A

SYNOPSIS REPORT

on

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

Submitted to Autonomous Institute,

Affiliated to The Rashtrasant Tukadoji Maharaj Nagpur University Department of Emerging Technologies

Bachelor of Technology (B. Tech)

Submitted By

Ms. Shrushti Adkane (AM22005)

Ms. Isha Bairam (AM22019)

Ms. Khushi Ghatode (AM22029)

Mr. Rohit Khadse (AM22041)

Guided By

Ast Prof. Harshika Deheriya

S. B. JAIN INSTITUTE OF TECHNOLOGY, MANAGEMENT AND RESEARCH, NAGPUR

2025 – 2026

INDEX

ABSTRACT

In modern healthcare systems, the secure storage, transmission, and management of medical images has 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.

The novelty of this project lies in combining dual-layer encryption with adaptability to healthcare's real-time demands, without significantly increasing computational overhead. To further enhance security, the framework may embed encrypted images into steganographic carriers, thereby adding an additional concealment layer against adversarial detection. The proposed system will be evaluated through experiments on real medical imaging datasets, where parameters such as encryption speed, key sensitivity, entropy analysis, and resistance to statistical and differential attacks will be tested.

By implementing this framework, healthcare organizations can improve compliance with standards such as HIPAA and GDPR while ensuring patient trust and confidentiality. This work contributes to bridging the gap between traditional cryptographic techniques and modern, AI-driven, and quantum-aware security models for healthcare data protection.

Keywords: *Medical Image Security, Dual Encryption, AES, RSA, Healthcare System, Cryptography, Optimization, Steganography.*

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 approaches for key generation and adaptive encryption, while advanced frameworks such as MID-Crypt [Ahmad et al., 2022] combined ECDH, AES, and Merkle trees to enhance both confidentiality and integrity. These works highlight the pressing demand for security mechanisms that are not only resistant to classical attacks but also adaptive to emerging threats such as quantum computing and side-channel attacks.

The proposed project, “A Dual Encryption-Based Framework for Securing Medical Images in Healthcare System,” seeks to build upon these advancements by integrating symmetric and asymmetric cryptography into a unified framework. This framework aims to achieve three key goals: (1) ensure confidentiality of medical images during storage and transmission, (2) provide robust key management resistant to interception, and (3) maintain system efficiency suitable for real-time healthcare applications. By leveraging dual encryption and potential

steganographic embedding, the framework intends to create a secure yet practical solution aligned with healthcare standards such as HIPAA and GDPR.

However, the digital transformation of medical imaging has also introduced critical cybersecurity challenges. Medical images contain not only diagnostic information but also embedded metadata that can reveal a patient's identity, medical history, and personal details. Any unauthorized disclosure, manipulation, or destruction of such data can have severe consequences, including loss of patient privacy, incorrect diagnoses, legal liabilities, and reputational damage to healthcare institutions. Reports have shown that cyberattacks on healthcare systems have been increasing, with attackers targeting not only patient records but also imaging databases for ransom or malicious use.

Traditional encryption techniques like the Advanced Encryption Standard (AES) are well established for protecting textual and numerical data. AES is a symmetric block cipher that offers strong resistance against brute-force attacks when implemented correctly. However, applying standard AES directly to medical images can be inefficient and potentially insecure. This is due to the inherent properties of images like large file sizes, high redundancy, and strong pixel correlation. These properties can result in partial pattern visibility in the encrypted image, which could aid statistical cryptanalysis.

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.

AIM AND OBJECTIVES

The main aim of this project is to design, develop, and evaluate a dual encryption-based security framework for safeguarding medical images in healthcare systems. This framework must ensure confidentiality, integrity, and resilience against cyber threats while complying with stringent healthcare data protection regulations. By combining chaos-based symmetric encryption, asymmetric encryption, and steganography in a unified system, the goal is to provide end-to-end secure storage and transmission of sensitive medical imagery without compromising performance or accessibility.

➢ Objective

- **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.
  - Modify the static key by flipping a single bit and record the position of this flip to enhance security.
- **Secure Key Transmission Using Steganography**
  - Encode the dynamic key and modified static key into a QR code.
  - Use Least Significant Bit (LSB) steganography to embed the bit-flip position as a modulated hidden message within the 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.
  - Apply chaos-enhanced dynamic S-boxes in AES to increase unpredictability and resistance against statistical or brute-force cryptanalysis.
- **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.

    - Use RSA to protect symmetric AES keys during transmission, ensuring secure distribution across healthcare networks and preventing unauthorized access or interception.
- **Apply Asymmetric Encryption for Authentication and Confidentiality**
    - Encrypt the modulated message containing the bit-flip position using ElGamal encryption with the receiver's public key.
    - Ensure that only the intended recipient, with the corresponding private key, can recover the original static key.
- **To establish a dual-layer encryption framework**
    - Combine symmetric (AES) and asymmetric (RSA) techniques to provide layered security, balancing speed and scalability with strong protection against brute-force and man-in-the-middle attacks.
- **Secure Key Management**
    - Utilize asymmetric cryptography for safe exchange of symmetric keys, thereby addressing vulnerabilities in traditional key distribution systems. By embedding methods such as RSA or ECC, the system will minimize risks of key interception and tampering.

4. LITERATURE SURVEY

Sr no.	Year	Author	Title	Methodology/ Approach	Finding/ Contribution
1	2018	T.Avudaiappan1 & R. Balasubramanian	Medical Image Security Using Dual Encryption	Analytical approach to security models.	Highlights gaps in data hiding techniques and proposes enhanced secure transmission models.
2	2025	Omar Alnaseri & Yassine Himeur,	Complexity of Post-Quantum Cryptography in Embedded Systems	Comparative complexity analysis of with case studies of CRYSTALS-Kyber and McEliece.	Provided detailed analysis of PQC algorithms computational, memory, and energy profiles.
3	2021	Aiman Jan & Shabir A. Parah,	Double Layer Security using Crypto-Stego Techniques: A Comprehensive Review	Literature review of cryptography + steganography hybrid approaches from 2016–2021.	Summarized spatial and frequency domain steganography techniques.
4	2022	Paresh Kumar Pasayat & Soumya Ranjan Panigrahi	Design of Complex Data Security Algorithm Using Crypto+Stego Techniques	Proposed a hybrid crypto-stego algorithm for 256-bit data using four encryption keys and embedding in cover media	Resistant to brute-force and timing attacks.
5	2023	V. Pavani & Lakshman Narayana	Dual Key Authentication Model with Secure Data Transmission in Smart Cities	Dual key authentication protocol integrated with secure transmission for smart city devices.	Improves confidentiality and integrity in smart city communication.
6	2024	Kumar Sekhar Roy &	Dual-Layer Authentication Scheme	implementation of AES + ECC authentication	Enhanced UAV authentication security against

		Murikipudi Sujith	Utilizing AES and ECC	validated with AVISPA tool.	impersonation, replay, and tampering.
7	2025	A. Riva-Cambrin, Rahul Singh	Extensible Post Quantum Cryptography Based Authentication	Proposed a quantum-safe, single-shot protocol using lattice-based DSAs and KEMs, formally verified with TAMARIN.	Introduced a scalable, future-proof authentication protocol for machine-to-machine communication.
8	2025	Anne Broadbent, Raza Kazmi	On the Semantic Security of NTRU with a Gentle Introduction to Cryptography	Expository analysis of the NTRU cryptosystem with security proofs, concluding with formal security evaluation.	Proved that original NTRU is not IND-CPA secure; suggested padding schemes that achieve IND-CCA2 security.
9	2023	Kusum Lata, Linga Reddy Cenkeramaddi	Deep Learning for Medical Image Cryptography: A Comprehensive Review	Review of over 150 studies integrating deep learning with cryptography for medical image security.	Summarized authentication, key generation, and compression method. Provided taxonomy and future research directions.
11	2022	Ashraf Ahmad & Remah Younisse	MID-Crypt: A Cryptographic Algorithm for Advanced Medical Images Protection.	Proposed MID-Crypt, combining ECDH, AES with updatable keys, Merkle trees, and digital signatures.	Outperformed existing schemes in PSNR, entropy, and overhead. Resistant to side-channel and algebraic attacks.
12	2023	V. Pavani & Lakshman Narayana	Dual Key Authentication Model with Secure Data Transmission in Smart Cities	Dual key authentication protocol integrated with secure transmission for smart city devices.	Improves confidentiality and integrity in smart city communication.

5. PROPOSED WORK

The proposed project introduces a dual encryption-based framework to ensure secure storage and transmission of medical images in healthcare systems. This framework leverages both symmetric encryption for high-speed image protection and asymmetric encryption for secure key exchange, thereby providing a comprehensive defence mechanism against modern cyber threats. The architecture is designed as a multi-layered security model, where each layer contributes to strengthening confidentiality, integrity, and resilience.

Layer 1 – Chaotic AES-Based Image Encryption

The first layer of the framework focuses on symmetric encryption of medical images using the Advanced Encryption Standard (AES) algorithm. AES is selected due to its proven robustness, computational efficiency, and ability to handle large datasets such as CT, MRI, and X-ray images. In this stage, the raw medical image is pre-processed and converted into a standardized format before encryption. AES ensures that the bulk image data is scrambled into an unreadable form, protecting it from unauthorized viewing or tampering.

The first layer focuses on enhancing the traditional AES algorithm with chaos theory to overcome its limitations in image encryption. This layer incorporates:

- Chaotic Pixel Permutation – A logistic map is used to generate pseudo-random sequences that reorder the pixel positions of the medical image before encryption. This disrupts the inherent spatial correlation in medical images, making statistical attacks more difficult.
- Dynamic S-Box Generation – A two-dimensional Hénon map produces dynamic substitution boxes for AES encryption. Unlike fixed S-boxes in standard AES, these change for every session, significantly increasing unpredictability and resistance to cryptanalysis.
- Feedback XOR Diffusion – After AES encryption, a feedback mechanism applies XOR operations between adjacent pixel blocks, enhancing diffusion and ensuring that even a one-pixel change in the original image results in a drastically different ciphertext.
- CBC Mode Operation – Cipher Block Chaining mode is implemented to ensure that identical plaintext blocks produce different ciphertext blocks, further eliminating repetitive patterns in the encrypted image.

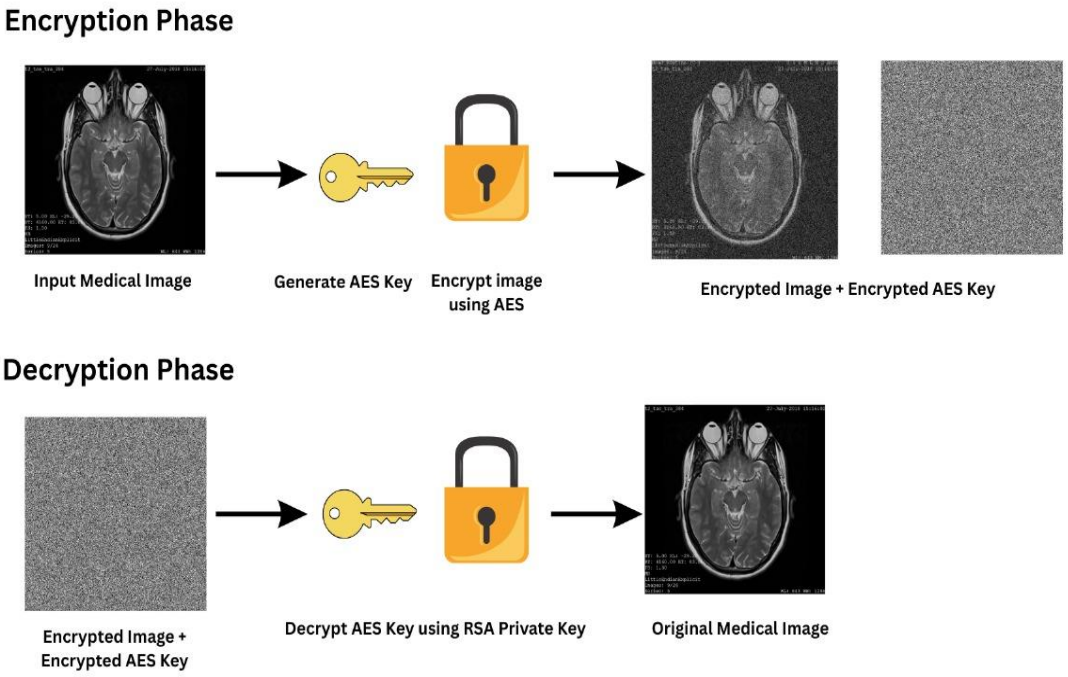

Figure 5.1

Layer 2 – Dual-Key Secure Transmission

The second layer addresses one of the most critical vulnerabilities in symmetric cryptography—secure key distribution. While AES ensures efficient encryption of the image, its secret key must be securely shared with the receiver. To achieve this, the project integrates asymmetric encryption techniques such as RSA or Elliptic Curve Cryptography (ECC).

The second layer addresses secure and covert key distribution, which is essential in symmetric encryption systems. This involves:

- Dual-Key Structure – Two keys are generated:
    - Static Key: Used to encrypt the dynamic key.
    - Dynamic Key: Used for image encryption.
- Bit-Flip Security Enhancement – A random bit in the static key is flipped to create a modified version. The position of this flip is recorded in a modulated message.

- ElGamal Encryption of Bit-Flip Position – The modulated message is encrypted using the recipient's public key, ensuring that only the intended recipient can reconstruct the correct static key.
- Steganographic QR Code Embedding – The modified static key and encrypted dynamic key are encoded into a QR code. Using LSB steganography, the ElGamal-encrypted message is hidden inside the QR code's pixel values without altering its visual structure.

By combining **Layer 1 (AES-Based Image Encryption)** and **Layer 2 (Dual-Key Secure Transmission)**, the framework provides a balanced, hybrid solution that ensures both efficiency and strong protection. This dual encryption model is expected to enhance healthcare security by aligning with regulatory standards like HIPAA and GDPR while maintaining real-time applicability in telemedicine and cloud-based diagnostic systems.

Technology Stack

Component	**Technologies used**
Frontend (UI)	Streamlit, Flask
Backend	Python 3.x
Encrypt/Decrypt	cryptography (RSA for key exchange), AES (Chaotic AES for image encryption)
Medical Image Handling	pydicom (for.dcm medical images), Pillow (image processing).
Security	Dual-layer security → AES (Chaotic), RSA (asymmetric), QR code steganography
Deployment/ Hosting	Heroku, PythonAnywhere, or Local server
Environment & Dependencies	virtualenv, requirement.txt

6. 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 (e.g., NIH, Kaggle). Since medical images often exist in formats such as DICOM, initial preprocessing will involve format conversion, resizing, and noise reduction to ensure consistency across the dataset. This prepares the images for systematic encryption without affecting diagnostic quality.

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 or Elliptic Curve Cryptography (ECC). 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. This ensures that the framework can resist both conventional cryptanalysis and emerging threats such as quantum cryptographic challenges.

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.
- **Regulatory Compliance Checks** → Ensures alignment with **HIPAA and GDPR** standards.

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.

7. 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. Protecting this data is not only a technical necessity but also a legal and ethical obligation for healthcare institutions.

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.

The modular design allows seamless integration into PACS, telemedicine systems, and cloud-based storage while maintaining compliance with HIPAA and GDPR regulations. Low computational overhead ensures minimal delay, making it suitable for real-time clinical environments.

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.

REFERNCES

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. Multimedia Tools and Applications, 80(13), 20381–20401.

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. [Journal info].

16. Islam, S., Modi, M. R., & Gupta, P. (2018). Performance analysis of medical image security using steganography based on fuzzy logic. Cluster Computing.

17. Singh, S. & Attri, V. K. (2015). Dual layer security using LSB image steganography and AES. Intl J Signal Process, Image Process, and Pattern Recognit., 8(5), 259–266.

18. Puech, W. (Year). Image encryption and compression for medical image security. IEEE IPTTA Conference Proceedings.

19. Yang, M., Song, L., Trifas, M., Aires, D. B., Chen, L. & Elston, J. (Year). Secure patient information and privacy in medical imaging. IEEE.

20. Zhang, X. (Year). Reversible data hiding in encrypted image. IEEE Signal Processing Letters, 18(4), 255.

21. Mitra, A., Rao, Y. S., & Prasanna, S. R. (2006). A new image encryption approach using combinational permutation techniques. Int J Comput Sci, 1(2), 127–131.

22. Elbirt, A. J. & Paar, C. (2005). Instruction-level distributed processor for symmetric-key cryptography. IEEE TPDS, 16(5), 468–480.

23. Di Laura, C., Pajuelo, D., & Kemper, G. (2016). Steganography with SDTV-H.264/AVC encoded video. Intl J Digit Multimed Broadcast, 2016, ID 6950592.

24. Vimala, S., Rajakani, M., & Poomi, U. (2016). Steganography using absolute moment block truncation coding. Int J Adv Eng Res Sci, 3.

25. Al-Shatanawi, O. M. & Emam, N. N. (2015). Image steganography using MLSB with random pixels. IJNSA, 7(2).

BIBLIOGRAPHY:

Books & Foundational Texts

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.
2. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.
3. Gonzalez, R. C. & Woods, R. E. (2018). Digital Image Processing. Pearson.
4. Fridrich, J. (2009). Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press.
5. Kahn, D. (1996). The Codebreakers: The Comprehensive History of Secret Communication. Scribner.

Reports & Standards

1. NIST. (Publication Year). Advanced Encryption Standard (AES). NIST FIPS-197.
2. HIPAA Journal. (Latest). HIPAA Compliance and Data Security in Healthcare.
3. Electronic Frontier Foundation (EFF). (Regular updates). Steganography and Privacy Issues.

Online & Multimedia Resources

1. Practical demonstrations of LSB steganography tools and tutorials.
2. GitHub repositories for image steganography project implementations.
3. IEEE Xplore – Collections on medical image security.
4. Deep Learning frameworks for encrypted medical image analytics.