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 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.

Key Topics

1. **Dual Encryption Mechanism**

The framework combines symmetric (AES with chaos-based enhancements) and asymmetric (RSA/ElGamal) cryptography. This hybrid approach balances speed with strong protection, making medical image security more robust.

2. Chaotic AES for Image Protection

AES is enhanced with chaotic pixel permutation, dynamic S-boxes, and diffusion techniques**.** These prevent statistical and brute-force attacks while ensuring that encrypted medical images appear as random noise.

3. Secure Key Management

A dual-key structure (static + dynamic keys) is implemented. Keys are further secured by steganography in QR codes, ensuring that cryptographic materials are transmitted covertly and protected from interception.

4. Steganography Integration

Using LSB embedding in QR codes**,** encryption keys and hidden messages are securely concealed. This adds an extra layer of secrecy and prevents adversaries from detecting cryptographic data.

5. Compliance with Healthcare Standards

The system is designed to align with HIPAA and GDPR regulations, ensuring secure handling of patient data and supporting legal, ethical, and trust requirements in healthcare institutions.

6. Performance & Real-Time Efficiency

The proposed framework maintains low computational overhead**,** making it practical for real-time applications like telemedicine, cloud storage, and hospital information systems without slowing workflows.

7. Resilience against Advanced Threats

The use of quantum-resistant techniques, digital signatures, and entropy-based key generation provides strong resistance to modern threats, including cyber-attacks, data breaches, and quantum computing risks**.**

LITERATURE REVIEW

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. It effectively resists side-channel, differential, MITM, and algebraic attacks, making it suitable for secure transmission of sensitive medical data.

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 levels, preserving image quality while resisting brute force and differential attacks. Performance is evaluated using histogram analysis, entropy, NPCR, UACI, PSNR, and correlation measures, demonstrating strong robustness and efficiency in healthcare data protection.

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.

Summarization

1. R.M. van Steenbergen et al.:

- **Focus:** Introduction of the Demand Forest method.
- **Approach:** Combines K-means clustering, Random Forest, and Quantile Regression Forest.
- **Application:** Uses historical sales data and product characteristics to forecast demand for new products.
- **Outcome:** Provides prelaunch forecasts and supports inventory management by predicting demand patterns and quantiles.

2. Mangesh B. Potdar et al.:

- **Focus:** Comprehensive review of crypto-stego methods for secure data transmission.
- **Approach:** Examines spatial, edge-based, frequency-domain, and hybrid crypto-stego schemes.
- **Application:** Data hiding and encryption for e-health, IoT, cloud security, mobile devices, and secure communication systems.
- **Outcome:** Confirms that crypto-stego provides double-layer security (encryption + concealment).

3. Ahmad et al.:

- **Focus:** Development of MID-Crypt for medical image protection.
- **Approach:** Combines ECDH, AES, key rotation, digital signatures, and Merkle tree.
- **Application:** Secures patient medical images in healthcare communication systems.
- **Outcome:** Provides high encryption quality, robustness, and attack resistance.

4. Lata & Cenkeramaddi et al.:

- **Focus:** Comprehensive review of deep learning-based medical image cryptography.
- **Approach:** Surveys encryption, authentication, compression, and adversarial defense methods using deep learning.
- **Application:** Secure storage, transmission, and analysis of medical images in IoMT and cloud-based healthcare systems.
- **Outcome:** Identifies opportunities and challenges in applying AI for robust, privacy-preserving healthcare solutions.

5. Abdulameer et al.

- **Focus:** Cloud data security and integrity in outsourced storage.
- **Approach:** Dual system encryption + CP-ABPRE + selective proof + PRE.
- **Application:** Secure data storage, sharing, and verification in cloud systems.
- **Outcome:** Ensures integrity, privacy, and low-overhead verification for cloud users.

6. Sharma et al.

- **Focus:** Hybrid DNA-chaos-based cryptographic scheme for medical image security.
- **Approach:** Combines DNA encoding with chaotic key generation for encryption.
- **Application:** Protecting patient medical images from unauthorized access in healthcare systems.
- **Outcome:** Ensures high entropy, robustness, and resistance to brute force and statistical attacks.

7. Sykota et al.

- **Focus:** Hybrid quantum-classical cryptographic framework with steganography.
- **Approach:** Combines QKD (E91), SHA hashing, AES encryption, and deep steganography.
- **Application:** Secure digital image communication requiring strong confidentiality.
- **Outcome:** Provides resistance to classical and quantum attacks with strong entropy and robustness.

8. Roy et al.

- **Focus:** Introduction of an FPGA-based dual-layer authentication scheme for unmanned aerial vehicles (UAVs).
- **Approach:** Combines Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC).
- **Application:** Provides secure user and UAV registration and mutual authentication in UAV communication, leveraging FPGA hardware to handle computational tasks.
- **Outcome:** Demonstrates improved resistance to attacks such as impersonation, replay, and tampering.

Strength and Weakness

1. T. Avudaiappan et al. (2018)

Strengths:

- **Enhanced Security:** Dual encryption (Blowfish + Signcryption) with optimized key generation improves resistance against cryptographic attacks.
- **Performance Efficiency:** Achieves high PSNR and entropy with low MSE, ensuring both image quality and strong protection.
- **Robust Key Management:** OFP optimization enhances private and public key generation for more secure encryption.
- **Wide Applicability:** Suitable for safeguarding sensitive patient data across healthcare networks.

Weaknesses:

- **Computational Complexity:** Dual encryption with optimization increases processing overhead, which may limit real-time applications.
- **Implementation Difficulty:** Requires expertise in both cryptography and optimization algorithms, making adoption challenging in resource-constrained healthcare setups.
- **Scalability Concerns:** Effectiveness may vary with very large medical datasets or under heavy transmission loads.

2. Mangesh B. Potdar et al.

Strengths

- **Comprehensive Review**: Covers multiple domains (spatial, frequency, edge, hybrid).
- **Dual-layer Security:** Combines cryptography and steganography for enhanced robustness.
- **Evaluation Parameters:** Provides detailed comparative analysis using strong metrics.
- **Wide Application:** Relevant for healthcare, IoT, cloud, and secure digital communications.

Weaknesses

- **Computational Complexit**y: Many methods are resource-heavy and complex.
- **Generalizability Issues:** Most techniques tested only on grayscale images; limited color image studies.
- **Attack Resistance:** Many methods not fully tested against geometric, noise, or signal processing attacks.
- **Lack of Benchmarking:** Absence of standard datasets for uniform performance evaluation.

3. Ahmad et al.

Strengths:

- Strong hybrid architecture combining multiple cryptographic techniques.
- Secure key management with rotation and patient PIN integration.
- High performance (PSNR, entropy) and robustness against attacks.
- Suitable for practical healthcare data security applications.

Weaknesses:

- Increased computational complexity due to multiple modules.
- May be challenging to implement in real-time or low-resource environments.
- Scalability and interoperability with large medical datasets need validation.

4. Lata & Cenkeramaddi et al.

Strengths:

- Extensive survey covering >150 research papers.
- Explores multiple applications: encryption, compression, authentication, and security.
- Highlights vulnerabilities and adversarial attack defense strategies.
- Strong relevance to IoMT and modern healthcare security needs.

Weaknesses:

- Survey-based, lacks experimental implementation or benchmarking.
- Practical deployment challenges (computation, regulatory compliance) not deeply addressed.
- Rapidly evolving field—findings may become outdated quickly.

5. Abdulameer et al.

Strengths:

- Dual encryption enhances confidentiality.
- Proxy re-encryption supports efficient and flexible data sharing.
- Distributed verification (TPAs/SUBTPAs) improves trustworthiness.
- Low computational overhead compared to baseline methods.

Weaknesses:

- Increased complexity in deployment and key management.
- Relies on third-party auditors, which may introduce dependency risks.
- Limited scalability evaluation under large-scale cloud environments.

6. Sharma et al.
Strengths:

- Strong randomness from DNA + chaotic system integration.
- High resistance against brute force, statistical, and differential attacks.
- Maintains image quality (high PSNR, low correlation).

Weaknesses:

- Complexity in DNA sequence operations.
- Limited large-scale or real-time testing.
- Key management and interoperability not fully explored.

7. Sykota et al.
Strengths:

- Integrates quantum and classical cryptography with steganography.
- Demonstrates strong entropy, NPCR, UACI, and histogram results.
- Resistant to both quantum and classical attacks.

Weaknesses:

- Requires quantum hardware (E91 QKD), limiting practical deployment.
- Higher complexity due to multi-layered integration.
- Computational overhead from hashing, AES, and steganography.

8. Roy et al.
Strengths:

- Dual-layer Security: Integration of AES (symmetric) and ECC (asymmetric) provides robust security suitable for UAVs with limited resources.
- Hardware-based Implementation: Using FPGA enhances efficiency, reduces computational burden on UAVs, and improves resistance to physical and software-based attacks.

Weaknesses:

- Complexity of Deployment: Requires specialized FPGA integration and expertise, which may limit ease of adoption.
- Performance Trade-offs: Although efficient, the computational cost (20 ms) is higher compared to some lightweight schemes, which may affect scalability in high-volume UAV networks.

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 cloudbased 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.

Significance:

- **Enhanced Security for Medical Images** – The framework provides dual-layer protection by combining symmetric (AES with chaos-based enhancements) and asymmetric (RSA/ElGamal) encryption, ensuring strong confidentiality and resilience against brute-force and statistical attacks.
- **Secure Key Management** – By integrating dual-key mechanisms with steganographic QR code embedding, the project overcomes traditional key distribution vulnerabilities, making the transmission of encryption keys both secure and covert.
- **Compliance with Healthcare Standards** – The system is designed to meet regulatory requirements like **HIPAA** and **GDPR**, safeguarding sensitive patient data while maintaining patient trust and legal compliance.
- **Real-Time and Scalable Application** – With low computational overhead and optimized cryptographic operations, the framework supports real-time healthcare scenarios such as telemedicine, PACS, and cloud-based medical image sharing.