DUAL ENCRYPTION-BASED FRAMEWORK FOR SECURING MEDICAL IMAGES IN HEALTHCARE SYSTEM

Ms. Harshika Dehariya
Project Guide
Dept. of EM-Tech (AI&ML),
SBJITMR, Nagpur, INDIA
E-mail:
harshikadehariya@sbjit.edu.in

Ms. Isha Bairam
Student
Artificial Intelligence & Machine Learning
SBJITMR, Nagpur, INDIA
E-mail: ishab.aiml22@sbjit.edu.in

Ms. Khushi Ghatode
Student
Artificial Intelligence & Machine Learning
SBJITMR, Nagpur, INDIA
E-mail: khushig.aiml22@sbjit.edu.in

Mr. Rohit Khadse
Student
Artificial Intelligence & Machine Learning
SBJITMR, Nagpur, INDIA
E-mail: rohitk.aiml22@sbjit.edu.in

Ms. Shrushti Adkane
Student
Artificial Intelligence & Machine Learning
SBJITMR, Nagpur, INDIA
E-mail: shrushtia.aiml22@sbjit.edu.in

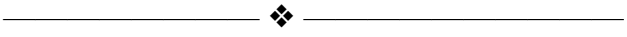
Abstract

In modern healthcare systems, the secure storage, transmission, and management of medical images become a critical concern due to the growing risks of cyberattacks, data breaches, and unauthorized access. Medical images such as CT, MRI, and X-ray scans contain highly sensitive patient information that, if compromised, may lead to privacy violations, identity theft, and legal complications. Traditional encryption techniques, while useful, often face limitations when addressing the high-volume, real-time requirements of medical image data. This project proposes a dual encryption-based framework that integrates the robustness of symmetric cryptography with the advanced protection of asymmetric cryptography to achieve enhanced security for medical imaging systems in healthcare environments.

The framework builds upon advancements in lightweight cryptography, optimization-based key management, and hybrid security protocols as highlighted in existing research. The symmetric component, such as AES (Advanced Encryption Standard), ensures fast and efficient encryption of large image files, while the asymmetric component, such as RSA or Elliptic Curve Cryptography (ECC), secures the encryption keys during exchange and authentication phases. Additionally, modern methods like oppositional-based optimization (OBOA) and quantum-resistant key distribution can be integrated to strengthen resilience against brute-force and quantum attacks.

Keywords

Medical Image Security, Dual Encryption, AES, RSA, Healthcare System, Cryptography, Optimization.



1. INTRODUCTION

The rapid digital transformation in healthcare has led to widespread adoption of electronic health records (EHRs), telemedicine, and cloud-based medical data sharing platforms. Among these, medical imaging systems play a central role in clinical diagnosis, treatment planning, and patient monitoring. However, as imaging technologies advance and data volumes grow, the security and privacy of medical images have become increasingly vulnerable to threats such as cyberattacks, unauthorized access, and data manipulation. Healthcare data breaches have surged globally, resulting in both economic losses and compromised patient trust, emphasizing the urgent need for robust protection mechanisms tailored specifically to medical images.

Traditional single-layer cryptographic solutions, though effective in certain contexts, often struggle to provide comprehensive protection when applied to large-scale medical datasets. Symmetric algorithms such as AES are efficient for encrypting high-volume image files, but they face challenges in secure key distribution. Conversely, asymmetric algorithms like RSA and ECC offer stronger key management but introduce higher computational complexity. This imbalance necessitates a hybrid or dual encryption approach that can combine the efficiency of symmetric encryption with the security guarantees of asymmetric cryptography. Several research studies have explored medical image encryption frameworks. For example, optimization-driven dual encryption techniques [Avudaiappan et al., 2018] demonstrated promising results in improving key sensitivity and resistance to statistical attacks. More recent studies [Kusum Lata & Cenkeramaddi, 2023] have incorporated deep learning.

The proposed Dual Encryption-Based Framework for Securing Medical Images takes this hybrid approach a step further by embedding the encryption keys within QR codes using steganography. This not only makes key transmission secure but also covert, as the QR code appears to be an ordinary image while secretly carrying the cryptographic materials. The combination of chaos-enhanced AES, logistic map permutation, ElGamal encryption, and LSB steganography creates a multi-layered defense strategy that is highly suited to the sensitive and regulated environment of healthcare.

- Implement Dual-Key Mechanism for Secure Key Management: Generate two distinct keys: Static Key: Used to encrypt the dynamic key. Dynamic Key: Used for the actual image encryption.
- Secure Key Transmission Using Steganography: Encode the dynamic key and modified static key into a QR code.
- To implement AES-based encryption for medical images: Ensure efficient pixel-level encryption using the Advanced Encryption Standard (AES) to guarantee high confidentiality, low computational cost, and compliance with medical data standards.
- Integrate RSA for secure key exchange in medical imaging systems: Incorporate RSA digital signatures to validate sender authenticity, ensuring that keys are not only encrypted but also verifiable for integrity.
- Apply Asymmetric Encryption for Authentication and Confidentiality.

2. LITERATURE SURVEY

T. Avudaiappan et al. (2018) proposes a secure method to protect sensitive medical images during transmission. The approach combines Blowfish encryption and Signcryption, with Oppositional-based Flower Pollination (OFP) optimization to generate stronger private and public keys. Experimental results show high PSNR, entropy, and low MSE, indicating both strong image protection and preserved quality. This dual encryption model enhances confidentiality and resistance to attacks, making it suitable for secure medical data sharing.

Mangesh B. Potdar et al., The paper presents a comprehensive review of crypto-stego techniques, which combine cryptography and steganography to achieve double-layer security in digital communication. Various approaches are discussed, including spatial domain, edge-based, frequency domain, and hybrid crypto-stego methods. The paper evaluates techniques based on parameters like PSNR, MSE, entropy, NPCR, UACI, key sensitivity, and robustness. The review also outlines challenges such as computational complexity, resistance to attacks, and limited application to color images, suggesting future research directions.

Ahmad et al., The paper introduces MID-Crypt, a hybrid cryptographic algorithm designed to protect medical images. It integrates Elliptic-curve Diffie–Hellman (ECDH) for image masking, AES with updatable keys for encryption, and a Merkle tree digital signature for data integrity. A dedicated key management system ensures secure public/private key handling and rotation. Evaluation using PSNR, entropy, histogram, and timing analysis shows MID-Crypt's superiority in security and performance.

Lata & Cenkeramaddi et al., This review explores the integration of deep learning with cryptography for securing medical images in the context of IoMT (Internet of Medical Things). It surveys more than 150 studies covering encryption, authentication, steganography, key generation, adversarial attack resistance, and end-to-end secure processing. The paper highlights CNNs, GANs, and transfer learning as enabling technologies for secure image classification, segmentation, and compression. It also emphasizes vulnerabilities like adversarial attacks and data breaches in healthcare, while suggesting future research directions for privacy-preserving deep learning in medical cryptography.

Abdulameer et al., The paper introduces a cloud data protection model integrating dual system encryption with a selective proof technique for secure data outsourcing. It leverages Proxy Re-Encryption (PRE) within an attribute-based framework (CP-ABPRE), enabling secure data sharing while maintaining integrity and privacy. The model includes distributed verification through Third Party Auditors (TPAs) and SUBTPAs to ensure reliability. Experimental results show reduced computation overhead, efficient verification, and resistance against insider/external threats.

Sharma et al., This paper introduces a hybrid cryptography framework for securing medical images. It integrates DNA sequence operations with a chaotic logistic map to generate encryption keys, enhancing randomness and resistance against statistical attacks. The method encrypts image pixels at both diffusion and confusion.

Sykota et al., The paper proposes a multi-layered security model combining Quantum Key Distribution (QKD), SHA-based hashing, AES encryption, and deep learning-based steganography. Using the E91 QKD protocol, entangled photons generate secret keys that are hashed and then used for AES encryption of steganographic images. Steganography hides sensitive data within cover images, providing double-layer protection. Experimental evaluation demonstrates high entropy (~8), strong NPCR and UACI values, and efficient encryption/decryption speeds. The framework is resilient against both classical and quantum attacks, offering a robust security solution for future communication systems.

Roy et al., The paper addresses the security challenges faced by unmanned aerial vehicles (UAVs), such as identity management, secure communication, and resistance to attacks, in the context of the Internet of Drones (IoD). To overcome these challenges, the authors propose a dual-layer authentication scheme that integrates Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) on Field-Programmable Gate Arrays (FPGAs). The scheme operates in three phases: user registration, UAV registration, and mutual authentication between user, ground base station (GBS), and UAV. AES provides fast symmetric encryption suitable for constrained UAV devices, while ECC ensures secure key exchange and authentication on the user side. In conclusion, the paper demonstrates that combining AES and ECC in FPGA hardware provides a practical and robust authentication solution for UAV systems, with potential for future improvements such as post-quantum cryptography and real-world deployment.

2.1 Abstractive Summarization

The reviewed papers explore diverse advancements in cryptography, steganography, and data security across domains like healthcare, cloud computing, and UAV systems. Techniques such as hybrid DNA-chaos encryption, deep learning-based cryptography, and FPGA-enabled authentication enhance privacy, robustness, and resistance against cyber and quantum attacks.

Collectively, these studies emphasize the integration of AI, quantum methods, and hybrid encryption frameworks to achieve double-layered protection and efficient data management. Applications span secure medical image transmission, cloud data integrity, and intelligent forecasting, underscoring the growing role of cryptography-steganography fusion in ensuring confidentiality and trust in modern digital ecosystems.

2.2 Research Gaps

- Limited Real-Time Implementation – Many frameworks demonstrate strong encryption but lack real-world or clinical deployment testing in telemedicine or PACS environments.

- Scalability Issues – Existing hybrid and crypto-stego methods have not been extensively evaluated for large-scale or high-volume medical image datasets.

- Quantum-Resistant Adaptation – Few studies fully address quantum-era threats, despite growing interest in post-quantum cryptography for healthcare systems.

• Standardization and Benchmarking – There is no unified benchmarking dataset or standardized evaluation metrics for comparing performance and robustness across studies.

• Efficient Key Management Integration – While several models use dual or dynamic keys, secure, lightweight, and automated key distribution mechanisms (especially using steganography) remain underexplored.

3.0 RESEARCH METHODOLOGY

The research methodology for this project is designed to systematically develop, implement, and evaluate the proposed dual encryption-based framework for securing medical images in healthcare systems. The approach integrates cryptographic modeling, algorithm implementation, and experimental validation to ensure both theoretical soundness and practical applicability. The methodology is divided into six major phases: data collection, preprocessing, Layer 1 encryption, Layer 2 secure transmission, experimental implementation, and evaluation.

Phase 1: Data Collection and Preprocessing

Medical imaging datasets, such as MRI, CT, and X-ray scans, will be collected from open medical repositories. Since medical images often exist in formats such as DICOM will involve format conversion, resizing, and noise reduction to ensure consistency across the dataset.

Phase 2: Layer 1 – AES-Based Image Encryption

The first encryption layer employs the Advanced Encryption Standard (AES), a symmetric-key algorithm widely recognized for its balance between speed and security.

Each image is encrypted using a randomly generated session key, which guarantees uniqueness and reduces the probability of key reuse. The encrypted image appears as random noise, protecting it from unauthorized access. Furthermore, enhancements such as oppositional-based optimization (OBOA) will be explored to generate stronger keys with higher entropy, increasing resistance against correlation and statistical attacks.

Phase 3: Layer 2 – Dual-Key Secure Transmission

Since symmetric algorithms face vulnerabilities in key distribution, the second layer secures the AES session key using asymmetric cryptography such as RSA. The AES key is encrypted with the receiver's public key before transmission, ensuring that only the corresponding private key can decrypt it. This eliminates risks of interception and man-in-the-middle attacks. Additionally, digital signatures and hash-based verification will be integrated to confirm sender authenticity and guarantee integrity of transmitted data.

Phase 4: Experimental Implementation

The encryption framework will be implemented in Python, utilizing libraries such as PyCryptodome (for AES and RSA/ECC), OpenCV (for image processing), and NumPy (for matrix operations). Experiments will simulate real-world healthcare scenarios, including telemedicine data exchange, cloud-based storage, and multi-user medical image sharing between hospitals and diagnostic centers.

Phase 5: Security and Attack Resilience Testing

The framework will be subjected to robust attack simulations, including brute-force, statistical, chosen-plaintext, differential, and side-channel attacks.

Phase 6: Evaluation Metrics

System performance will be assessed using:

- Encryption/Decryption Time → Measures efficiency in real-time usage.
- PSNR (Peak Signal-to-Noise Ratio) → Ensures decrypted images retain diagnostic quality.
- Entropy & Histogram Analysis → Validates randomness and resistance to statistical attacks.
- Key Sensitivity Tests → Confirms robustness against minor key variations.

By following this layered and iterative methodology, the project ensures that the dual encryption framework is robust, efficient, and scalable, making it suitable for real-world adoption in modern healthcare ecosystems.

4.0 DISCUSSION / RESULT

The study highlights the growing importance of integrating cryptography and steganography for medical image security. Future work should focus on quantum-resistant encryption, AI-driven key generation, lightweight IoMT models, blockchain integration, and privacy-preserving AI. These advancements will enhance real-time security, scalability, and compliance in healthcare data transmission and storage.

Security Strength: Hybrid crypto-stego and chaos-based approaches combine encryption and data hiding to enhance confidentiality, randomness, and robustness. They effectively resist brute-force, statistical, and differential attacks, ensuring stronger protection of sensitive medical images.

Performance Limitation: Despite their security benefits, these models often require heavy computation and memory, making them unsuitable for real-time or low-resource healthcare devices such as IoMT sensors and telemedicine platforms.

Standardization Gap: Existing studies use different datasets, parameters, and evaluation metrics, preventing fair comparison. Establishing standardized benchmarks and testing protocols is essential for consistent performance evaluation and global adoption.

4.1 Performance Metrics

Performance metrics such as PSNR, MSE, entropy, NPCR, and UACI evaluate image quality, randomness, and robustness of encryption. Low correlation and high key sensitivity indicate strong security, while execution time and energy efficiency assess real-time feasibility. These parameters collectively determine effectiveness, reliability, and efficiency of crypto-stego systems in healthcare.

5. CONCLUSION

Medical imaging has revolutionized healthcare by enabling accurate diagnostics, treatment planning, and long-term monitoring. However, as these images transition from physical film to digital storage and transmission, they become highly susceptible to cyberattacks, unauthorized access, and privacy breaches. This risk is particularly concerning given that medical images often contain identifiable patient information embedded in both image data and metadata.

The proposed Dual Encryption-Based Framework for Securing Medical Images addresses the most pressing vulnerabilities in existing systems by integrating chaos-based AES encryption with secure and covert key distribution. Unlike traditional encryption schemes that rely on fixed substitution and permutation operations, this framework employs dynamic S-box generation using the Hénon chaotic map and pixel permutation using the logistic map, ensuring that every encryption session is unique and resistant to statistical and differential cryptanalysis.

In conclusion, the framework offers end-to-end security by protecting both image content and encryption keys. By uniting chaos theory, symmetric encryption, asymmetric encryption, and steganography, it provides a scalable, compliance-ready, and highly resilient solution for safeguarding sensitive medical images in healthcare systems.

6. FUTURE SCOPE

- Post-Quantum Cryptography Integration – Develop quantum-resistant algorithms to safeguard medical images from future quantum computing attacks.
- AI-Driven Key Generation – Use deep learning for adaptive and intelligent key generation to enhance unpredictability and reduce manual key management.
- Lightweight Encryption for IoMT Devices – Design efficient, low-power crypto-stego models suitable for Internet of Medical Things.
- Standardized Evaluation Frameworks – Create benchmark datasets and standard metrics to uniformly assess image security performance and robustness.
- Blockchain-Enabled Medical Data Security – Employ blockchain for secure audit trails, access control, and decentralized storage of medical images.
- Hybrid Quantum–Classical Security Models – Combine quantum key distribution (QKD) with classical cryptography and steganography for next-generation data protection.
- Real-Time Cloud Implementation – Optimize crypto-stego algorithms for high-speed cloud platforms to enable real-time encrypted telemedicine.
- Enhanced Steganographic Techniques – Explore deep learning-based or adaptive steganography for higher embedding capacity and undetectability.
- Privacy-Preserving Deep Learning Models – Develop secure AI frameworks that allow encrypted data processing without decryption (e.g., homomorphic encryption).
- Regulatory and Ethical Compliance Systems – Implement automated compliance validation tools ensuring adherence to HIPAA, GDPR, and medical ethics standards during secure data handling.

7. REFERENCES

1. Gawande, A. A. & Sonavane, S. S. (2018). Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm. Int. J. Computer Sciences and Engineering, 6(5), 230–238.
2. Gulia, S., Mukherjee, S. & Choudhury, T. (2016). An Extensive Literature Survey on Medical Image Steganography. CSI Transactions on ICT, 4, 293–298.
3. Khalil, M. I. (2017). Medical Image Steganography: Study of Medical Image Quality Degradation when Embedding Data in the Frequency Domain. IJCNIS, 9(2), 22–28.
4. Nagm, A. & Elwan, M. S. (2021). Protection of the patient data against intentional attacks using a hybrid robust watermarking code. arXiv:2110.09519.
5. Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K.-K. R., & Qin, Z. (2020). DeepKeyGen: A Deep Learning-based Stream Cipher Generator for Medical Image Encryption. arXiv:2012.11097.
6. Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., & Qin, Z. (2020). DeepEDN: A Deep Learning-based Image Encryption and Decryption Network for IoMT. arXiv:2004.05523.
7. AbdelRaouf, A. (2021). A new data hiding approach for image steganography based on visual color sensitivity. Multimedia Tools and Applications, 80(15), 23393–23417.
8. Hussain, Q., Riaz, S., Saleem, A., Ghafoor, A., & Jung, K.-H. (2021). Enhanced adaptive data hiding using LSB and pixel value differencing.
9. Yanuar, M. R., Mt, S., Apriono, C., & Syawaludin, M. F. (2024). Image-to-image steganography with Josephus permutation and LSB 3-3-2 embedding. Applied Sciences, 14(16), 7119.
10. Ali, M. Z., Riaz, O., Hasnain, H. M., Sharif, W., Ali, T., & Choi, G. S. (2024). Fusion of MSB matching and LSB substitution for enhanced concealment. Computational Materials & Continua, 79(2), 2923–2943.
11. Rubaie, A., Fadhel, S., & Maher, K. M. (2024). High capacity double precision image steganography based on chaotic maps. Bulletin of EEI, 13, 320–331.
12. Siddiqui, G. F. et al. (2020). A dynamic three-bit image steganography algorithm for medical and e-healthcare systems. IEEE Access, 2020.
13. Bhardwaj, R. (2020). An improved separable reversible patient data hiding algorithm for e-healthcare. Multimedia Tools and Applications.
14. Mansour, R. F. & Parah, S. A. (2021). Reversible data hiding for electronic patient information security. Arab J Sci Eng.
15. Loan, N. A., Parah, S. A., Sheikh, J. A., Akhoon, J. A., & Bhat, G. M. (Year). Hiding EPR in medical images: high capacity technique for e-healthcare.