its libraries. Arduino boards equipped with medical sensors (e.g., heart rate monitors) to simulate a healthcare monitoring system. Private cloud is installed on the mini pc 17 7000 series on an Intel Core TM i7-3120 M processor, 2.50 GHz 8G.B. RAM. Private cloud set up is used for storage, key generation and encryption process. Configured IoT devices to collect real-time data (e.g., vital signs) and transmit it to the private cloud storages. It is used to generate synthetic medical data (e.g., images, patient records) which is used for testing purposes.

The input and encrypted images' grey statistics differ significantly from one another. The input image's histogram is smooth and regular, but the encrypted picture's histogram is erratic and uneven. The encrypted picture grey value distribution differs greatly from the inputimage's. As a result, the encrypted image's grey value distribution, which is resistant to statistical attacks, cannot provide details about the input picture.

The unpredictability of an picture is measured by its entropy. The mathematical definition of entropy is expressed in eq. [1] below, where P(c) is the probability that c will appear; for greyscale images, the greatest entropy value is 8. When the entropy number is near eight, the image's pixels are more arbitrary. Table 3 shows the information entropy for pictures.

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

Table 3: Image Information Entropy

Image	Input Image	Encrypted Image
CT Scan	6.465890	7.9981
Ultrasound	5.926256	7.9924
X-Ray	6.344654	7.9972
MRI	5.279447	7.9989

Nonetheless, the encrypted images are highly unpredictable since their entropies are near the theoretical value of 8. This enhances the level of difficulty for an attacker to retrieve valuable data from the encrypted pictures.

The differential attack relies on predicting data about an image by slightly altering the plain picture and using the same procedure to encrypt both images. A comparison of the two images finds a correlation among the original the encrypted picture. Any modification to the original picture should effect in a dissimilar encrypted picture when using a viable technique. NPCR and UACI were employed to estimate the algorithm's performance. Calculations for the NPCR and UACI are as follows:

$$NPCR = \frac{1}{xy} \sum_{i=1}^{x} \sum_{j=1}^{y} D_{ij} * 100 \quad [2]$$

$$D_{ij} = \{0 \; if \; E_{ij}^1 = E_{ij}^2 \; 1 \; if \; E_{ij}^1 \neq E_{ij}^2 \quad [3]$$

$$UACI = \frac{1}{xy} \sum_{i=1}^{x} \sum_{j=1}^{y} \frac{|E_{ij}^1 - E_{ij}^2|}{255} * 100 \quad [4]$$

Images are susceptible to noise distortion during distribution through channels that can adversely affect their clarity. To safeguard encrypted images from such assaults, resilient encryption algorithms are essential. The efficacy of an encryption algorithm in countering noise attacks can be assessed by decrypting the encrypted images altered by noise and analyzing the structures in the deciphered images using the peak signal-to-noise ratio (PSNR).

The PSNR measures the dissimilarity when comparing the original and encrypted images. It is calculated by eq. [5] and eq. [6] stated below. The original image is called OI, and the encrypted image (EI).Lesser PSNR values indicate a considerable divergence among the original and the encrypted picture. Table 4 shows the outcomes of NPCR, UACI, PSNR and MSE.

$$PSNR = 10 * log_{10}\left(\frac{255^2}{MSE}\right) \quad [5]$$

$$MSE = \frac{1}{xy}\sum_{i=1}^{x}\sum_{j=1}^{y} |OI_{ij} - EI_{ij}|^2 \quad [6]$$

Table 4: NPCR, UACI, PSNR and MSE

Image	NPCR	UACI	PSNR	MSE
CT Scan	99.6984	33.6134	11.6254	0.068421
Ultrasound	99.7571	33.5787	10.8194	0.073852
X-Ray	99.8540	33.6421	9.98243	0.145127
MRI	99.8721	33.7824	10.7341	0.075813

The Table 5 presents results from different approaches used in a study related to medical image encryption. It compares four different methods based on three important metrics: Entropy, NPCR, and UACI. Each of these metrics helps to measure how secure and effective the encryption methods are.

Entropy: This is a measure of randomness or unpredictability in the encrypted data. In simple terms, higher entropy means that the encrypted image is more complex and harder to guess. Although all the approaches has a value close to 8 which seems like they provide a good security but vulnerable to complexity and computational overhead.

NPCR (Number of Pixels Change Rate): This measure indicates how many pixels in the encrypted image change when a small change is made to the original image. A higher NPCR value means that even a tiny change in the original image will result in a significant change in the encrypted image, making it harder for someone to decipher the original data. In this Table 5, the proposed approach have NPCR of 99.87, which is excellent.

UACI (Unified Average Changing Intensity): This measure looks at the average change in intensity of the pixels in the encrypted image compared to the original image. It helps to understand how much the encryption alters the image. Higher UACI values indicate that the encryption is effective in disguising the original image. In Table 5 the proposed approach has higher UACI of 33.78 which indicates that it has better security with other approaches. From Table 5 , it is observed that the proposed method is slightly better than other approaches in terms of entropy, NPCR and UACI. All other existing approaches (18, 28, 29, 31) have a major drawback such a as lesser throughput, computational overhead, larger key size and doesn't focus on various images and its properties. The approaches' performance depends on the size and type of the images. The suggested approach entropy value is lower than the approach (31) due to the image properties (width, height, and pixel).

Table 5: Performance Comparison

Approach	Entropy	NPCR	UACI
(18)	7.9921	99.61	33.16
(28)	7.9972	99.61	33.24
(29)	7.9992	99.61	33.42
(30)	7.9973	99.60	33.60
Proposed	7.9989	99.87	33.78

Discussion

The intrinsic variability in DNA sequences implies that minor alterations in encoding can result in diverse outputs, thereby enhancing protection against attacks. DNA possesses the capacity to store vast quantities of information within a compact physical space, rendering it more challenging to access and manipulate than conventional data storage techniques. DNA encoding can integrate error-correcting codes, thereby ensuring data integrity and increasing resilience against data loss or corruption.

Furthermore, DNA encryption can be amalgamated with additional encryption methodologies, offering multiple layers of security and complicating unauthorized access for attackers.

Alongside stringent security, computational speed constitutes a crucial element of any image encryption framework. The suggested encryption method amalgamates diverse encryption techniques, including DNA and homomorphic methods. Nevertheless, the execution time escalates due to the integration of multiple techniques and the mathematical operations necessary for generating the encrypted image. A notable problem with the design of the suggested encryption schemes is the relatively constrained key space. This limited key space renders the scheme susceptible to brute force attacks, as an adversary can readily attempt all conceivable combinations of secret keys.

In a statistical attack, attackers or malevolent individuals attempt to identify a correlation among the encrypted image and the original image by analyzing pixel luminance. An effective picture encryption technique must ensure that all pixels of the encoded image are homogeneous and evenly distributed throughout the image. The suggested approach converts all pixel values of the image into DNA sequences through many rounds of operations, hence enhancing data security. The suggested cryptosystem employs the Paillier encryption method to encrypt the medical image, followed by numerous DNA operations that transform the original image into an encrypted version that is entirely distinct from the original. Consequently, the hacker is unable to establish any correlation among the encrypted picture and the original picture.

Conclusion

This research suggests a method for encrypting medical image using lightweight homomorphic encryption with DNA sequence-based techniques. First, a secret key and several sub-keys are generated using DNA sequences and lightweight operations such as shifting and Josephus ring permutation. Next, partial homomorphic encryption (pailliercryptosystem) and DNA sequence-based encryption are applied for image encryption. The image encryption algorithm includes multiple rounds with simple, lightweight operations (DNA Xor, addition, left and right shifts). The efficacy of the suggested approach is evaluated using different medical images, and the findings demonstrate that the suggestedhDNA_MIE is highly sensitive and secure.

Abbreviations

HDNA_MIE: Homomorphic with DNA-based Medical Image Encryption, JRP: Josephus ring-based permutation, NPCR: Number of Pixels Change Rate, UACI: Unified Average Changing Intensity, MSE: Mean Square Error.

Acknowledgment

The authors would like to express their sincere gratitude to Dr. T. Kokilavani, Assistant Professor, Department of Computer Science, Christ University, Nagasandra, Bangalore, for her invaluable guidance, support, and insightful suggestions throughout the research process. Her expertise and encouragement were instrumental in the successful completion of this work.

The authors would also like to thank S. Lakshmanan, Research Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli and Dr. Joseph Charles P, Assistant Professor and Co-guide, Department of Computer Science, St. Joseph's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli for their contributions and collaborative efforts.

Author Contributions

Lakshmanan S: Conceptualization, Methodology, Software, Investigation and Writing-original paper draft. Kokilavani T: Validation, Supervision and Project Administration. Joseph Charles P: Validation, Formal analysis.

Conflicts of Interest

The authors declare that they have no competing interests.

Ethics Approval

Not applicable.

Funding

No funding received by any government or private concern.

References

1. Darwish A, Hassanien AE, Elhoseny M, Sangaiah AK, Muhammad K. The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open

problems. J Ambient IntellHumanizComput. 2019;10(10):4151-4166.
2. Elhoseny M, Ramírez-González G, Abu-Elnasr OM, Shawkat SA, Arunkumar N, Farouk A. Secure medical data transmission model for IoT-based healthcare systems. IEEE Access. 2018;6:20596-20608.
3. Thakor VA, Razzaque MA, Khandaker MRA. Lightweight cryptography algorithms for resource-constrained IoT devices: A Review, Comparison and Research Opportunities. IEEE Access. 2021;9:28177-28193.
4. Ullah S, Zheng J, Din N, Hussain MT, Ullah F, Yousaf M. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. ComputSci Rev. 2023;47:100530.
5. Tsafack N, Sankar S, Abd-El-Atty B, Kengne J, Jithin KC, Belazi A, Mehmood I, Bashir AK, Song OY, Abd El-Latif AA. A new chaotic map with dynamic analysis and encryption application in internet of health things. IEEE Access. 2020;8:137731-137744.
6. Mfungo DE, Fu X. Fractal-based hybrid cryptosystem: Enhancing image encryption with RSA, homomorphic encryption, and chaotic maps. Entropy. 2023;25(11):1478.
7. Chen Y, Tang C, Ye R. Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Processing. 2019;167:107286.
8. Wang XY, Li P, Zhang YQ, Liu LY, Zhang H, Wang X. A novel color image encryption scheme using DNA permutation based on the Lorenz system. Multimedia Tools and Applications. 2018;77:6243-6265.
9. Nandy N, Banerjee D, Pradhan C. Color image encryption using DNA based cryptography. Int J Inf Technol. 2018;13(2):533-540.
10. Chen J, Chen L, Zhou Y. Cryptanalysis of a DNA-based image encryption scheme. Inf Sci. 2020;520:130-141.
11. Akkasaligar PT, Biradar S. Selective medical image encryption using DNA cryptography. InfSecur J Glob Perspect. 2020;29(2):91-101.
12. Hasan MK, Islam S, Sulaiman R, Khan S, Hashim AHA, Habib S, Islam M, Alyahya S, Ahmed MM, Kamil S, Hassan MA. Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access. 2021;9:47731-47742.
13. Rajendran S, Doraipandian M. Chaos based secure medical image transmission model for IoT-powered healthcare systems. IOP ConfSer Mater Sci Eng. 2021;1022(1):012106.
14. Li M, Pan S, Meng W, Guoyong W, Ji Z, Wang L. Medical image encryption algorithm based on hyper-chaotic system and DNA coding. CognitComput Syst. 2022;4(4):378-390.
15. Yin S, Liu J, Teng L. Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption. Int J NetwSecur. 2020;22(3):421-426.
16. John S, Kumar S. IoT based medical image encryption using linear feedback shift register–Towards ensuring security for teleradiology applications. Meas Sens. 2023;25:100676.
17. Adithya B, Santhi G. A DNA Sequencing Medical Image Encryption System (DMIES) Using Chaos Map and Knight's Travel Map. Int J ReliabQual E-Healthcare. 2022;11(4):1-22.
18. Xie HW, Zhang YZ, Zhang H, Li ZY. Novel medical image cryptogram technology based on segmentation and DNA encoding. Multimedia Tools Appl. 2023;82:27593-27613.
19. Wu Y, Zhang L, Berretti S, Wan S. Medical image encryption by content-aware DNA computing for secure healthcare. IEEE Trans Ind Inform. 2023;19(2):2089-2098.
20. Thabit F, Can O, Alhomdy S, Al-Gaphari GH, Jagtap S. A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. Int J Intell Networks. 2022;3:16-30.
21. Uddin M, Jahan F, Islam MK, Rakib Hassan M. A novel DNA-based key scrambling technique for image encryption. Complex Intell Syst. 2021;7:3241-3258.
22. Patel B, Tandel P, Sanghvi S. Efficient Ballot Casting in Ranked Based Voting System Using Homomorphic Encryption. In: Advances in Computing and Data Sciences: Third International Conference, ICACDS 2019, Ghaziabad, India, April 12–13, 2019, Revised Selected Papers, Part II. Springer Singapore; 2020:565-576. https://link.springer.com/chapter/10.1007/978-981-13-9942-8_53
23. Munjal K, Bhatia R. A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex Intell Syst. 2022;9(4):3759-3786.
24. Zhang X, Wang L, Wang Y, Niu Y, Li Y. An image encryption algorithm based on hyperchaotic system and variable-step Josephus problem. Int J Optics. 2020;2020:6102824.
25. Wang X, Zhu X, Zhang Y. An image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access. 2018;6:23733-23746.
26. Hua Z, Xu B, Jin F, Huang H. Image encryption using Josephus problem and filtering diffusion. IEEE Access. 2019;7:8660-8674.
27. Guan Z, Li J, Huang L, Xiong X, Liu Y, Cai S. A novel and fast encryption system based on improved Josephus scrambling and chaotic mapping. Entropy. 2022;24(3):384.
28. Iqbal N, Hanif M, Abbas S, Khan MA, Rehman ZU. Dynamic 3D scrambled image based RGB image encryption scheme using hyperchaotic system and DNA encoding. J InfSecur Appl. 2021;58(05):102809.
29. Xue X, Jin H, Zhou D, Zhou C. Medical image protection algorithm based on deoxyribonucleic acid chain of dynamic length. Front Genet. 2021;12:654663.
30. National Libray of Medicine, OPENi. https://openi.nlm.nih.gov
31. Sarosh P, Parah SA, Bhat GM. An efficient image encryption scheme for healthcare applications. Multimedia Tools and Applications.2022;81(5):7253-7270.