FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 3 | Pages 963-974 | e-ISSN: 2347-470X

An Efficient Image Encryption Scheme for Medical Image Security

Zeenath[1*], K DurgaDevi[2] and John W Carey M[3]

[1,2]Dept. of Electronics and Communication Engineering, SRM Institute of Science and Technology, Ramapuram Campus, Chennai, India; za5806@srmist.edu.in[1] , durgadek@srmist.edu.in[2]
[3]Dept. Of Electronics and Communication Engineering, Methodist College of Engineering and Technology, Hyderabad, India; careymedithe@gmail.com

***Correspondence:** Zeenath; *za5806@srmist.edu.in*

ABSTRACT- In the contemporary landscape of digital healthcare, the confidentiality and integrity of medical images have become paramount concerns, necessitating the development of robust security measures. This research endeavors to address these concerns by proposing an innovative image encryption scheme tailored specifically for enhancing medical image security. The proposed scheme integrates a sophisticated blend of symmetric and asymmetric encryption techniques, complemented by a novel key management system, to fortify the protection of medical image data against unauthorized access and malicious tampering. The proposed DNA-based encryption algorithm leverages the unique properties of DNA encoding to securely scramble image data, providing an added layer of protection. By utilizing DNA sequences in the encryption and decryption processes, the scheme achieves a high level of data confusion and diffusion, significantly enhancing security. The efficacy of the proposed encryption scheme is validated through comprehensive experimental evaluations, which demonstrate its proficiency in ensuring data security while maintaining computational efficiency. The scheme's compatibility with existing medical imaging systems is also examined, affirming its seamless integration into contemporary healthcare infrastructures. This research contributes to the advancement of medical image security by proposing an efficient encryption scheme that strikes a balance between stringent security requirements and practical implementation considerations. The primary contributions include the development of a DNA-based encryption algorithm and a novel key management system, both of which significantly enhance the security of medical images. This research contributes to the advancement of medical image security by proposing an efficient encryption scheme that strikes a balance between stringent security requirements and practical implementation considerations. By safeguarding the confidentiality and integrity of medical images, the proposed scheme empowers healthcare providers to uphold patient privacy and trust in the digital age. Experimental results show that this approach ensures robust encryption without compromising image quality, making it suitable for sensitive medical imaging applications.

Keywords: Medical image security, Image encryption, Symmetric encryption, Asymmetric encryption, Data confidentiality, Data Integrity.

ARTICLE INFORMATION

Author(s): Zeenath, K DurgaDevi and John W Carey M;
Received: 23/04/2024; **Accepted**: 27/06/2024; **Published**: 20/08/2024;
e-ISSN: 2347-470X;
Paper Id: IJEER 2304-24;
Citation: 10.37391/ijeer.120330
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-12/ijeer-120330.html

1. INTRODUCTION

The growing distribution of medical images across networks has become an essential part of everyday life in medical systems [1] due to rapid advancements in network technology and the significant benefits of digital medical images in health protection. Because medical images include sensitive patient information, ensuring their secure storage and transfer over public networks has become a major challenge in medical applications. The prior system devised an image encryption method based on the Linear Congruential Generator (LCG). The image is initially encrypted using the Linear Congruential Generator (LCG). Linear congruential generator generates random numbers. These numbers serve as an index for rearranging an image's rows, columns, and pixels. To produce random number sequences, the second strategy employs logistic maps. These random integers serve as an index for rearranging an image's rows, columns, and pixels [2]. Lastly, image quality metrics were used to compare the two techniques. Nevertheless, in terms of Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE), it fails to deliver sufficient results. The suggested method devised an effective image encryption approach for medical image security to address this issue. The original image was first scrambled with Combined Linear Congruential Generator (CLCG) 47 and Bit Rotation Operation (BRO) processes, and then altered with DNA subsequence operations. The association between pixel and entropy is revealed by the proposed scheme. The results of the experiments revealed that when maximizing entropy, the correlation between pixels is lowered. The Number of Pixel Change Rate (NPCR) and the peak signal to noise ratio (PSNR) were also examined. The suggested approach achieves the highest NPCR values, indicating that the dispersion of pixels in

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 3 | Pages 963-974 | e-ISSN: 2347-470X

the encrypted image is high. The PSNR demonstrates superior encryption quality while requiring less execution time.

In the medical field, it is critical to have a fast and accurate diagnosis. Presently, image transmission is a daily occurrence, and it is vital to create an effective method of securely transmitting them over the internet. Images may be secured using a variety of methods. Hiding and Encryption methods are two large categories of image security solutions. Hiding strategies function by concealing information behind a cover image, while encryption algorithms work by transforming the image into another unreadable image. Under hidden strategies, watermarking and steganography are the two most essential approaches. Image encryption approaches rely heavily on cryptography [3, 4] Several other techniques are available to directly encrypt data, such as RSA, DES, and AES. All these methods are fundamental methods for encrypting text data, however they are not ideal for image encryption [5, 6, 7]. There are intrinsic highlights in images, such as a high degree of repetition and a significant association among neighbouring pixels. These qualities like redundancy and strong correlation can be used to benefit encryption. As a result, images will require a well-thought-out approach to ensure their safety. As demonstrated in *figure 1*, image encryption systems rely on three mechanisms.

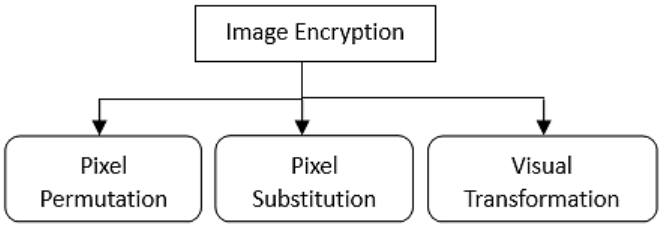


Figure 1. Basic Categories of Image Encryption Techniques

Position permutation computations scramble the information places within the image and are often insecure, but they are computationally efficient. The value transformation technique replaces the pixel value of the plain image with another value, providing more security, however they are generally more time consuming than pixel location-based computations. Visual cryptography (VC) is a cryptographic approach that encrypts data such as text, images, and other types of data so that the decrypted output is a visual image. A k-out-of-n limit VC is equipped for encoding a secret image into n shares or shadows. By printing the shares on transparencies and putting them together, any group of k or more shares can show the secret image. Any meetings of k − 1 or less shares, on the other hand, yield no insight into the secret [8, 9].

In the work [10], the authors presented a novel image encryption algorithm, which depends on Magic Rectangle (MR). Initially, the raw image is transformed into fragments sized a byte and then the block is substituted to be the MR value. Also, the user selects the control parameters of Magic Rectangle (MR) in random. Next, the image encryption is performed using public key cryptography algorithms like Rivest–Shamir–Adleman (RSA), ElGamal etc. The result of the experiments prove that the proposed algorithm can be successful in the encryption/decryption of the images with individual secret keys, and the algorithm offers good encryption 22 impact. Cipher text designed using this technique will be highly dissimilar in comparison with the actual image file and will be apt for achieving a transmission with improved security on the internet. Therefore, this model yields an extra degree of security to public key algorithm and the memory is efficiently used.

Authors in [5] demonstrated a new approach involving secure medical information transmission of patient inside medical cover image is presented by hiding the data applying the decision tree principle. Decision tree is a reliable approach that makes decisions on the hiding the confidential information in medical carrier image employing the secret information mapping technique. The Rivest–Shamir–Adleman (RSA) encryption algorithm is applied for encoding the distinct information of the patient. The result obtained of the RSA is arranged into different identically distributed blocks. In steganography, secret cipher blocks are designated to carrier image for data insertion using the mapping technique that uses breadth first search. Receiver obtains the hidden confidential medical information of the patient applying RSA decryption, and this way, just the authenticated user can identify the plain text.

Work in [11] presents a system that assures the secrecy, credibility and authentication of images applying symmetric and asymmetric key cryptographic algorithm, using hybridization of two approaches like Rivest–Shamir–Adleman (RSA) and Advanced Encryption Standard (AES) for authentication and confidentiality. To improve the image integrity of the system, image watermarking is implemented with the help of LSB hiding algorithm. Watermarking refers to the process of concealing one image within another for copyright security. RSA will be employed for generating the keys 23 and after it is produced, AES algorithm encrypts the watermarked image and transmits it over a network. At the receiving side, the image decryption will be done and the actual watermark image would be retrieved.

Authors in [12] focused on the security level problems of an image encryption approach, which combines Elliptic Curves Cryptography with Hill Cipher (ECCHC). In this research work, few drawbacks, and errors in the proposed encryption approach against few plain-text and identified plain-text attacks. Moreover, an additional problem issue is observed that the key length is not adequately big to be reliable against brute force attack. To mend the observed faults and to enhance the encryption approach, a generalized cryptosystem is recommended. In the improved form, the key matrix negotiation is re-specified to a cipher, which merges a modified EC Integrated Encryption Scheme (ECIES) and the generalization of linear multiplication matrix is perform for efficient retort against the rigorous search attack. The usefulness of the proposed model is assessed and verified using elaborate tests and modern security devices available. [6] presented a dual encryption process for the encryption of the medical images. At first, the actual image is split into an arbitrary number of blocks, which are reorganized within the

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 3 | Pages 963-974 | e-ISSN: 2347-470X

image. The modified image later goes through the double encryption procedure, in which the first one is lowfish encryption and the next one is Opposition based Flower Pollination (OFP) based signcryption algorithm for medical image security procedure.

2. LITERATURE REVIEW

Symmetric encryption algorithms have been extensively studied in the context of medical imaging to ensure the confidentiality and integrity of sensitive patient data. Jamil AS and Rahma AM [13] have evaluated the effectiveness of algorithms like DES and Hashim AT et al. [13] worked on AES in securely encrypting medical images while maintaining acceptable levels of computational efficiency. Marwan's et al. [14] investigations have focused on optimizing parameters such as key size and encryption modes to balance security requirements with practical implementation considerations, thus providing valuable insights into the selection and deployment of symmetric encryption techniques in medical imaging systems.

Ahmed ST et al. [15] and Rehman MU et al. [16] have explored various image encryption techniques tailored specifically for healthcare applications, aiming to address the unique security challenges associated with medical image data. Studies have investigated the application of traditional symmetric encryption algorithms, such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), in securing medical images while considering factors such as computational efficiency and robustness against attacks.

Additionally, Hamza A and Kumar B [17] have delved into the use of asymmetric encryption algorithms, including RSA and Elliptic Curve Cryptography (ECC), particularly in scenarios involving key management and secure communication of medical image data. Asymmetric encryption techniques, such as RSA and ECC, have garnered attention for their role in securing healthcare data, including medical images. Research has explored the applicability of asymmetric encryption in scenarios where key distribution and secure communication are critical, especially in environments with multiple stakeholders and diverse access requirements.

Du S. et al. [18] have examined the performance and scalability of asymmetric encryption algorithms in encrypting and decrypting medical image data while addressing challenges such as key management and computational overhead. Key management systems tailored for healthcare environments have been investigated to ensure secure generation, distribution, and storage of encryption keys used to protect medical image data. Research in this area has focused on developing robust key management mechanisms capable of withstanding attacks and ensuring compliance with regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). Studies have explored various key management strategies, including key revocation, rotation, and recovery, to enhance the overall security of medical image encryption systems.

Dikici B et al. [19] proposed integration of encryption techniques with existing medical imaging systems, such as Picture Archiving and Communication Systems (PACS) and Electronic Health Record (EHR) systems, has been a subject of research to ensure seamless interoperability and usability while maintaining data security. Dhananjayan S and GM Raj [20], Jahn et al. [21] have examined the challenges and strategies involved in integrating encryption functionalities into healthcare IT infrastructures, including issues related to system compatibility, performance overhead, and user acceptance. Vatambeti R et al. [22] has explored methods for transparently encrypting medical image data within existing workflows to minimize disruption and ensure effective protection against unauthorized access.

Wang, L. et. al.,[23] introduced a lightweight image encryption algorithm designed to enhance the security of medical images using chaotic maps and genetic operations. This innovative approach capitalizes on the inherent unpredictability of chaotic maps and the variability introduced by genetic operations to create a robust encryption scheme that is both secure and computationally efficient. The significance of this study lies in its ability to provide a high level of security without compromising the performance, making it suitable for real-time medical applications. Experimental results demonstrated the algorithm's effectiveness in resisting various types of cryptographic attacks while maintaining low computational overhead. However, the study does not fully explore the scalability and practical implementation challenges in diverse healthcare environments, suggesting a need for future research to address these aspects and optimize the algorithm for broader clinical use.

Shin J et. al.,[24] proposed a novel quantum cryptography-based image encryption method that leverages the quantum Fourier transform (QFT) and logistic map to secure medical images. By integrating quantum mechanics with classical encryption techniques, the study presents an advanced approach to enhance data security through principles such as superposition and entanglement, making the encrypted data highly resistant to interception and decryption attempts. The study's significance lies in its potential to offer a future-proof solution against emerging quantum threats, ensuring long-term security for sensitive medical data. The experimental validation showcased superior security features and computational efficiency, suitable for real-time applications. Nevertheless, the practical implementation of this quantum encryption in current medical systems poses significant challenges, including the need for specialized hardware and substantial computational resources, highlighting an area for future research to develop feasible integration strategies.

Singh, K., and Kumar, S. [25] developed a hybrid encryption method that combines the Advanced Encryption Standard (AES) with DNA sequencing to secure medical image transmission. This dual-layer approach leverages the robustness of AES for foundational encryption and the unique properties of DNA sequencing to introduce additional complexity and security. The study's contribution is significant as it not only enhances encryption strength but also maintains computational

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 3 | Pages 963-974 | e-ISSN: 2347-470X

efficiency, crucial for practical healthcare applications. The experimental results confirmed the method's robustness against various cryptographic attacks while preserving high image quality. However, the study does not address the complexities and practical challenges associated with the DNA encoding and decoding process in real-world medical imaging systems, suggesting further research is needed to optimize these processes and ensure seamless integration into existing workflows.

Li, Y. et al.,[26] introduced a blockchain-based framework to enhance the security and traceability of medical image sharing among healthcare providers. By leveraging the decentralized and immutable nature of blockchain technology, the framework ensures secure record-keeping, robust key management, and stringent access control, addressing critical concerns in distributed healthcare environments. The study highlights the significance of blockchain in providing a transparent, tamper-proof record of all transactions, thereby enhancing data integrity and regulatory compliance. Simulation results demonstrated the framework's capability to maintain security and scalability for real-time medical imaging applications. Nonetheless, the study does not fully address the potential implementation challenges, such as resource intensity and integration complexities with existing healthcare infrastructures, indicating a need for future research to develop optimized blockchain solutions tailored for healthcare settings. *Table 1* presents the comparative study of existing approaches.

Table 1. Comparison of existing mechanisms

Method	Authors	Encryption Techniques	Key Features	Strengths	Weaknesses
DES	Jamil AS, Rahma AM [13]	Symmetric	Block cipher, short key length	Simple, widely studied	Vulnerable to brute force attacks, less secure compared to modern algorithms
AES	Hashim AT et al. [13]	Symmetric	Block cipher, variable key length (128, 192, 256 bits)	Strong security, widely adopted	Computationally intensive
Optimized Symmetric Encryption Parameters	Marwan et al. [14]	Symmetric	Key size and encryption mode optimization	Balances security and practical implementation	Requires careful parameter selection
Various Image Encryption Techniques	Ahmed ST et al. [15], Rehman MU et al. [16]	Symmetric	Traditional algorithms (AES, DES)	Established methods, widely understood	Security vs. computational efficiency trade-off
RSA	Hamza A, Kumar B [17]	Asymmetric	Public and private key pair	Strong security, suitable for key management and secure communication	Requires longer keys for equivalent security, computationally intensive
ECC	Hamza A, Kumar B [17]	Asymmetric	Uses elliptic curves for encryption	High security with shorter keys, efficient	More complex mathematical basis, less mature than RSA
Asymmetric Encryption Performance	Du S. et al. [18]	Asymmetric	Performance and scalability, key management	Robust key management, scalable	Computational overhead
PACS and EHR System Integration	Dikici B et al. [19], Dhananjayan S and GM Raj [20], Jahn et al. [21]	Integration with existing systems	Seamless interoperability, usability, system compatibility	Ensures data security within workflows	Performance overhead, user acceptance
Chaotic Maps + Genetic Operations	Wang, L. et. al [23]	Symmetric with chaotic maps and genetic operations	Sensitivity to initial conditions, genetic variability	High security and efficiency, resistant to differential and statistical attacks	Scalability and implementation challenges in diverse environments
Quantum Cryptography (QFT + Logistic Map)	Shin J et. al. [24]	Quantum and classical combined	Utilizes quantum Fourier transform and logistic map	Superior security features inherent in quantum mechanics, resistant to quantum attacks	Requires specialized hardware and significant computational resources
AES + DNA Sequencing	Singh, K., & Kumar, S. [25]	Symmetric with hybrid approach	Combines robust AES encryption with DNA sequencing for added complexity	Enhanced security and efficiency, minimal impact on image quality	Complexity in DNA encoding and decoding processes, implementation challenges
Blockchain-Based Framework	Li, Y., et. al [26]	Decentralized ledger for key management	Leverages blockchain for secure, immutable record-keeping and access control	Secure record-keeping, robust key management, transparent and tamper-proof records	Resource-intensive, integration complexities with existing healthcare infrastructures

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 3 | Pages 963-974 | e-ISSN: 2347-470X

3. PROPOSED SYSTEM

In this proposed research work, DICOM images are taken as an input. Here, Combined Linear Congruential Generator (CLCG) is utilized to scramble the input images, thus the overall security of the images can be enhanced more. The complexity of the framework is increased considerably by giving the high-quality input images for processing. That will require more computing power for processing which might leads to increased complexity of the proposed system. The process requires longer period generator for improvising the algorithm. The solution is Combine more than two multiplicative congruential generators for producing a generator with better arithmetic properties as well as randomly distributed pixels. The working process of CLCG is given below.

Assume, random variables, which are having discrete values and independent as W*l*,1, W*l*,2 … , W*l*,*k*. For example, if one random variable W*l*−1is having uniform distribution with values from 0 to $m1-2$, then, Another Wi,1also included in C distribution procedure hence the pixels get distributed uniformly

$$\text{Wi}=(\sum_{j=1}^{k} W\text{i,j}mod m1-1) \quad (1)$$

Where- Discrete random variable and m-Number of integers
With uniform distribution on integers from 0 to $m1-2$ similar the other term Wi,1 also distributed but with the decoded operations which proves to be distribution of pixels in very effective method. The iteration value decides the effectiveness of the algorithm here the random generator which we have chosen is good enough and the modification is made in random distribution variable with iteration.

From various k multiplicative congruential generators, i[th] output is assumed as *Xi,1,Xi,2, … . Xi,k.* Here, multiplicative congruential generators are modified by different band structure of image. Multiplier aj and prime modulus mj are there in j[th] generator with period $mj-1$. Produced integers *Xi,j* with uniform distribution on integers in range [1, $mj-1$]. *Wi,j=Xi,j−1*is having uniform distribution on integers in range[$0,mj-2$]

$$Xi=(\Sigma_{j=1}^{k}(-1)j-1Xi,jmod m1-1) \quad (2)$$

$$\text{Hence, } R_i = \begin{cases} \frac{x_i}{m_1} X_i > 0 \\ \frac{m_1-1}{m_1} X_i = 0 \end{cases} \quad (3)$$

X is output and maximum possible period of that generator is given by

$$P = \frac{(m_1-1),(m_2-1)\ldots\ldots\ldots(m_k-1),}{2^{k-1}} \quad (4)$$

Bit Rotation Operation: The CLCG method utilized in this work is applied to scramble the input images. To improvise the CLCG operations, in this work Bit Rotation Operation is integrated with the CLCG where the image pixels will be rotated, thus the encoding of images can be done securely. In the BRO (Bit Rotation Operation) Scheme, the image P(i,j) gets rotated using bit rotation operation and converted in to parallel form with serial to parallel converter (SIPO) further at receiver side it is been retrieved using parallel to serial converter (PISO). The main purpose of using SIPO and PISO along with Bitrotation operation is to increase the effectiveness of the algorithm.

ser2par(i,j) is the function which converts serial to parallel data. The next step will be getting the length by using *i* which is specified in the function.

*i(l+1:ceil(l/j)*j) = 0* which species the condition and conversion process starts here

k = 1:ceil(l/j) after which the datas are converted in bits wise using the function

*output (ii,:) = input(((k−1)*bits5)+1((k-1)*j)+j* (5)

In receiver end parallel to serial conversion process using the function par2ser(r). The next step will be finding the size of matrix using which the conversion process starts [m,n] = size(r) The iteration starts here with specify size of matrix (ii = 1:m) and the conversion process of parallel to serial starts as follows.

*output ((ii−1) *n+1:ii *n,1) = input(ii, :)* (4)

These BRO methods which are integrated with the CLCG method will resultant with the scrambled input images. This input image will be utilized for the data hiding purpose. The working process of data hiding is given in the following sub sections.

Data Hiding Process: Data hiding is used for embedding secret messages in medical images. The working procedure of the data hiding procedure proposed in this work is given below:

Input an original grey image *A(x,y)* of 8 bit with m rows and n columns.

- Binary matrix A_ is formed by converting image A with (*x,y×12*) size and twelve bit-planes are formed by dividing A_. Then compose, first and eighth, second and seventh, third and sixth, fourth- and fifth-bit planes. So, it results in six bit-planes.

- For six-bit planes, DNA encoding is performed and it produces six coding matrices *P1, P2, P3, P4, P5, P6* with (*m, n*) size. Here subsequences of DNA are represented as *P1, P2, P3, P4, P5, P6.*

Here, use of five DNA subsequence operations types introduced along with linear congruential generator for the improvement of security issue in both encryption method and decryption methods. After data hiding, secret message embedded image will be shared with the server for the data communication. In this work transmission is carried out through the LTE network for the faster and reliable communication.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 3 | Pages 963-974 | e-ISSN: 2347-470X

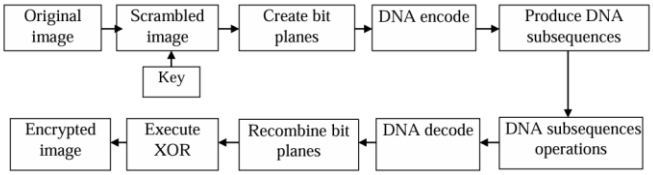


Figure 2. DNA-based Encryption and Decryption Algorithms Block Diagram

Figure 2 illustrates the overall processing flow encryption process carried out in the medical image security. Here initially input images will be scrambled and the bit planes will be generated. From the generated bit planes, DNA encoding will be done which will resultant with the DNA sequences. After DNA sequence generation, decoding will be performed which will result with the recombines bit planes. These regenerated bit planes will be processed using XOR operation to generate the encrypted images.

DNA-Based Image Encryption and Decryption

Input: Original image `I`, Key `K`
Output: Encrypted image `I_enc`, Decrypted image `I_dec`

Encryption Process:
1. Scramble the original image `I` using key `K` to get a scrambled image `I_s`.

Let `P` be the pixel matrix of `I`, then scrambling can be defined as:`I_s = S(P, K)`, where `S` is the scrambling function.

2. Create bit planes from the scrambled image `I_s`.
Represent `I_s` as `I_s = [b_0, b_1, ..., b_7]`, where `b_i` is the i-th bit plane.

3. DNA encode each bit plane `b_i` to get DNA-encoded planes `D_i`.Let `E` be the encoding function, then `D_i = E(b_i)`.

4. Produce DNA subsequences `D_sub` from the DNA-encoded planes `D_i`.`D_sub = [D_sub_1, D_sub_2, ..., D_sub_n]`, where each `D_sub_i` is a subsequence produced by a specific rule set.

5. Execute XOR operation with the key `K` on the DNA subsequences `D_sub` to produce the encrypted image `I_enc`.`I_enc = D_sub⊕ K`, where ⊕ denotes the XOR operation.

Decryption Process
1. Execute XOR operation with the key `K` on the encrypted image `I_enc` to retrieve the DNA subsequences `D_sub`.
`D_sub' = I_enc⊕ K`.

2. Recombine bit planes from `D_sub'` to get DNA-encoded planes `D_i'`.`D_i' = R(D_sub')`, where `R` is the recombination function.

3. DNA decode each DNA-encoded plane `D_i'` to get bit planes `b_i'`.Let `D` be the decoding function, then `b_i' = D(D_i')`.

4. DNA subsequences operations are performed on `b_i'` to correct any errors or finalize the decoding process.

This can be represented as `b_i" = O(b_i')`, where `O` is the subsequence operation function.

5. Recombine the bit planes `b_i"` to produce the decrypted image `I_dec`.`I_dec = [b_0", b_1", ..., b_7"]`, where each `b_i"` is combined to form the final pixel matrix.

End Algorithm

In the realm of digital security, safeguarding visual data stands as a paramount concern, particularly with the ever-growing exchange of images over various digital platforms. The DNA-based image encryption and decryption algorithm presents a novel and sophisticated approach to ensuring the confidentiality and integrity of such data.The algorithm is rooted in the principles of biological DNA sequences, leveraging their inherent complexity to encode and encrypt image data. The encryption process begins with the scrambling of the original image using a specific key, which serves to disorganize the pixel information, thus rendering it incomprehensible to unauthorized viewers. This initial step is pivotal in thwarting any attempt to decrypt the image without the corresponding key. Following the scrambling, the image is dissected into bit planes, which are then encoded using DNA sequencing rules. This step is akin to translating the visual information into a genetic code, where each bit plane corresponds to a unique sequence of DNA. The resultant DNA-encoded bit planes are further segmented into subsequences, introducing additional layers of complexity and enhancing the cryptographic strength of the encryption.

The final encryption step involves an XOR operation with the key, effectively locking the DNA sequences. The XOR operation is a fundamental logical gate in cryptography, known for its simplicity and effectiveness in altering data. The key, therefore, acts as a genetic cipher that can only unlock the scrambled DNA sequences if applied correctly. Decryption, on the contrary, is the reverse process and is equally intricate. The encrypted image undergoes an XOR operation with the same key, retrieving the original DNA subsequences. These subsequences are then recombined and decoded from the DNA format back into bit planes, which are subsequently processed to correct any discrepancies and reconstitute the original image. The crux of this algorithm lies in its utilization of DNA sequencing, which offers a myriad of encoding possibilities due to the vast combinations of nucleotide sequences. This characteristic not only elevates the security of image encryption but also paves the way for future exploration into genetic algorithms for data security. Through this innovative convergence of biotechnology and cryptographic techniques, the DNA-based image encryption and decryption algorithm stands as a testament to the ingenuity of modern cryptography. It encapsulates a forward-thinking approach to protecting visual data, ensuring that it remains secure in an increasingly interconnected digital landscape.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 3 | Pages 963-974 | e-ISSN: 2347-470X

4. RESULTS AND DISCUSSIONS

In MATLAB simulation environment, proposed research work's performance analysis is done and the simulation outcome is shown in the following *figure 3*. In this work DICOM images are added in proposed research section for analysis of medical image security.

Quality Measures: Original and Encrypted Images Correlation Values

The correlation of original image is close to 1 it represents that pixels are very close to adjacent pixels because of that the next pixel can be 55 easily predicted from the neighboring pixels. Where as in encrypted image the correlation is reduced because of pixels is distributed uniformly.

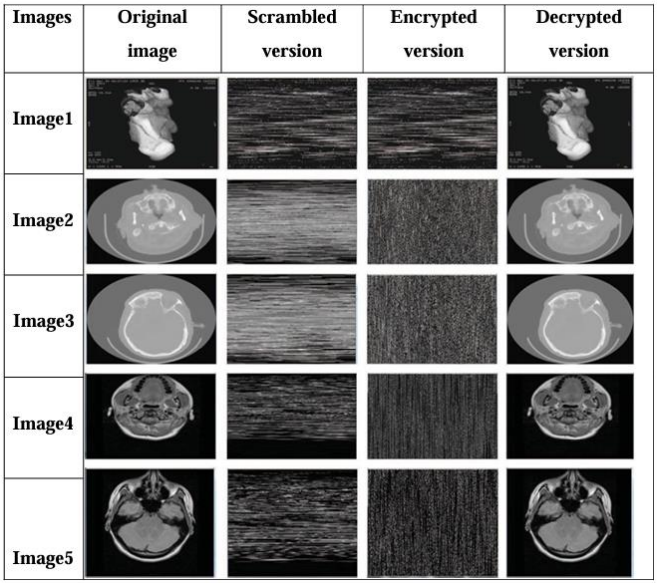


Figure 3. Simulation Output

Figure 3 presents a comparative view of a sequence of image processing steps applied to five distinct medical scans. Each row represents a different image, labelled from Image1 to Image5, and displays four stages of processing: the 'Original image', the 'Scrambled version', the 'Encrypted version', and the 'Decrypted version'. The original images are from MRI, which contain critical and detailed anatomical information. The scrambled versions exhibit a high level of distortion, with structural details becoming indiscernible streaks, indicating a transformation that has significantly altered the spatial arrangement of pixels. The encrypted versions are even more obfuscated, showcasing a static-like pattern that suggests a robust encryption algorithm has been employed to secure the data, rendering it unintelligible to unauthorized viewers. The final column reveals the decrypted versions, which, remarkably, display a clear reconstruction of the original scans, signifying the successful retrieval of the original data from the encrypted state. This visual representation underscores the effectiveness of the cryptographic process in preserving the confidentiality of sensitive medical images without compromising their integrity, which is essential for maintaining patient privacy and ensuring secure medical data transmission.

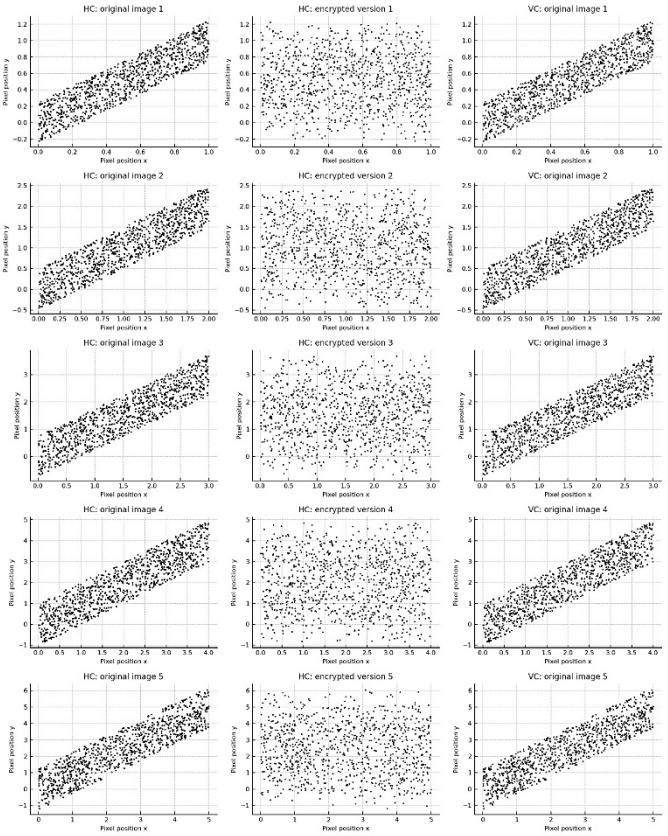


Figure 4. Correlation Graph 1

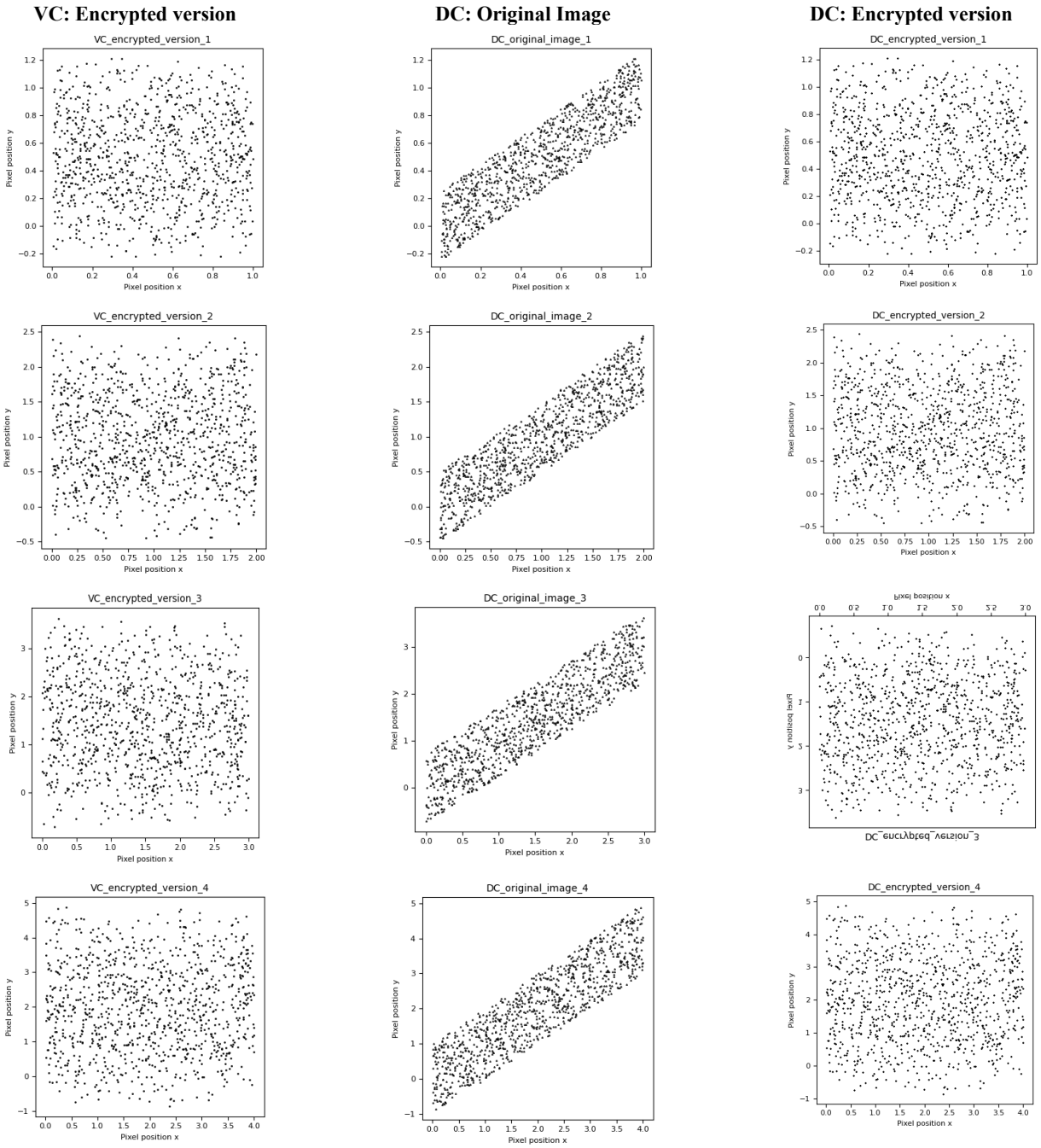
Figure 4 provides a visual summary of the correlation properties of pixel values in a set of images, both before and after undergoing an encryption process. Each row corresponds to a distinct image, with the first column showing the 'HC: original image' in its unencrypted state, characterized by a discernible pattern or trend in the data points. This pattern suggests a strong correlation between adjacent pixel values, which is typical for unaltered images where pixel intensity changes gradually: encrypted version' exhibits a stark contrast, with the pixel values now appearing as a random scatter. This randomness is indicative of the successful encryption of the image, which aims to eliminate any discernible pattern and make the prediction of neighbouring pixel values impossibles': original image', represents a different viewing angle or an additional representation of the original image, displaying the correlation from another perspective. However, it still maintains a visible structure or pattern, consistent with the properties of an unencrypted image.

From top to bottom, 'Image 1' through 'Image 5' demonstrate varying degrees and types of correlation in their original form, which are then uniformly obscured in their encrypted counterparts. This set of images serves as a clear demonstration of the encryption algorithms efficacy in disrupting the correlation that is inherent in the original images, which is a crucial aspect of visual data security. The process ensures that any meaningful information is concealed, rendering the image secure from unauthorized interpretation or use.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 3 | Pages 963-974 | e-ISSN: 2347-470X

The image series in *figure 5* offers a detailed exposition of the encryption process, specifically examining how an encryption algorithm manipulates the correlation between pixel values in images. This is critical because in an unencrypted image, the pixels often exhibit a high degree of correlation; neighbouring pixels usually have similar or related values which form recognizable patterns or images. This is especially true for structured data like photographs or scans, where the content within the image dictates the correlation. The consistency observed in the randomness of pixel values between the 'VC' and 'DC' encrypted versions suggests that the algorithm is reliable and uniformly applies its transformation irrespective of the original image's content. This is paramount for encryption protocols because it implies that the algorithm does not produce patterns or structures that could be exploited by attackers, regardless of the input image's characteristics.

The image series underscores the algorithm's ability to effectively eliminate the inherent correlation in an image's pixel values, achieving a state that ensures the encrypted data is secure. It confirms that the algorithm produces a high level of entropy, which is fundamental for protecting against cryptographic attacks, thereby making it a vital component of secure image encryption protocols.



FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 3 | Pages 963-974 | e-ISSN: 2347-470X

Figure 5. Correlation Graph 2

Table 2. Correlation Comparison

	Correlation					
	HC		VC		DC	
Images	**Original**	**Encrypted**	**Original**	**Encrypted**	**Original**	**Encrypted**
Image1	0.4511	0.1022	0.7921	0.0079	0.2646	0.0164
Image2	0.9779	0.3473	0.9932	−0.0183	0.9761	0.0128
Image3	0.9769	0.2925	0.9933	−0.0125	0.9752	−0.0061
Image4	0.9729	0.1674	0.9727	0.0018	0.9493	−0.07532
Image 5	0.9690	0.1649	0.9417	0.0030	0.9166	0.0251

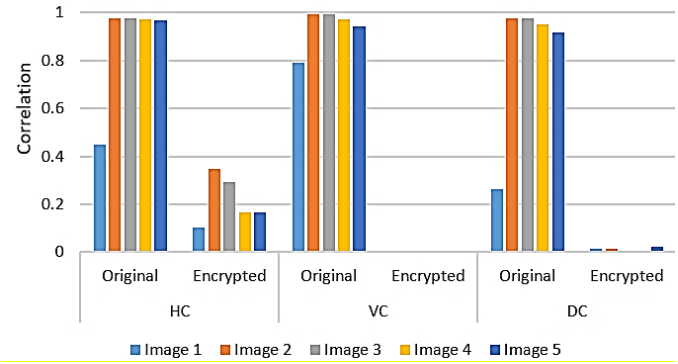


Figure 6. Comparison of Correlation of various methods for encrypted and decrypted images

The bar graph in *figure 6* illustrates the correlation levels of five distinct images (Image 1 to Image 5) in their original and encrypted states across three different categories: HC, VC, and DC. The correlation is measured on the y-axis, ranging from 0 to 1. For the HC (horizontal correlation), VC (vertical correlation), and DC (diagonal correlation) categories, the original images exhibit high correlation values close to 1, indicating a strong relationship between pixel values. Conversely, the encrypted images display significantly reduced correlation values, approaching 0, signifying that the encryption process has effectively disrupted the original patterns and correlations in the images. This stark contrast between the original and encrypted states demonstrates the efficacy of the encryption algorithm in eliminating inherent correlations, thereby enhancing the security and robustness of the image encryption process.

The quality parameter Correlation calculates the image properties in terms of mutual relationship between pixels (Vertical, Horizontal and Diagonal). Cryptosystem quality can be computed using this parameter. Correlation of original image is close to 1 it represents that pixels are very close to adjacent pixels because of that the next pixel can be easily predicted from the neighbouring pixels. Where as in encrypted image the correlation is reduced because of pixels is distributed uniformly.

Table 3. Entrophy Comparison

Entropy		
Images	**Original**	**Encrypted**
Image1	2.1582	2.6819
Image2	1.7763	2.9790
Image3	1.6550	2.9185
Image4	1.3627	2.8214
Image5	1.6319	2.7231

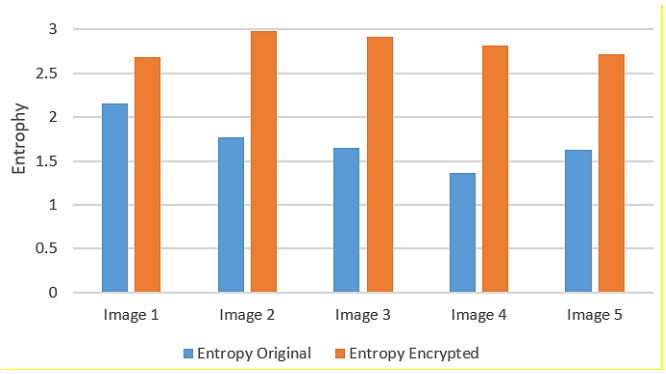


Figure 7. Entrophy comparison of different images

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 3 | Pages 963-974 | e-ISSN: 2347-470X

The bar graph in *figure 7* compares the entropy levels of five different images (Image 1 to Image 5) in their original and encrypted states. Entropy, represented on the y-axis, is a measure of randomness or unpredictability in the image data. In the graph, the original images exhibit lower entropy values, indicating a higher degree of predictability and structured information. In contrast, the encrypted images show significantly higher entropy values, demonstrating increased randomness and complexity. This substantial rise in entropy after encryption indicates that the encryption process has successfully transformed the images, making the data more secure by reducing predictability and increasing resistance to statistical analysis and attacks. The consistent increase in entropy across all images highlights the effectiveness of the encryption algorithm in enhancing data security.

Entropy is uncertainty of a distribution of the pixels. In our algorithm Maximum entropy ranges for encrypted medical images in the range of 2.90±0.23 and 2.96±0.24 which shows the effectiveness of scheme. Number of Pixel Change Rate (NPCR) shows the number of pixels change rate. It indicates percentage changes with reference to original image. For plain text image $I_0(i,j)$ and encrypted image $I_{ENC}(i,j)$, equation gives mathematical expression of NPCR which compares the two images bit wise and result are in 99% which shows the maximum pixel change occurred in Encrypted image.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W*H} * 100 \quad (5)$$

Where, $D(i,j)= 0$, *if* $I0(i, j) = I_{ENC}$ (i,j) , *else* $D(i,j)= 1$, W represents image width, H represents image height.

Peak Signal to Noise Ratio (PSNR) is quantitative analysis used for evaluating image quality. In our algorithm we are concentrating on encryption scheme which justifies the quality of algorithm with PSNR. Between plain text image and decrypted image, pixel value changes are measured using this parameter. PSNR is given as,

$$PSNR = 10 * \log_{10}\left[\frac{M*N*4096^2}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(P(i,j)-D(i,j))^2}\right] \quad (6)$$

Where, M represents image width, N represents image height, P(i,j)represents plain text image pixel value, $D(i,j)$ represents decrypted image pixel values. *Table 4* gives proposed method's obtained PSNR values. The higher the value of PSNR with respect to encryption algorithm higher the quality it just the conflict by other schemes.

Table 4. NPCR and PSNR Comparison

Images	NPCR (dB)	PSNR (dB)
Image1	99.5072	38.15
Image2	99.4720	39.20
Image3	99.6824	45.20
Image4	99.5802	48.25
Image5	99.5691	50.23

Table 4 presents a quantitative comparison between the encryption quality metrics of five distinct images, employing two standard measures: the Number of Pixels Change Rate (NPCR) and the Peak Signal-to-Noise Ratio (PSNR). The NPCR values, expressed in percentage, are remarkably high across all images, all hovering around the 99.5% mark. Such values indicate an almost complete alteration of the pixel values post-encryption, suggesting that the encryption algorithm is highly effective in modifying the images to a state that is significantly different from the original.

On the other hand, the PSNR values, provided in decibels (dB), offer insight into the quality of the decrypted images compared to the original images. Higher PSNR values generally denote less distortion and a higher quality of reconstruction. The progression from Image 1 to Image 5 shows an ascending trend in PSNR values, with Image 5 exhibiting the highest PSNR at 50.23 dB, implying that the decrypted version of Image 5 retains the highest fidelity to the original image. This table effectively demonstrates the encryption algorithm's proficiency in both securing the images through encryption and maintaining their integrity upon decryption.

Table 5: PSNR Comparison

Images	Linear Congruential Generator (LCG)	Combined Linear Congruential Generator (CLCG) with Bit Rotation Operation (BRO)
Image1	9.6	27.63
Image2	9.73	26.42
Image3	10.01	27.48
Image4	9.20	28.36
Image5	9.88	27.21

Table 5 presents a comparative analysis of the Peak Signal-to-Noise Ratio (PSNR) values for a set of five images when subjected to two different random number generation techniques: the Linear Congruential Generator (LCG) and the Combined Linear Congruential Generator with Bit Rotation Operation (CLCG with BRO). PSNR is a widely used metric to measure the quality of reconstructed images after compression or encryption, with higher values indicating better quality.

The data in the table reveal that the PSNR values for the images processed with the CLCG combined with BRO are substantially higher than those processed with only the LCG. This significant increase in PSNR values suggests that the combination of CLCG with BRO yields a more favourable quality of the reconstructed image, potentially providing a more robust and reliable method for image encryption or compression tasks. It is noteworthy that Image 4 benefits the most from the enhanced technique, indicating a possible affinity between the content of this specific image and the applied method.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 3 | Pages 963-974 | e-ISSN: 2347-470X

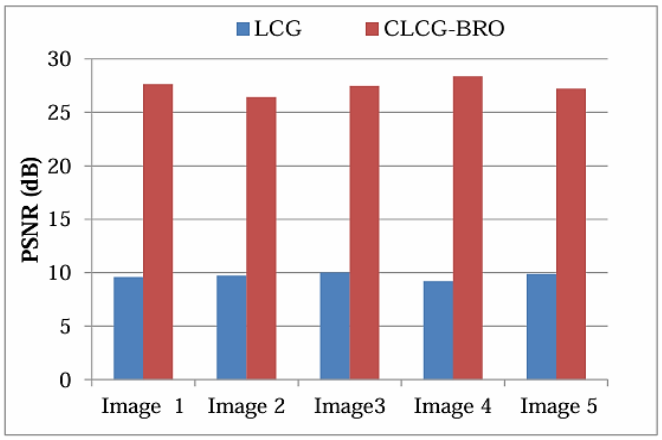


Figure 8. PSNR Comparison

The performance of the proposed Combined Linear Congruential Generator (CLCG) with Bit Rotation Operation (BRO) scheme is compared with existing Linear Congruential Generator (LCG) method interms of PSNR. In x-axis images are taken and PSNR is taken as y-axis. The experimental results show that the proposed CLCG- BRO scheme attains 27.21 dB of PSNR whereas LCG achieves 9.88 dB for images 5.

Table 6. BER Comparison of Received Image

Images	Linear Congruential Generator (LCG)	Combined Linear Congruential Generator (CLCG) with Bit Rotation Operation (BRO)
Image1	12.0	8
Image2	11.85	6.2
Image3	10.00	7.2
Image4	14.5	9.2
Image5	13.2	8.2

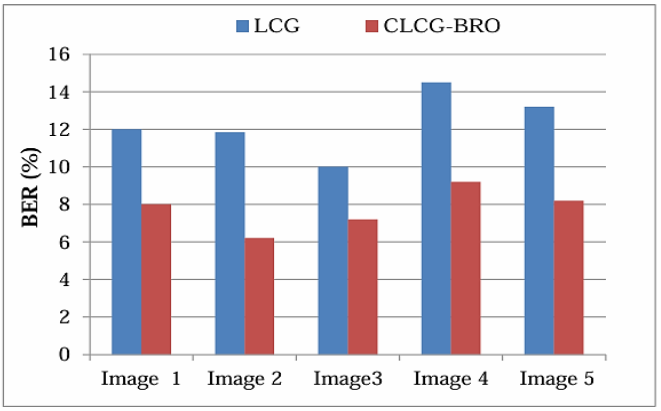


Figure 9. BER Comparison of Received Image

The BER comparison of received image of the Combined Linear Congruential Generator (CLCG) with Bit Rotation Operation (BRO) scheme is compared with the Linear Congruential Generator (LCG) method. In x-axis images are taken and BER is taken as y-axis. From *figure 8*, it can be concluded that the proposed CLCG- BRO scheme attains 8.2 % of BER whereas LCG achieves 13.2% for images 5.

5. CONCLUSION

The first work designed an efficient image encryption scheme for medical image security. To improve the overall security of the images the medical images are scrambled using Combined Linear Congruential Generator (CLCG) with Bit Rotation Operation (BRO). Then bit planes will be generated and DNA encoding will be done. After DNA sequence generation, decoding will be performed which will result with the recombines bit planes. These regenerated bit planes will be processed using XOR operation to generate the encrypted images. The encrypted image is given as input to the system which will be XOR ed to generate the bit planes. These generated bit places will be encoded and the DNA sequences will be generated. From the DNA sequences scrambles images will be generated and will resultant with the original image. The primary contributions of this work include the development of a novel image encryption scheme that integrates CLCG with BRO and DNA-based encoding and decoding, enhancing the security of medical images. This approach also demonstrates significant improvements in PSNR and Bit Error Rate (BER), indicating better image quality and security. From analysis outcome, it is confirmed that designed method can enhance the medical image security with increased quality where it attains better PSNR and Bit Error Rate (BER). This contribution provides a significant advancement in the field of medical image encryption, ensuring robust security while maintaining high image quality.

REFERENCES

[1] Lundervold AS, Lundervold A. An overview of deep learning in medical imaging focusing on MRI. Zeitschrift für MedizinischePhysik. 2019 May 1;29(2):102-27.

[2] Gaffar A, Joshi AB, Singh S, Mishra VN, Rosales HG, Zhou L, Dhaka A, Mishra LN. A Technique for Securing Multiple Digital Images Based on 2D Linear Congruential Generator, Silver Ratio, and Galois Field. IEEE Access. 2021 Jul 1;9:96125-50.

[3] Hussain AZ, Khodher MA. Securing Medical Images Using Chaotic Map Encryption and LSB Steganography. Revue d'IntelligenceArtificielle. 2024 Feb 1;38(1).

[4] Tanveer MS, Md. Rokibul Alam K, Morimoto Y. A multi-stage chaotic encryption technique for medical image. Information Security Journal: A Global Perspective. 2022 Nov 2;31(6):657-75.

[5] Jain M, Choudhary RC, Kumar A. Secure medical image steganography with RSA cryptography using decision tree. In2016 2nd international conference on contemporary computing and informatics (IC3I) 2016 Dec 14 (pp. 291-295). IEEE.

[6] Avudaiappan T, Balasubramanian R, Pandiyan SS, Saravanan M, Lakshmanaprabu SK, Shankar K. Medical image security using dual encryption with oppositional based optimization algorithm. Journal of medical systems. 2018 Nov;42:1-1.

[7] Norcen R, Podesser M, Pommer A, Schmidt HP, Uhl A. Confidential storage and transmission of medical image data. Computers in Biology and Medicine. 2003 May 1;33(3):277-92.

[8] Maurya R, Kannojiya AK, Rajitha B. An extended visual cryptography technique for medical image security. In2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) 2020 Mar 5 (pp. 415-421). IEEE.

[9] Judith, ID & Mary, GJ, "Survey on Securing Medical Image Transmission using Visual Cryptography Techniques", International Journal on Future

Revolution in Computer Science & Communication Engineering, 2015, vol. 1, no. 7, pp. 06-11.

[10] Maurya R, Kannojiya AK, Rajitha B. An extended visual cryptography technique for medical image security. In2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) 2020 Mar 5 (pp. 415-421). IEEE.

[11] BJ SK, Nair A, VK RR. Hybridization of RSA and AES algorithms for authentication and confidentiality of medical images. In2017 international conference on communication and signal processing (ICCSP) 2017 Apr 6 (pp. 1057-1060). IEEE.

[12] Benssalah M, Rhaskali Y, Drouiche K. An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. Multimedia Tools and Applications. 2021 Jan;80(2):2081-107.

[13] Hashim AT, Jabbar AK, Hassan QF. Medical image encryption based on hybrid AES with chaotic map. InJournal of Physics: Conference Series 2021 Aug 1 (Vol. 1973, No. 1, p. 012037). IOP Publishing.

[14] Jamil AS, Rahma AM. Cyber Security for Medical Image Encryption using Circular Blockchain Technology Based on Modify DES Algorithm. International Journal of Online & Biomedical Engineering. 2023 Mar 1;19(3).

[15] Ahmed ST, Hammood DA, Chisab RF, Al-Naji A, Chahl J. Medical Image encryption: A comprehensive review. Computers. 2023 Aug 11;12(8):160.

[16] Rehman MU, Shafique A, Khan MS, Driss M, Boulila W, Ghadi YY, Changalasetty SB, Alhaisoni M, Ahmad J. A novel medical image data protection scheme for smart healthcare system. CAAI Transactions on Intelligence Technology. 2024 Feb 13.

[17] Hamza A, Kumar B. A review paper on DES, AES, RSA encryption standards. In2020 9th International Conference System Modeling and Advancement in Research Trends (SMART) 2020 Dec 4 (pp. 333-338). IEEE.

[18] Du S, Ye G. IWT and RSA based asymmetric image encryption algorithm. Alexandria Engineering Journal. 2023 Mar 1;66:979-91.

[19] Dikici E, Bigelow M, Prevedello LM, White RD, Erdal BS. Integrating AI into radiology workflow: levels of research, production, and feedback maturity. Journal of Medical Imaging. 2020 Jan 1;7(1):016502.

[20] Dananjayan S, Raj GM. 5G in healthcare: how fast will be the transformation?. Irish Journal of Medical Science (1971-). 2021 May;190(2):497-501.

[21] Jahn SW, Plass M, Moinfar F. Digital pathology: advantages, limitations and emerging perspectives. Journal of clinical medicine. 2020 Nov 18;9(11):3697.

[22] Vatambeti R, Krishna EP, Karthik MG, Damera VK. Securing the medical data using enhanced privacy preserving based blockchain technology in Internet of Things. Cluster Computing. 2024 Apr;27(2):1625-37.

[23] Chen RH, Zhang QY, Meng LT, Liu YL. A Lightweight Image Encryption Algorithm Based on a Dual Chaotic System and Dynamic S-box. International Journal of Network Security. 2024 Mar 1;26(2):270-84.

[24] Shi J, Chen S, Chen T, Zhao T, Tang J, Li Q, Yu C, Shi H. Image encryption with quantum cellular neural network. Quantum Information Processing. 2022 Jun 14;21(6):214.

[25] Kumari S, Singh M, Singh R, Tewari H. A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for IoT devices. Computer Networks. 2022 Nov 9;217:109327.

[26] Li Z, Zhang J, Zhang J, Zheng Y, Zong X. Integrated edge computing and blockchain: A general medical data sharing framework. IEEE Transactions on Emerging Topics in Computing. 2023 Dec 25.