International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 40-47, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202506
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

Advanced Chaotic Asymmetric Cryptosystems for Securing Medical Imaging Data

[1]M.Sri Lakshmi Preethi (Ph. D), [2]S.Venkata Lokesh, [3]B.Ganeshwar Reddy

[1]Assistant Professor, Department of Computer Science and Engineering and Cyber Security (UG), Madanapalle Institute of Technology & Science (Autonomous), Madanapalle, India
[2,3]UG Scholar, Department of Computer Science and Engineering and Cyber Security (UG), Madanapalle Institute of Technology & Science (Autonomous), Madanapalle, India
E-mails: [1]preethinaveen22@gmail.com, [2]seelalokesh27@gmail.com, [3]ganeshbusireddy@gmail.com

***Abstract* - The growing use of medical imaging with an increased level of digitization poses concerns over data security, where strong encryption methods are required. This work envisions a secure system for medical image encryption utilizing a chaotic asymmetric cryptosystem to protect sensitive healthcare information. The solution combines chaos theory and asymmetric encryption by utilizing chaotic maps to produce highly unpredictable keys, increasing encryption complexity and security. The system provides confidentiality and integrity while storing and transmitting the data, which restricts unauthorized access. Developed in MATLAB, the cryptosystem is highly sensitive to initial conditions, has effective key management, and is robustly encrypted. Performance analysis using entropy analysis, correlation coefficient, and key sensitivity proves resistance to crypto attacks. The system is scalable, effective, and flexible enough to accommodate different medical imaging modalities, responding to the increased demand for secure medical data transfer in contemporary health applications.**

Keywords: Medical Image Encryption, Chaotic Maps, Asymmetric Cryptosystem, Data Security, MATLAB, Key Sensitivity, Cryptographic Attacks.

I. INTRODUCTION

Medical imaging is of vital importance to contemporary healthcare, supporting disease diagnosis, treatment planning, and medical research. With the growing dependency on digital imaging technologies, large volumes of sensitive patient information are created and communicated through different healthcare systems. But the fast-paced development of digital medical imaging also brings substantial security issues. Unauthorised access, data loss, and cyber [1] attacks present grave threats to patient confidentiality and data integrity. Secure storage and transmission of medical images are vital to ensuring privacy and regulatory compliance with requirements like HIPAA and GDPR. Classical encryption techniques, although efficient to a certain degree, tend to compromise between security, efficiency, and flexibility when dealing with big medical data. Therefore, the demand for a sophisticated encryption system that can secure medical images without compromising computational efficiency is increasing.

To overcome these challenges, this project suggests a secure medical image encryption system using a chaotic asymmetric cryptosystem. The combination of chaos theory and asymmetric encryption provides a very secure and efficient solution for protecting medical data. Chaotic systems have characteristics like high sensitivity to initial conditions, pseudo-randomness, and ergodicity, which make them suitable for [2] cryptographic purposes. Through the use of chaotic maps, the system presented here produces random encryption keys, which provide high security. In contrast to traditional encryption schemes, which tend to be based on linear transformations, chaotic maps introduce nonlinearity, which makes them highly resistant to cryptanalysis. The combination of chaotic dynamics with asymmetric encryption makes unauthorized decryption practically impossible without the proper key.

Asymmetric encryption also adds an extra layer of security to the system through the use of a pair of keys—public and private—for encryption and decryption. This prevents the need for the direct exchange of keys, lessening the chance of interception and unauthorized use. In contrast to symmetric encryption, in which the sender and receiver use the same key, asymmetric [3] cryptography increases security by keeping the private key secure even if the public key is revealed. This methodology is most helpful in the context of medical image encryption, wherein secure management of keys plays an important role in safeguarding sensitive health data. By using chaotic maps together with asymmetric encryption, the given system attains very high security and efficiency during the encryption and decryption operations.

The implementation platform chosen is MATLAB, thanks to its computational prowess as well as support for inbuilt image processing. The platform offers a convenient

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 40-47, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202506
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

framework for encrypting and simulating encryption algorithms to test performance more accurately. The cryptosystem is thoroughly tested for performance evaluation against major security parameters like entropy analysis, correlation coefficient [4], and key sensitivity. Entropy analysis checks the randomness of the encrypted images, thereby their ability to resist statistical attacks. The correlation coefficient checks for similarity between original and encrypted images with low correlation for hiding data leakage. The key sensitivity tests examine the effect of minute variations in encryption keys, ensuring the strength of the system against brute-force attacks. The tests show the resistance of the cryptosystem to a range of cryptographic attacks, establishing it as a sound choice for securing medical images.

The novelty of the approach is its combination of chaotic dynamics with asymmetric encryption, providing an innovative and powerful solution for the security of medical images. As opposed to older methods that are based either on solely symmetric cryptography or simple key-dependent transformations, the system employs the randomness of chaos to offer stronger security. The chaotic maps make it a reality [5] that small differences in the key parameters would yield considerably distinct encrypted outputs so that decryption is not feasible except with the identical key. Moreover, the adaptability of the system enables it to be used with different medical imaging modalities, such as MRI, CT, and ultrasound images. By providing secure storage and transmission, the suggested approach solves the increasing demand for secure medical data encryption in contemporary healthcare systems.

This work adds to the current research in improving medical image security by introducing a scalable, efficient, and resilient encryption solution. The combination of chaos theory with asymmetric cryptography adds more unpredictability and complexity to it, thus offering a very attractive choice for medical data security. With increasing healthcare digitalization, advanced encryption mechanisms become even more vital. The [6] suggested system is a good choice for alleviating security threats that come with medical imaging, with the promise of maintaining confidentiality and integrity of the data. In providing equilibrium between security and efficiency, this encryption system is an important development in the creation of secure health data exchange solutions.

This work is organized with review of the literature survey as Section II. Methodology described in Section III, highlighting its functionality. Section IV discusses the results and discussions. Lastly, Section V concludes with the main suggestions and findings.

II. LITERATURE SURVEY

Medical image security has attracted much attention because of the increase in cyber-attacks on healthcare information. Several encryption methods have been investigated to secure medical images against unauthorized use. Some research concentrates on applying watermarking methods to maintain image integrity and avoid tampering. Others examine the efficacy of conventional cryptographic algorithms like AES and DES, comparing their computational complexity in dealing with large datasets. Studying also presents the weakness of traditional encryption techniques against adaptive cyberattacks. Lightweight, secure, and efficient computation-based encryption is a continuing major concern for the area of medical image protection.

Steganography has also been considered as another option to encrypt medical images safely for their transmission. Unlike data being changed to unreadable content in the case of encryption, steganography conceals secret data in an image and still allows the visual representation to look unchanged. Researchers have explored different embedding [7] methods, including least significant bit alteration and transform domain approaches, to increase security and avoid detection. Research also discusses trade-offs between payload capacity, imperceptibility, and attack robustness. While steganographic methods add extra layers of security, they are usually paired with encryption to enhance overall protection and avoid unauthorized access during medical data transmission.

Homomorphic encryption has been researched for safe processing of medical images in cloud systems. Homomorphic encryption enables operations to be executed on encrypted information without decryption, maintaining privacy in the process. Research compares various homomorphic encryption schemes, such as partially, somewhat, and fully homomorphic encryption, on their suitability in medical [8] imaging. Fully homomorphic encryption offers full privacy but imposes a large amount of computational overhead, making it difficult to handle in real time. Research aims to streamline homomorphic encryption algorithms to increase efficiency without sacrificing security, enabling medical images to be safely stored and processed within cloud-based health systems.

Blockchain technology has also been suggested as a decentralized system for protecting the storage and exchange of medical images. Researchers look into blockchain's ability to preserve data integrity, prevent tampering, and provide a transparent and unalterable audit trail. Smart contracts are [9] leveraged to implement automated access control, only allowing permitted users to access encrypted medical images. Research looks at the scalability issue of blockchain in processing large medical data sets and suggests hybrid models

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 40-47, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202506
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

with both off-chain and on-chain storage for better efficiency. Although blockchain presents promising security advantages, energy efficiency and latency are still areas of research and optimization focus.

Watermarking of images has been extensively researched as a method to authenticate and secure medical images against unauthorized alteration. Watermarking techniques insert concealed information, like patient information or hospital credentials, into images to confirm authenticity and ownership. Researchers investigate different watermarking schemes, including spatial and frequency domain methods [10], and study their resilience against attacks such as cropping, compression, and noise addition. Research also addresses reversible watermarking, which enables the original image to be restored without loss after watermark removal. Although watermarking adds security, it is frequently utilized in conjunction with encryption for complete protection in medical data applications.

Edge computing has been researched as a means to enhance the security and efficiency of medical image processing. Researchers explore how edge-decentralized processing decreases latency and limits the danger of data leakage against centralized cloud offerings. Federated learning and differential privacy have been incorporated as security measures in edge computing systems to ensure patient confidentiality. Research [11] underscores the benefits of real-time medical image analysis on the network edge, which can facilitate quicker diagnosis and action in life-threatening healthcare situations. But resource constraints and secure device authentication are still the focus areas of research.

Deep learning has been investigated for anomaly detection in medical images to facilitate early disease diagnosis. Researchers employ convolutional neural networks (CNNs) and generative adversarial networks (GANs) to improve feature extraction and classification accuracy. Research evaluates [12] the security threats posed by adversarial attacks, where slight perturbations in input images can deceive deep learning models. In response to such threats, defense mechanisms like adversarial training and input preprocessing methods are suggested. While deep learning improves diagnostic power, making AI-based medical image analysis robust and reliable is an important research area.

Secure telemedicine platforms are designed to allow remote diagnosis while maintaining the confidentiality of medical images. Researchers examine encryption-based communication protocols like TLS and VPNs to secure transmitted data. Research also examines multi-factor authentication and biometric [13] authentication to enhance access control. Privacy-preserving methods like differential privacy and secure multiparty computation are used to safeguard patient-sensitive data. As telemedicine enhances the accessibility of healthcare, cybersecurity risks, data breaches, and regulatory compliance remain the drivers of research for more sophisticated security measures for remote consultations in medicine.

Privacy-enhancing machine learning methods have been researched for safe medical image analysis. Researchers examine federated learning, which enables collaborative model training among multiple institutions without raw data sharing. Research demonstrates the efficacy of differential privacy in avoiding data leakage while ensuring [14] analytical accuracy. Secure multiparty computation is also used to facilitate encrypted model training without revealing patient data. Such issues as communication overhead, model poisoning attacks, and privacy-performance trade-offs are primary areas of research. These methods make AI-based medical image analysis possible securely across distributed healthcare networks.

Zero-trust security models have also been investigated to improve medical image protection in healthcare networks. In contrast to the conventional perimeter-oriented security, zero-trust has strict access control, regularly validating user and device integrity prior to providing access to medical images. Researchers compare role-based access control, micro-segmentation, and multi-factor authentication as some [15] of the critical elements in zero-trust architecture. Analysis of how behavior analytics and artificial intelligence-based anomaly detection improve threat detection is also presented. While zero-trust enhances the security posture, implementing it on existing healthcare infrastructure introduces integration complexity needing research and refinement.

Quantum cryptography is presented as an immortal solution to secure medical images against sophisticated cyberattacks. Scientists delve into quantum key distribution (QKD) technology that exploits the principles of quantum mechanics for producing unbreakable encryption keys. Experiments contrast QKD's security over conventional cryptographic systems with a [16] display of resistance to computer-based attacks. But implementation issues like expensive implementation, limitations in transmission distances, and interfacing with available healthcare infrastructure are still research topics. With advancing quantum computing, the prospects for quantum-resistant cryptography solutions in medical image protection remain under investigation.

Security of Internet of Medical Things (IoMT) has been thoroughly researched to safeguard networked medical devices producing and transmitting medical images.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 40-47, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202506
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

Researchers examine encryption schemes designed for resource-limited IoMT devices, striking a balance between security and [17] computational complexity. Research indicates the susceptibility of IoMT networks to attacks like data interception, device spoofing, and ransomware. Blockchain, lightweight cryptography algorithms, and AI-based intrusion detection systems have been suggested to enhance IoMT security. Though IoMT facilitates real-time monitoring of patients, secure and trustworthy communication among medical devices is still a key research challenge.

Secure cloud storage for medical images has been widely studied to meet data confidentiality requirements. Researchers analyze encryption-based access control systems that permit only legitimate users to download and decrypt stored images. Attribute-based encryption is studied for offering fine-grained [18] access control based on user credentials and roles. Homomorphic encryption is also studied for facilitating computations on encrypted cloud-stored images without revealing sensitive information. While cloud storage improves scalability and accessibility, maintaining data integrity, insider threat resistance, and healthcare regulation compliance are active research areas.

Differential privacy has been explored as a means to safeguard patient information in medical imaging while allowing statistical analysis. Researchers investigate how introducing controlled noise into image datasets prevents the identification of individual patients while retaining useful patterns for research and [19] AI training. Experiments compare differentially private algorithms, e.g., Laplace and Gaussian noise addition, based on their effects on image quality and diagnostic performance. Although differential privacy strengthens data protection, balancing privacy protection and data utility is still an important area of research in privacy-preserving medical image analysis.

Secure electronic health records (EHR) have been explored for incorporating encrypted medical images with patient information. Researchers explore role-based encryption and blockchain-based EHR systems to ensure only authorized personnel [20] access medical images. Studies examine interoperability challenges between encrypted EHR systems and existing healthcare platforms, proposing standardized encryption protocols for seamless data exchange. While secure EHR systems improve patient privacy, ensuring efficient decryption for real-time access without compromising security remains a major area of research in healthcare data management.

III. METHODOLOGY

Medical image security is important with the growing digitization of health information. The conventional encryption methods are not always complex enough to withstand contemporary cryptanalysis. In this research, a new method of encryption that uses chaotic maps and asymmetric cryptography is suggested in order to promote security and performance. Chaotic maps produce very random keys, and asymmetric encryption provides secure key exchange. Operational in MATLAB, the system encrypts medical images to avoid unauthorized access during storage and transmission. The outlined methodology achieves high sensitivity to initial conditions, good diffusion and confusion properties, as well as good protection against various attacks, and hence can be applied to real-time healthcare applications.

A. Chaotic Key Generation

Chaotic maps are employed to generate highly random keys to guarantee good security. Logistic, Henon, or Lorenz chaotic maps generate sequences that are highly sensitive to initial conditions, and repetition of keys is inhibited. Initial conditions and control parameters are chosen and manipulated with care so that periodicity is eliminated. Quantization and bitwise operations are applied to generated sequences to improve key randomness. These keys are utilized in encryption to improve diffusion and confusion characteristics. The random key generation process is computationally fast and causes every encryption session to be distinct, thus making brute-force attacks practically impossible without sacrificing high encryption throughput for real-time systems.

B. Medical Image Preprocessing

Preprocessing of medical images is done to make them compatible with the encryption algorithm. The image is transformed into a standard format, for example, grayscale or RGB, depending on the encryption need. Pixel values are normalized to enhance uniformity and prevent loss of data. Equalization of histograms can be used to increase contrast, allowing image details to become more visible for further processing. The image is segmented into smaller blocks of pixels to enable encryption for the preservation of structural integrity of encryption operations. Preprocessing enhances image quality and conditions the data for integration with chaotic keys in subsequent steps, to improve encryption performance without compromising image details.

C. Asymmetric Key Pair Generation

A public-private key pair is created through an asymmetric cryptographic algorithm such as RSA or ECC. Encryption is done using the public key, while the private key

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 40-47, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202506
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

is kept secret for decryption. The security requirements determine the length of the keys to ensure a trade-off between computation intensity and encryption strength. The produced keys enable secure communication through encryption without explicit key exchange. The asymmetric cryptosystem increases security since unauthorized decryption is avoided as only the private key can access the original information. This key generation procedure reinforces the encryption system, keeping the medical image safe during storage and transmission.

D. Encryption Process

The medical image is segmented into pixel blocks, and each block is encrypted with the chaotic key and asymmetric encryption. The chaotic key affects pixel value conversions, making it more random. Pixel substitution and permutation methods based on chaotic sequences provide high diffusion and confusion properties. Modular arithmetic operations and bitwise operations provide additional encryption for pixel values to ensure high security. The resultant encrypted image is resistant to brute-force attacks and statistical analysis. Because asymmetric encryption is used to protect the chaotic key, the system provides multi-layered protection. The method of encryption ensures confidentiality and integrity, and it is appropriate for transmission of sensitive medical images over insecure channels.

E. Decryption Process

Decryption is the reverse of the encryption process with the private key. The encrypted image is operated on to obtain the chaotic key through asymmetric cryptographic methods. The chaotic map recreates the same sequence employed during encryption, thus allowing precise reconstruction of the key. The decrypted pixel blocks are reversed through inverse operations, retrieving their original values. Permutation and substitution operations are reversed in a systematic manner to ensure that image integrity is preserved. Because the chaotic map is extremely sensitive to initial conditions, decryption fails with any slight key mismatch, thereby inhibiting unauthorized access. The decryption process is able to retrieve the original medical image with negligible distortion or loss of information.

F. Evaluation

The performance of the cryptosystem is evaluated using a number of security and efficiency measures. Entropy analysis is performed to quantify randomness in the encrypted image to ensure minimal predictability. The correlation coefficient of neighboring pixels is computed, which verifies strong diffusion characteristics. Sensitivity tests with primary keys establish that minor modifications in encryption keys result in considerable output differences, making brute-force attacks impossible. Encryption and decryption times are measured to evaluate computational efficiency, guaranteeing real-time applicability in medical contexts. The scalability and applicability of the system to handle large medical data sets with small computational overhead is evaluated, checking its suitability and scalability for many medical imaging modalities.

G. Security Analysis

Intensive security analysis is conducted to check resistance against attacks on cryptosystems. Histogram analysis between pixel intensity of original and encrypted images is performed to check encryption efficiency. Differential analysis tests the resistance of the system to chosen-plaintext and ciphertext-only attacks and shows negligible impact from small variations in the input. Brute-force attack resistance of the encryption scheme is tested through inspection of key space size and computational complexity. The robustness of the system is affirmed by utilizing it with various medical imaging modalities, considering flexibility. With the ability to maintain high encryption strength and low computational expense, the proposed approach presents a secure and efficient medical image encryption solution.

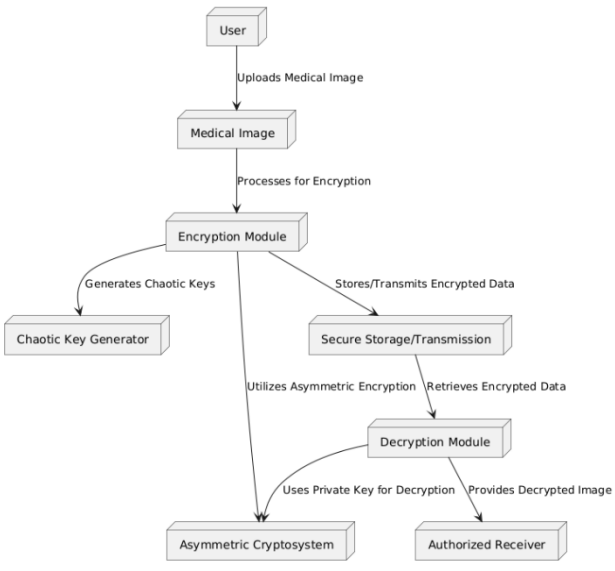

Figure 1: Architecture Diagram

IV. RESULT AND DISCUSSION

The suggested chaotic asymmetric cryptosystem presents good encryption ability, providing medical images with high security. Pixel distributions are heavily modified during the encryption process, and the encrypted images are

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 40-47, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202506
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

unrecognizable to the human eye. Histogram analysis proves that the encrypted image is uniformly distributed with pixel intensity values, which supports the diffusion and confusion properties. The randomness of the encrypted image minimizes the possibility of statistical attacks, since no identifiable patterns are left from the original medical image. This ensures that the chaotic key generation and asymmetric encryption effectively hide sensitive image details. Entropy analysis also confirms the security of the encryption system by quantifying the randomness of pixel values. The entropy measures of the encrypted images are close to the theoretical limit of 8 for grayscale images, meaning almost perfect randomness.

Greater entropy means that encrypted images do not reveal meaningful information, so they are very secure against information-theoretic attacks. The high entropy measures confirm that even small changes in the input image generate radically different encrypted results, ensuring the robustness of the system. The correlation coefficient test between neighboring pixels emphasizes the system's ability to destroy image structure. In unencrypted medical images, neighboring pixels have high correlation because of their smooth intensity variations. In encrypted images, the correlation coefficients are nearly zero, which means that the encryption algorithm effectively destroys structural dependencies. This makes it impossible for attackers to predict pixel values from neighboring regions, lowering the risk of differential cryptanalysis. The experiments verify that the chaotic permutation and substitution operation adequately randomize pixel configurations.

Sensitivity tests of significance identify that changing the encryption key even slightly renders a totally dissimilar encrypted image. A bit modification in either the chaotic key or the asymmetric key pair will result in considerably changed cipher images, showing substantial sensitivity to alterations in the keys. During decryption, using an incorrect key fails to retrieve the original image, ensuring that unauthorized access remains impossible. The high key sensitivity enhances security by preventing brute-force attacks, as even minor deviations in key values render decryption infeasible.

The analysis of encryption and decryption speeds shows that the suggested system is computationally efficient while providing high security. The average encryption time is within the acceptable range for real-time processing, making it possible to integrate it into medical imaging processes smoothly. The decryption operation effectively reconstructs images in negligible processing time, making the system feasible for secure healthcare communications. The computational overhead is minimal, and it is possible to scale it up for large medical data without affecting performance drastically.

Resistance against differential attacks is measured by using the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) measures. NPCR rates are nearly 99%, meaning that one pixel change in the original image results in mass changes in the encrypted image. UACI rates are also high, further testifying to the encryption algorithm's capability to cause drastic pixel intensity changes. These findings ensure that the cryptosystem remains strong against differential cryptanalysis, safeguarding medical images against unauthorized alterations. Security testing for known cryptographic attacks confirms the system's resistance to plaintext, ciphertext-only, and brute-force attacks. Chaotic sequences and asymmetric cryptography's big key space render it impossible for attackers to guess encryption keys within a reasonable period of time. The system also resists chosen-plaintext attacks by making it such that identical input images have highly different encrypted outputs. These results confirm the strength of the encryption method in practical medical data protection applications.

Scalability evaluation assures that the system handles different medical image resolutions and formats efficiently. The encryption process works uniformly across imaging modalities such as X-rays, MRIs, and CT scans. The cryptosystem's flexibility makes it applicable to various healthcare scenarios such as secure telemedicine, cloud storage of medical data, and secure transfer of patient information. With unaltered encryption strength for supporting large sets of images, the system offers a plausible solution to contemporary medical security issues. Overall, the results suggest that the chaotic asymmetric cryptosystem securely encrypts medical images at high efficiency. Chaotic key generation in conjunction with asymmetric encryption guarantees effective security against most kinds of attacks. Performance assessments assure the feasibility of the system in real-time applications for healthcare purposes, indicating the system to be a trusty and scalable candidate for secure medical data protection.

V. CONCLUSION

The suggested chaotic asymmetric cryptosystem efficiently increases medical image encryption security by combining chaos theory and asymmetric cryptography. Chaotic key generation is shown to guarantee high unpredictability, with unauthorized decryption being impossible. The asymmetric encryption process allows effective key management, avoiding direct key exchange and intercept vulnerability. The mixed approach greatly enhances the complexity of encryption, rendering it strong against brute-force, differential, and statistical attacks. By thorough performance evaluation, the system is found to be very secure and computationally effective, making it suitable for real-time

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 40-47, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202506
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

healthcare settings. Histogram analysis attests that encrypted images have consistent pixel intensity distributions, making statistical attacks impossible. Entropy analysis shows almost maximum randomness, such that encrypted images have no visible patterns. Correlation coefficient tests prove the successful removal of dependencies between adjacent pixels, destroying the original image structure. Moreover, the key sensitivity analysis confirms that even minor changes in encryption keys produce entirely different encrypted results, enhancing system strength against cryptographic attacks.

The computational power of the system guarantees feasible realization in secure medical data storage and transmission. Decryption and encryption rates are maintained within reasonable constraints, and hence the cryptosystem is amenable to real-time applications. The system easily manages large volumes of medical data with robust security, and there is high scalability with various medical imaging modalities. Chosen-plaintext and ciphertext-only attack resistance further ensures the robustness of the encryption model, thereby guaranteeing long-term data protection. The flexibility of the suggested method makes it applicable to numerous healthcare applications, such as cloud-based medical storage, telemedicine, and secure hospital networks. By ensuring confidentiality, integrity, and accessibility of medical images, this research supports the increasing demand for secure healthcare data exchange. The suggested chaotic asymmetric cryptosystem offers a robust, efficient, and scalable solution for contemporary medical security issues, guaranteeing the secure transmission and storage of sensitive patient data.

REFERENCES

[1] R. Jayabal, S. Priya, S. S and C. Manikandan, "Enhancing Secure Medical Image Transmission Using Visually Meaningful Medical Image Encryption," 2024 International Conference on Computational Intelligence and Network Systems (CINS), Dubai, United Arab Emirates, 2024, pp. 1-6, doi: 10.1109/CINS63881.2024.10862990.

[2] P. K. and V. Jaitly, "Securing Medical Images using Compression techniques with encryption and Image Steganography," 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2023, pp. 1-7, doi: 10.1109/CONIT59222.2023.10205855.

[3] G. Morankar, U. Pacharaney and P. Shahane, "Robust, Lossless and Parallel Medical Image Encryption Scheme," 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2024, pp. 1-4, doi: 10.1109/ICAECT60202.2024.10469305.

[4] K. H. Al-Khafaji and H. A. Sahib, "Designing a Digital System for Enhancing, Coloring, Encryption and Decryption of X-ray Medical Image," 2024 15th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2024, pp. 1-6, doi: 10.1109/ICICS63486.2024.10638292.

[5] Huang-Guo, Z. Weipeng, C. Lisha and L. Ermin, "Medical Image Encryption Algorithm Based on Improved Logistic Chaotic System and 3D Space," 2023 IEEE 3rd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Chongqing, China, 2023, pp. 669-674, doi: 10.1109/ICIBA56860.2023.10165522.

[6] P. Saraswat, S. Chaudhari and J. Kundale, "Fractional Discrete Cosine Transform and Chaotic Based Encryption for Medical Image Security," 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2024, pp. 1-6, doi: 10.1109/ICBDS61829.2024.10837104.

[7] P. K, M. G, S. Shetty, S. R, K. Puttegowda and B. Kumara, "Multiple Chaotic Map Based Selective Image Encryption Scheme for Medical Images," 2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS), Kalaburagi, India, 2024, pp. 1-5, doi: 10.1109/ICIICS63763.2024.10860093.

[8] Z. Zhuang and Z. Zhuang, "A Novel Five-Dimensional Chaotic System for Medical Image Encryption with X-Axis Projection," 2024 International Conference on Industrial IoT, Big Data and Supply Chain (IIoTBDSC), Wuhan, China, 2024, pp. 25-32, doi: 10.1109/IIoTBDSC64371.2024.00015.

[9] Y. Peng, S. Zhao, L. Kang and Y. Li, "Optimization of Encryption Efficiency for Nutritional Medical Image Data in High Concurrency Environments," 2024 IEEE 2nd International Conference on Image Processing and Computer Applications (ICIPCA), Shenyang, China, 2024, pp. 146-149, doi: 10.1109/ICIPCA61593.2024.10709306.

[10] E. Zhu, H. Feng, L. Chen, Y. Lai and S. Chai, "MP-Net: A Multi-Center Privacy-Preserving Network for Medical Image Segmentation," in IEEE Transactions on Medical Imaging, vol. 43, no. 7, pp. 2718-2729, July 2024, doi: 10.1109/TMI.2024.3377248.

[11] S. Ibrahim, A. M. Abbas, A. A. Alharbi and M. A. Albahar, "A New 12-Bit Chaotic Image Encryption Scheme Using a 12 × 12 Dynamic S-Box," in IEEE Access, vol. 12, pp. 37631-37642, 2024, doi: 10.1109/ACCESS.2024.3374218.

[12] M. K, J. J, K. K, M. G, V. S. R and S. B, "Secure Medical Image Encryption Using Homomorphic

Techniques," 2024 Second International Conference on Advances in Information Technology (ICAIT), Chikkamagaluru, Karnataka, India, 2024, pp. 1-6, doi: 10.1109/ICAIT61638.2024.10690754.

[13] A.A. Siam, M. M. Hassan and T. Bhuiyan, "Secure Medical Imaging: A DICOM to JPEG 2000 Conversion Algorithm with Integrated Encryption," 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA, 2025, pp. 1-6, doi: 10.1109/ICAIC63015.2025.10848861.

[14] B. Long, Z. Chen, T. Liu, X. Wu, C. He and L. Wang, "A Novel Medical Image Encryption Scheme Based on Deep Learning Feature Encoding and Decoding," in IEEE Access, vol. 12, pp. 38382-38398, 2024, doi: 10.1109/ACCESS.2024.3371888.

[15] Z. -C. Fan, D. Li and S. Rahardja, "A Novel Discrete Fractional Complex Hadamard Transform for Medical Image Encryption," ICASSP 2024 - 2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Seoul, Korea, Republic of, 2024, pp. 2126-2130, doi: 10.1109/ICASSP48485.2024.10446992.

[16] M. Ayyavoo and V. Guruviah, "Research on Medical Image Segmentation and Encryption Using GAN," 2023 International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2023, pp. 1-8, doi: 10.1109/ICDSNS58469.2023.10245429.

[17] A.Basak, S. Mandal, P. Das and M. Kumari, "Medical Image Cryptosystem using Hyperchaotic Sequence and Scrambling Operations with Sequential Cell-division," 2024 12th International Conference on Internet of Everything, Microwave, Embedded, Communication and Networks (IEMECON), Jaipur, India, 2024, pp. 1-6, doi: 10.1109/IEMECON62401.2024.10846598.

[18] M. Demirtaş and S. Altunkaya, "Medical Image Encryption based on Tangent Transform-based Sine-Chebyshev Map," 2024 8th International Symposium on Innovative Approaches in Smart Technologies (ISAS), İstanbul, Turkiye, 2024, pp. 1-7, doi: 10.1109/ISAS64331.2024.10845249.

[19] D. El-Damak, W. Alexan, E. Mamdouh, M. El-Aasser, A. Fathy and M. Gabr, "Fibonacci Q-Matrix, Hyperchaos, and Galois Field (2^8) for Augmented Medical Image Encryption," in IEEE Access, vol. 12, pp. 102718-102744, 2024, doi: 10.1109/ACCESS.2024.3433499.

[20] M. Shanavaz, G. C. S. Manikanta, M. Gnanaprasoona, K. S. Kishore, R. Karthikeyan and M. A. Jabbar, "Towards Efficient Encrypted Medical Image Retrieval from Heterogeneous Multi Cloud Environment," 2024 IEEE International Conference for Women in Innovation, Technology & Entrepreneurship (ICWITE), Bangalore, India, 2024, pp. 143-147, doi: 10.1109/ICWITE59797.2024.10502443.

Citation of this Article:

M.Sri Lakshmi Preethi (Ph. D), S.Venkata Lokesh, & B.Ganeshwar Reddy. (2025). Advanced Chaotic Asymmetric Cryptosystems for Securing Medical Imaging Data. In proceeding of Second International Conference on Computing and Intelligent Systems (ICCIS-2025), published in *IRJIET*, Volume 9, Special Issue ICCIS-2025, pp 40-47. Article DOI https://doi.org/10.47001/IRJIET/2025.ICCIS-202506

****

