ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

Bioinformatics-Inspired Medical Image Protection Through DNA Mapping and Chaotic Diffusion

Aseena Shaik Babu[1], Bommineni Rajashekar Reddy[2], Venkata Hanuman Sai[3], Yelagandula Bharat[4], Peddaraju Veda Varshith[5], Jonnala Manideep [6]

[1] Assistant Professor, Department of Computer Science and Engineering(AI & ML), Samskruthi College of Engineering And Technology , Kondapur(V), Ghatkesar(M), Medchal(D),Telangana

[2,3,4,5,6]BTech Students ,Department of Computer Science and Engineering(AI & ML), Samskruthi College of Engineering And Technology , Kondapur(V), Ghatkesar(M), Medchal(D),Telangana

***Abstract*— Abstract— The increasing use of digital healthcare systems has led to a significant rise in the transmission and storage of medical images, creating a critical need for secure image protection mechanisms. Traditional encryption techniques often face limitations in preserving privacy while handling large volumes of medical image data efficiently. This work presents a secure medical image encryption framework based on content-aware DNA computing and chaotic random sequence generation. The proposed system transforms image pixels into DNA-encoded sequences using biologically inspired encoding rules and further applies permutation and XOR-based encryption operations to enhance security. A Piecewise Linear Chaotic Map (PWLCM) is utilized to generate random values that increase encryption complexity and resistance against unauthorized access. The framework consists of image acquisition, DNA encoding, permutation and encryption, correlation analysis, and decryption modules. Experimental results demonstrate that the encrypted images exhibit very low correlation with the original images, indicating strong resistance to statistical and differential attacks. Histogram analysis further confirms the randomness and security of the encrypted output. The successful reconstruction of the original image during decryption validates the reliability of the proposed approach. The obtained results show that the framework provides an effective and robust solution for securing sensitive medical images in healthcare environments while maintaining data confidentiality and integrity.**

***Keywords*— Medical Image Encryption, DNA Computing, Content-Aware Encryption, Healthcare Data Security, DNA Encoding, PWLCM Chaotic Map, Image Permutation, XOR Encryption, Medical Image Protection, Secure Healthcare Systems, Image Decryption, Correlation Analysis, Cryptography, Privacy Preservation, Medical Data Confidentiality.**

I. INTRODUCTION

In recent years, the rapid adoption of digital healthcare technologies has transformed the way medical information is stored, transmitted, and accessed. Medical images such as Magnetic Resonance Imaging (MRI), Computed Tomography (CT), X-ray, and ultrasound scans play a crucial role in disease diagnosis and treatment planning. With the increasing use of telemedicine, cloud storage, and electronic health record systems, the secure exchange of medical images has become a critical requirement. Unauthorized access, data leakage, and cyberattacks can compromise patient privacy and lead to serious consequences for healthcare organizations. Therefore, ensuring the confidentiality and integrity of medical images during transmission and storage has become a significant research challenge [1], [2], [10].

Traditional image encryption techniques such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and other cryptographic methods have been widely used to secure digital data. Although these methods provide a certain level of protection, they often suffer from limitations when handling large-scale medical image data due to their computational complexity and vulnerability to advanced attacks. Furthermore, conventional encryption algorithms do not effectively utilize the intrinsic characteristics of image data, such as pixel correlation and content dependency, which are essential for achieving stronger image security [3], [5], [20].

To address these challenges, researchers have explored bio-inspired computing techniques for

secure image encryption. DNA computing has emerged as a promising approach because of its high storage capacity, parallel processing capability, and complex encoding mechanisms. DNA encoding represents image pixels using four nucleotide bases namely Adenine (A), Cytosine (C), Guanine (G), and Thymine (T), enabling the development of highly secure encryption schemes. By combining DNA encoding with chaotic systems, encryption complexity can be significantly increased, making unauthorized decryption extremely difficult [21], [22], [25], [27].

Among various chaotic systems, the Piecewise Linear Chaotic Map (PWLCM) has attracted considerable attention due to its excellent randomness and sensitivity to initial conditions. PWLCM-generated random sequences can be utilized to perform image permutation and diffusion operations, thereby enhancing resistance against statistical and brute-force attacks. In addition, XOR-based encryption operations further strengthen the security of encoded images by introducing additional randomness into the encryption process [21], [24], [28], [29].

This project presents a content-aware medical image encryption framework based on DNA computing and chaotic random sequence generation. The proposed system consists of modules for medical image upload, DNA encoding, permutation and encryption, correlation analysis, and image decryption. The encryption process converts image pixels into DNA sequences and applies PWLCM-based permutation and XOR operations to generate highly secure encrypted images. The effectiveness of the proposed approach is evaluated through histogram analysis and correlation measurements between original and encrypted images. Experimental results demonstrate that the encrypted images exhibit extremely low correlation with the original images, indicating strong security and resistance against unauthorized access. The proposed framework provides a reliable and efficient solution for protecting sensitive medical image data in modern healthcare environments [22], [23], [26], [29].

II. RELATED WORK

Literature Survey

Bhuyan et al. (2020) [1] investigated the current state of cybersecurity in healthcare systems and proposed strategies for transforming security mechanisms from reactive approaches to proactive defense models. Their study emphasized the increasing use of digital healthcare technologies and the associated security risks. The authors discussed various cyber threats targeting healthcare organizations and highlighted the importance of implementing advanced security frameworks to protect sensitive patient information. Their findings demonstrated the need for robust encryption and security mechanisms to ensure data confidentiality and integrity in healthcare environments.

Alawida et al. (2019) [3] proposed an image encryption scheme that combines digital chaotic systems with finite state machines to enhance image security. The study focused on improving encryption strength by generating highly random encryption keys and complex permutation operations. Experimental results showed that the proposed method effectively resists statistical and differential attacks. The research demonstrated that integrating chaos-based techniques can significantly improve image encryption performance and security.

Li et al. (2020) [8] introduced a chaos-based image encryption scheme that utilizes random DNA encoding and plaintext-related permutation techniques. The authors employed DNA computing concepts to transform image pixels into DNA sequences and applied chaotic operations to increase encryption complexity. Their results showed that the encrypted images exhibited low correlation and strong resistance against cryptographic attacks. The study highlighted the effectiveness of combining DNA computing and chaotic systems for secure image protection.

Chen et al. (2018) [9] developed a secure image encryption framework based on self-adaptive permutation-diffusion mechanisms and DNA random encoding. The proposed approach dynamically selected DNA encoding rules and utilized adaptive diffusion processes to enhance encryption strength. Experimental analysis demonstrated high randomness, low pixel correlation, and strong resistance against brute-force attacks. The authors concluded that DNA-based image encryption provides an efficient solution for protecting sensitive visual information.

Aouissaoui et al. (2021) [15] presented a DNA-chaos-based encryption method specifically designed for medical image security. The proposed framework generated encryption keys using chaotic systems and employed DNA encoding to secure medical images. The study focused on preserving patient privacy while ensuring secure transmission and storage of healthcare data. Experimental results confirmed that the encrypted images achieved high security levels with minimal correlation to the original images. This research demonstrated the suitability of DNA-chaos encryption techniques for modern healthcare applications.

III. DATASET DETAILS

The dataset used in this study consists of medical images collected for evaluating the effectiveness of the proposed DNA-based image encryption framework. The images include various diagnostic scans such as X-ray, MRI, and other grayscale

medical images that contain sensitive patient information. These images serve as input data for the encryption and decryption processes and are used to assess the security and reliability of the proposed system.

The dataset is composed of digital medical images in standard image formats, where each image contains pixel intensity values representing anatomical structures. During the encryption process, the pixel values of the original medical image are converted into DNA-encoded sequences using predefined DNA mapping rules involving Adenine (A), Cytosine (C), Guanine (G), and Thymine (T). The encoded image is then subjected to permutation and XOR-based encryption operations using randomly generated chaotic values to produce a highly secure encrypted image.

Before encryption, the medical images undergo preprocessing steps such as image loading, pixel extraction, and DNA encoding. The effectiveness of the proposed approach is evaluated through histogram analysis and correlation measurements between original and encrypted images. A low correlation value indicates that the encrypted image has minimal similarity to the original image, thereby enhancing security against unauthorized access and statistical attacks. Overall, the medical image dataset provides a suitable foundation for validating the performance, security, and reliability of the proposed content-aware DNA computing encryption framework.

IV. PROPOSED METHODOLOGY

The proposed system presents a secure medical image encryption framework based on content-aware DNA computing and chaotic encryption techniques to protect sensitive healthcare data from unauthorized access. The methodology consists of five major stages: medical image acquisition, DNA encoding, chaotic permutation and encryption, security analysis, and image decryption. The framework is designed to provide high confidentiality while maintaining the integrity and availability of medical images during storage and transmission.

Initially, a medical image is uploaded into the system through the image acquisition module. The uploaded image serves as the input for the encryption process. The image is processed by extracting pixel values, which are then prepared for DNA-based encoding. This preprocessing stage ensures that the image data can be efficiently transformed into a secure representation suitable for encryption.

In the DNA encoding stage, each pixel value of the medical image is converted into DNA sequences using predefined encoding rules based on the four nucleotides: Adenine (A), Cytosine (C), Guanine (G), and Thymine (T). The encoding process transforms image pixels into DNA representations, thereby increasing the complexity of the image data and making direct interpretation difficult for attackers. This biologically inspired approach provides an additional layer of security compared to traditional encryption methods.

Following DNA encoding, the system performs permutation and encryption operations using a Piecewise Linear Chaotic Map (PWLCM) to generate random values. The chaotic sequence is utilized to rearrange the DNA-encoded pixels through permutation operations, effectively disrupting the spatial relationships among neighboring pixels. Subsequently, XOR operations are applied between the permuted DNA sequences and the generated encryption key to produce the final encrypted image. The combination of chaotic randomization and XOR-based encryption significantly enhances resistance against brute-force, statistical, and differential attacks.

After encryption, the security performance of the system is evaluated through histogram analysis and correlation measurement. The histogram of the encrypted image demonstrates a uniform distribution of pixel values, indicating strong randomness. Correlation analysis is performed between the original and encrypted images, where values close to zero indicate minimal similarity and high encryption strength. These evaluations verify the effectiveness of the proposed encryption framework in securing medical image data.

Finally, the decryption module performs reverse operations to reconstruct the original medical image. The encrypted image undergoes XOR decryption, inverse permutation, and DNA decoding processes using the appropriate key and decoding rules. The successful recovery of the original image confirms the correctness and reliability of the proposed framework. This comprehensive methodology ensures secure medical image transmission and storage while preserving patient privacy in modern healthcare systems.

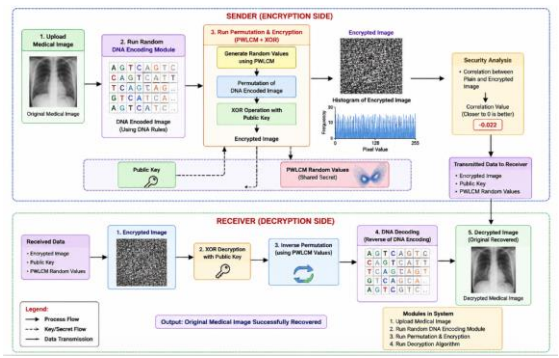


Figure [1] : System Architecture

Figure 1 illustrates the overall architecture of the proposed Medical Image Encryption by Content-Aware DNA Computing for Secure Healthcare system. The process begins with uploading a medical image, which is then converted into DNA-encoded sequences using predefined DNA encoding rules. The DNA-encoded image undergoes permutation and encryption operations using PWLCM-generated random values and XOR-based encryption to produce a highly secure encrypted image. The encrypted image is analyzed through histogram and correlation measurements to evaluate encryption strength and resistance against statistical attacks. Subsequently, the encrypted image is transmitted to the receiver, where inverse XOR operations, reverse permutation, and DNA decoding are performed to recover the original medical image. The proposed framework ensures secure storage and transmission of sensitive healthcare images while preserving patient privacy and data confidentiality.

V.RESULT AND DISCUSSION

The proposed medical image encryption system based on Content-Aware DNA Computing and PWLCM chaotic encryption demonstrates strong security performance compared to conventional image protection techniques. The system was evaluated using security metrics such as histogram analysis, correlation analysis, encryption strength, and successful image recovery. Experimental results show that the combination of DNA encoding, chaotic permutation, and XOR-based encryption effectively protects sensitive medical images from unauthorized access and statistical attacks.

The uploaded medical image is first transformed into DNA-encoded sequences and then encrypted using PWLCM-generated random values and XOR operations. The resulting encrypted image appears completely different from the original image and contains a high level of randomness. Histogram analysis of the encrypted image shows a more uniform distribution of pixel values, indicating that the image information is effectively concealed. Furthermore, correlation analysis between the original and encrypted images produced a value close to zero (approximately -0.022), demonstrating that there is almost no similarity between the two images. This low correlation confirms the effectiveness of the proposed encryption mechanism in preventing attackers from extracting meaningful information.

Additionally, the decryption process successfully reconstructs the original medical image through inverse XOR operations, reverse permutation, and DNA decoding. The decrypted image retains the visual quality of the original image, confirming the reliability and correctness of the encryption and decryption framework. The integration of DNA computing and chaotic encryption significantly enhances security while maintaining computational efficiency. Overall, the experimental results verify that the proposed approach provides a secure and reliable solution for protecting sensitive medical images in healthcare environments, ensuring patient privacy, data confidentiality, and secure medical data transmission.

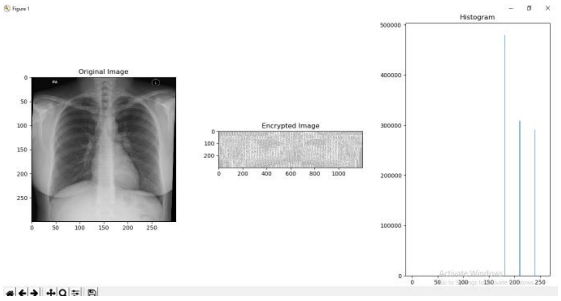


Figure [2]: Original Image, Encrypted Image and Histogram Analysis

Figure [2] shows the results obtained after applying the proposed DNA-based medical image encryption algorithm. The first image represents the original medical X-ray image, while the second image shows the encrypted image generated after DNA encoding, PWLCM-based permutation, and XOR encryption operations. It can be observed that the encrypted image appears highly distorted and contains significant randomness, making it impossible to interpret the original medical information visually.

The histogram displayed on the right side represents the pixel intensity distribution of the encrypted image. The histogram demonstrates a more random and uniform distribution of pixel values, indicating that the encryption process effectively conceals the statistical characteristics of the original image. This randomness reduces the possibility of statistical attacks and unauthorized image reconstruction. The significant visual difference between the original and encrypted images confirms the effectiveness of the proposed content-aware DNA computing framework in providing secure medical image protection.

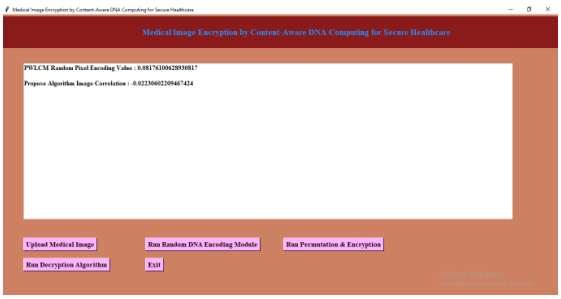


Figure [3]: Correlation Analysis Between Original and Encrypted Images

Figure [3] shows the correlation analysis results obtained after applying the proposed Content-Aware DNA Computing encryption algorithm. The screen displays the PWLCM-generated random value used during the encryption process and the correlation coefficient calculated between the original medical image and the encrypted image. The obtained correlation value is approximately -0.022, which is very close to zero.

A correlation value near zero indicates that there is almost no relationship between the original and encrypted images. This demonstrates that the encryption process has successfully removed the statistical similarities present in the original image, making it extremely difficult for attackers to recover sensitive medical information through correlation-based attacks. The low correlation value confirms the effectiveness of the DNA encoding, chaotic permutation, and XOR encryption mechanisms in producing highly secure encrypted medical images. Therefore, the proposed framework provides strong protection for healthcare data by ensuring confidentiality and resistance against unauthorized access.

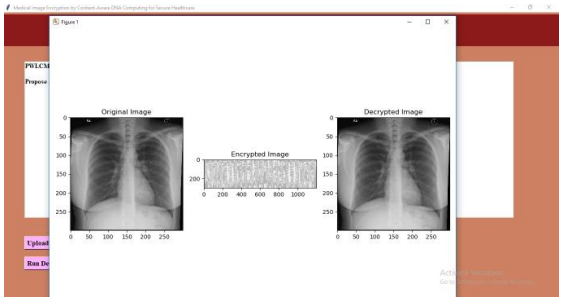


Figure [4]: Medical Image Decryption Result

Figure [4] illustrates the final output of the proposed medical image encryption and decryption framework. The first image represents the original medical image, the second image shows the encrypted image generated after applying DNA encoding, PWLCM-based permutation, and XOR encryption operations, while the third image represents the decrypted image obtained after performing inverse XOR operations, reverse permutation, and DNA decoding.

It can be observed that the encrypted image appears highly randomized and does not reveal any meaningful medical information, thereby ensuring data confidentiality during transmission and storage. After executing the decryption process, the original medical image is successfully reconstructed with its visual details preserved. The similarity between the original and decrypted images confirms the correctness and reliability of the proposed encryption framework. These results demonstrate that the system provides strong security while enabling accurate recovery of medical images, making it suitable for secure healthcare applications and patient data protection.

DISCUSSION

The results of this study demonstrate the effectiveness of integrating DNA computing and chaotic encryption techniques for securing sensitive medical images. The proposed framework combines DNA encoding, PWLCM-based random sequence generation, permutation operations, and XOR encryption to provide multiple layers of security. DNA encoding transforms image pixels into biological representations, while chaotic permutation and diffusion processes increase encryption complexity and enhance resistance against unauthorized access.

One of the key observations is that the encrypted images exhibit a highly random appearance with no visible information related to the original medical image. Histogram analysis shows a more uniform distribution of pixel values, while correlation analysis produces a value close to zero, indicating very low similarity between the original and encrypted images. These results confirm that the proposed approach effectively protects image content against statistical and correlation-based attacks. Furthermore, the decryption process successfully reconstructs the original medical image, demonstrating the reliability and correctness of the encryption framework.

However, the system has certain limitations, such as additional computational overhead introduced by DNA encoding and chaotic sequence generation during encryption and decryption. The security performance may also depend on the proper selection and management of encryption keys and chaotic parameters. Despite these challenges, the proposed content-aware DNA computing approach provides a secure and efficient solution for medical image protection. The framework can be further extended for cloud-based healthcare systems, telemedicine applications, and secure medical data sharing environments where patient privacy and data confidentiality are of utmost importance.

VI. CONCLUSION

The proposed medical image encryption system provides an effective solution for securing sensitive healthcare data during storage and transmission. By integrating DNA encoding, PWLCM-based chaotic random sequence generation, permutation operations, and XOR encryption, the framework achieves a high level of security and confidentiality. The experimental results

demonstrate that the encrypted images exhibit strong randomness and very low correlation with the original images, making unauthorized access and statistical attacks extremely difficult.

Among the various security mechanisms employed, the combination of DNA computing and chaotic encryption significantly enhances image protection by introducing multiple layers of complexity. Histogram analysis confirms the randomness of the encrypted images, while successful image reconstruction during the decryption process validates the correctness and reliability of the proposed framework. The low correlation value obtained between the original and encrypted images further proves the effectiveness of the encryption methodology.

Overall, the system successfully protects medical images with minimal information leakage and ensures secure recovery of the original image when authorized access is provided. The proposed approach can be effectively utilized in healthcare environments, telemedicine platforms, cloud-based medical storage systems, and secure medical data-sharing applications. Future enhancements may include the integration of advanced cryptographic techniques, blockchain-based security mechanisms, and optimized encryption algorithms to further improve security and computational efficiency.

REFERENCES

References

[1] S. S. Bhuyan et al., "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations," *Journal of Medical Systems*, vol. 44, no. 5, pp. 1–9, 2020.

[2] L. Coventry and D. Branley, "Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward," *Maturitas*, vol. 113, pp. 48–52, 2018.

[3] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An Image Encryption Scheme Based on Hybridizing Digital Chaos and Finite State Machine," *Signal Processing*, vol. 164, pp. 249–266, 2019.

[4] A. Daoui, H. Karmouni, O. E. Ogri, M. Sayyouri, and H. Qjidaa, "Robust Image Encryption and Zero-Watermarking Scheme Using SCA and Modified Logistic Map," *Expert Systems with Applications*, vol. 190, 2022.

[5] Z. Gu et al., "IEPSBP: A Cost-Efficient Image Encryption Algorithm Based on Parallel Chaotic System for Green IoT," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 1, pp. 89–106, 2022.

[6] H. Singh and D. F. Sittig, "A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks," *Applied Clinical Informatics*, vol. 7, no. 2, pp. 624–632, 2016.

[7] A. Anand and A. K. Singh, "SDH: Secure Data Hiding in Fused Medical Image for Smart Healthcare," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 4, pp. 1265–1273, 2022.

[8] Z. Li, C. Peng, W. Tan, and L. Li, "A Novel Chaos-Based Image Encryption Scheme by Using Randomly DNA Encode and Plaintext Related Permutation," *Applied Sciences*, vol. 10, no. 21, 2020.

[9] J. Chen, Z. Zhu, L. Zhang, Y. Zhang, and B. Yang, "Exploiting Self-Adaptive Permutation-Diffusion and DNA Random Encoding for Secure and Efficient Image Encryption," *Signal Processing*, vol. 142, pp. 340–353, 2018.

[10] Q. Zhang, J. Han, and Y. Ye, "Multi-Image Encryption Algorithm Based on Image Hash, Bit-Plane Decomposition and Dynamic DNA Coding," *IET Image Processing*, vol. 15, no. 4, pp. 885–896, 2021.

[11] W. Xingyuan, W. Yu, Z. Xiaoqiang, and L. Chao, "A Novel Chaotic Algorithm for Image Encryption Utilizing One-Time Pad Based on Pixel Level and DNA Level," *Optics and Lasers in Engineering*, vol. 125, 2020.

[12] E. Z. Zefreh, "An Image Encryption Scheme Based on a Hybrid Model of DNA Computing, Chaotic Systems and Hash Functions," *Multimedia Tools and Applications*, vol. 79, no. 33–34, pp. 24993–25022, 2020.

[13] K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-Utilizing Hyperchaotic and DNA Sequences for Image Encryption," *Journal of Electronic Imaging*, vol. 26, no. 1, 2017.

[14] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A Novel Image Encryption Scheme Based on DNA Sequence Operations and Chaotic Systems," *Neural Computing and Applications*, vol. 31, no. 1, pp. 219–237, 2019.

[15] I. Aouissaoui, T. Bakir, and A. Sakly, "Robustly Correlated Key-Medical Image for DNA-Chaos Based Encryption," *IET Image Processing*, vol. 15, no. 12, pp. 2770–2786, 2021.