IMPLEMENTATION PAPER ON DUAL ENCRYPTION-BASED FRAMEWORK FOR SECURING MEDICAL IMAGES

Prof. Harshika Dehariya
Computer Science & Engineering,
(AI&ML)
S.B. Jain Institute of Technology
Management & Research, Nagpur
harshikadehariya@sbjit.edu.in

Rohit Khadse
Computer Science & Engineering,
(AI&ML)
S. B. Jain Institute of Technology,
Management & Research, Nagpur
rohitk.aiml22@sbjit.edu.in

Khushi Ghatode
Computer Science & Engineering
(AI&ML)
S. B. Jain Institute of Technology
Management & Research,Nagpur
khushig.aiml22@sbjit.edu.in

Isha Bairam
Computer Science & Engineering,
(AI&ML)
S. B. Jain Institute of Technology,
Management & Research, Nagpur
ishab.aiml22@sbjit.edu.in

Shrushti Adkane
Computer Science & Engineering,
(AI&ML)
S. B. Jain Institute of Technology,
Management & Research, Nagpur
shrushtia.aiml22@sbjit.edu.in

Abstract—
In modern healthcare, medical images such as CT, MRI, and X-ray scans contain highly sensitive patient information. Protecting these images against unauthorized access, data breaches, and cyberattacks is a critical concern. Traditional single-layer encryption methods are often insufficient due to large file sizes, high redundancy, and real-time processing demands.

This paper proposes a dual encryption-based framework that combines chaotic AES (symmetric encryption) for fast image encryption and RSA/ECC (asymmetric encryption) for secure key management. Additionally, steganography is applied for covert key transmission by embedding encrypted keys into QR codes. The framework ensures confidentiality, integrity, and compliance with HIPAA and GDPR standards.

Experimental validation on medical datasets demonstrates strong resistance to brute-force, statistical, and differential attacks while maintaining low computational overhead. This approach provides a scalable and secure solution for real-time medical imaging applications.

I.INTRODUCTION

The contemporary healthcare sector is undergoing a profound digital revolution, marked by the widespread adoption of electronic health records (EHRs), telemedicine platforms, and cloud-based diagnostic systems. This transition, accelerated by the need for remote and accessible patient care, has fundamentally reshaped how medical data is generated, stored, and transmitted. While this digital paradigm offers unprecedented benefits in diagnostic efficiency and collaborative medicine, it simultaneously exposes a vast and sensitive attack surface for cybersecurity threats. At the heart of this challenge lies the security of medical images. Modalities such as Computed Tomography (CT), Magnetic Resonance Imaging (MRI), Positron Emission Tomography (PET), and Xray scans are foundational to modern diagnostics, but their digital nature makes them prime targets for unauthorized access, data breaches, and ransomware attacks.

Medical images are not merely visual data; they are complex data structures with unique characteristics that render conventional encryption methods less effective. They are typically large in file size, exhibit high levels of redundancy due to uniform tissue regions and possess a strong correlation between adjacent pixels. These properties can be exploited by attackers to perform statistical analyses that may reveal patterns even in encrypted data. Furthermore, medical images are intrinsically linked with a wealth of personally identifiable information (PII) and protected health information (PHI), often embedded within the metadata of formats like DICOM (Digital Imaging and Communications in Medicine). A breach of this data can lead to severe consequences, including patient privacy violations, identity theft, insurance fraud, and an erosion of trust in healthcare institutions.

The legal and ethical landscape governing patient data further underscores the critical need for robust security. International regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union mandate stringent technical safeguards for protecting PHI. These regulations champion principles like "data protection by design and by default," requiring that security measures be integrated into the very fabric of data processing systems, not merely applied as an afterthought. Failure to comply can result in substantial financial penalties and severe reputational damage.

Traditional, single-layer cryptographic solutions struggle to meet these multifaceted demands. Symmetric algorithms like the Advanced Encryption Standard (AES) offer the high throughput necessary for encrypting large image files but are encumbered by the persistent challenge of secure key distribution. If the single shared key is compromised, the entire security framework collapses. Conversely, asymmetric algorithms such as RSA and ECC (Elliptic Curve Cryptography) provide a powerful solution for secure key management via their public-private key architecture. However, their significant computational overhead makes them prohibitively slow for the direct encryption of large datasets, rendering them impractical for real-time clinical workflows where diagnostic speed is paramount.

To address this intricate set of challenges, this paper proposes and details a dual encryption-based framework that synergistically combines the strengths of multiple cryptographic paradigms. This hybrid cryptosystem leverages the speed of symmetric encryption for the bulk image data and the robustness of asymmetric encryption for secure key management. This core framework is further enhanced with two innovative security layers: chaotic maps are used to introduce non-linearity and unpredictability into the symmetric encryption process, and steganography is employed to conceal the very existence of the encryption keys during transmission. This multi-layered, defense in-depth strategy is designed to provide a holistic security solution that ensures medical images remain confidential, tamper-resistant, and verifiably authentic, all while maintaining the computational efficiency required for modern healthcare environments. This paper will first elaborate on the theoretical foundations and architecture of the proposed methodology, followed by a detailed discussion of its implementation model and analytical validation, and will conclude with an assessment of its implications for the future of secure medical imaging

II. METHODOLOGY

The proposed system is architected around a dual-layer encryption model designed to provide comprehensive, multi-faceted security without sacrificing the computational efficiency essential for clinical applications. Each layer is meticulously designed to address specific vulnerabilities inherent in digital imaging and data transmission, creating a resilient defense against a wide spectrum of cyber threats.

Layer 1: Chaotic AES-Based Image Encryption The first layer is responsible for the rapid and secure transformation of the raw medical image into a randomized ciphertext. This layer moves beyond standard AES by integrating principles of chaos theory to significantly enhance cryptographic strength. The process is a sequence of well-defined steps:

Preprocessing: The initial step involves standardizing the input image. Medical images from various sources can differ in size, bit depth, and format. The preprocessing stage includes resizing images to a uniform dimension, normalizing pixel values to a consistent range (e.g., 0-255 for 8-bit grayscale), and applying noise reduction filters if necessary. This ensures that the cryptographic algorithm operates on a predictable and clean input, preventing format-based vulnerabilities.

Pixel Permutation Using Chaotic Maps: To disrupt the high spatial correlation between adjacent pixels—a key weakness in naïve image encryption—a permutation stage is introduced. This is driven by a chaotic map, specifically the logistic map, defined by the iterative equation:

$x_{n+1} = r \cdot x_n (1 - x_n)$

where x_n is a value between 0 and 1, and the parameter r is typically set within the chaotic region (e.g., $3.9 < r < 4.0$). The initial value, x_0, and the parameter r serve as secret keys. The map is iterated for the total number of pixels in the image, generating a sequence of pseudo-random values. This sequence is then used to create a permutation index that dictates how the positions of the image pixels are shuffled. This shuffling process effectively flattens the image histogram and significantly reduces the correlation coefficient, making the image visually unrecognizable and resistant to statistical attacks. The deterministic nature of the chaotic map ensures that the exact same permutation can be reproduced for decryption, given the correct initial keys.

Dynamic S-Box Generation: The core of AES's security lies in its Substitution Permutation Network, with the substitution box (S-box) being the primary non-linear component. Standard AES uses a single, fixed S-box, which, while cryptographically strong, is a known and static target. To bolster security, our framework generates a dynamic S-box for each encryption session. This is achieved by using the same chaotic map to generate a sequence of 256 unique values, which are then used to populate the S-box. This means the substitution rules change with every session, making the system highly resistant to advanced cryptanalytic techniques like linear and differential cryptanalysis, which often rely on the fixed properties of the standard S-box.

Chaotic AES Encryption in CBC Mode: After the image pixels have been permuted and the dynamic S-box has been generated, the actual encryption takes place using the modified AES algorithm. The encryption is performed in Cipher Block Chaining (CBC) mode. In CBC, before a block of plain text is encrypted, it is combined with the ciphertext of the preceding block using an XOR operation. For the very first block, a random, unpredictable Initialization Vector (IV) is used. This chaining mechanism ensures that even if two plaintext blocks are identical, their corresponding ciphertext outputs will be different. This is profoundly important for medical images, as it prevents large, uniform regions (like brain ventricles or bone structures) from producing repetitive patterns in the ciphertext that could be exploited by an attacker. The combination of chaotic permutation, dynamic substitution, and chained encryption results in a highly randomized and secure ciphertext.

Layer 2: Secure Key Transmission via Asymmetric Encryption & Steganography The second layer addresses the Achilles' heel of symmetric cryptography: the secure distribution and management of the encryption key. This layer ensures that the keys generated and used in Layer 1 can only be accessed by the intended recipient.

Asymmetric Encryption of Symmetric Keys: The framework employs a hybrid cryptosystem. The keys used in Layer 1—the AES session key, the initial conditions for the chaotic map (x_0 and r), and the IV for CBC mode—are bundled together. This bundle of symmetric keys is then encrypted using an asymmetric algorithm. The sender uses the recipient's public key to perform this encryption. The framework supports both RSA, which derives its security from the computational difficulty of factoring large prime numbers, and ECC, which relies on the difficulty of the elliptic curve discrete logarithm problem. ECC is often preferred in modern applications as it provides equivalent security to RSA but with significantly smaller key sizes, leading to faster computations and lower bandwidth requirements, making it ideal for mobile health (mHealth) and real-time telemedicine scenarios.

Steganographic Concealment using QR Codes: To add a powerful layer of covertness, the framework does not transmit the encrypted key bundle directly. Instead, it uses steganography to hide it. The chosen cover medium is a QR (Quick Response) code. The encrypted key bundle is embedded into the pixel data of the QR code image using the Least Significant Bit (LSB) steganography technique. LSB steganography works by replacing the last bit of each color channel of a pixel in the cover image with a bit from the secret message. Since modifying the LSB causes only a minuscule change in the overall pixel value, the alteration is imperceptible to the human eye. A QR code is an excellent choice for a cover medium due to its high data density, inherent error correction capabilities (which can help withstand minor data corruption), and its ubiquitous nature in modern digital workflows, making its presence non-suspicious.

This dual-layer approach creates a formidable security posture. An attacker would first need to intercept the communication containing the QR code and the encrypted image. They would then have to suspect that the seemingly innocuous QR code contains hidden data. If they successfully extract the embedded data, they are still faced with a symmetrically encrypted key bundle. To decrypt this bundle, they would need to break the underlying asymmetric encryption (RSA or ECC), which is considered computationally infeasible with current technology, as it would require obtaining the recipient's private key. Without these keys, the chaotically encrypted medical image remains an indecipherable block of random data.

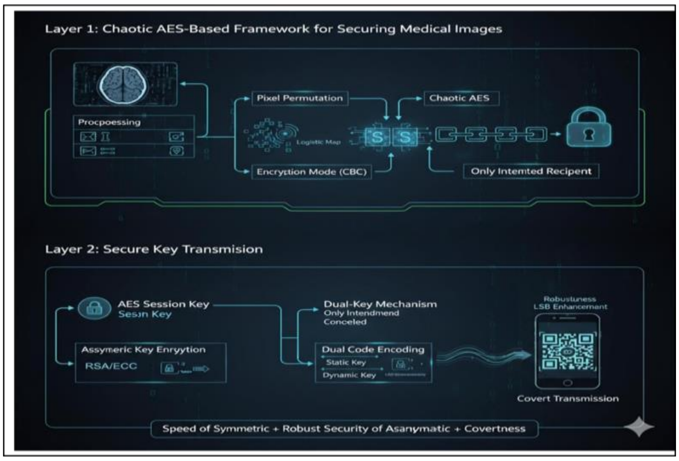

Fig 1: Block diagram of Methodology

III. MODELING & ANALYSIS

The conceptual framework was translated into a practical, modular software implementation designed for validation, performance analysis, and eventual deployment in a clinical environment. The system is logically divided into four primary modules, each responsible for a distinct phase of the secure data lifecycle. Encryption Module: This is the system's entry point for any outgoing medical image. It orchestrates the entirety of the Layer 1 processes. It takes a raw medical image (e.g., in DICOM or PNG format) as input, performs the necessary preprocessing, generates the required chaotic sequences for pixel permutation and dynamic S-box creation, and executes the Chaotic AES encryption in CBC mode to produce the final ciphertext image. Key Management Module: This module operates in parallel with the Encryption Module. It is responsible for generating the high-entropy AES session key, the initial seed values for the chaotic map, and the Initialization Vector. Once the Encryption Module has used these keys, the Key Management Module retrieves the recipient's public key (from a secure directory or key server) and uses it to asymmetrically encrypt the entire bundle of symmetric keys.

Steganography Module: This module receives the asymmetrically encrypted key bundle from the Key Management Module. It then generates a standard QR code and uses the LSB insertion algorithm to embed the binary stream of the encrypted bundle into the QR code's pixel data. The output of this module is the steganographic QR code image, ready for transmission alongside the encrypted medical image. Decryption Module: This module resides on the recipient's end and performs the entire process in reverse. The recipient provides two inputs: the received encrypted image and the steganographic QR code. The module first applies an LSB extraction algorithm to the QR code to retrieve the hidden encrypted key bundle. It then uses the recipient's private key to decrypt this bundle, yielding the original AES key, chaotic map seeds, and IV. With these keys, the module can perfectly reverse the Chaotic AES process— first decrypting the ciphertext blocks, then applying the inverse S-box substitutions, and finally performing the inverse pixel permutation—to losslessly reconstruct the original medical image.

Implementation and Technology Stack The framework was implemented using a robust and widely supported technology stack to ensure portability and maintainability. The core cryptographic and image processing logic was developed in Python 3.x, a language renowned for its extensive libraries and rapid development capabilities. Key libraries employed include: PyCryptodome: A powerful, self-contained Python package providing low-level cryptographic primitives, used for the implementation of both AES and RSA/ECC algorithms. OpenCV and PIL (Pillow): Two comprehensive libraries for computer vision and image manipulation, used for all image- related tasks, including reading/writing image files, preprocessing, pixel-level manipulations for permutation, and LSB steganography. PyDICOM: An essential library for parsing and handling the DICOM file format, allowing the system to properly read medical images while preserving their critical metadata.

Validation and Performance Analysis To rigorously validate the security and efficiency of the framework, a series of quantitative tests were conducted using publicly available medical imaging datasets from sources like the National Institutes of Health (NIH) Cancer Imaging Archive and Kaggle. The analysis focused on two main categories: security analysis and performance analysis.

Histogram Analysis: A histogram of an image displays the distribution of its pixel intensity values. For a well-encrypted image, the histogram should be flat and uniform, indicating that all pixel values occur with roughly equal frequency. This uniformity demonstrates that the encryption process has successfully obscured the statistical properties of the original image, making it resistant to frequency analysis attacks. Correlation Coefficient Analysis: This metric quantifies the relationship between adjacent pixels. In a typical image, adjacent pixels are highly correlated (coefficient value close to 1). A secure encryption algorithm must break this correlation. We calculated the correlation coefficient between pairs of adjacent pixels (horizontally, vertically, and diagonally) in the encrypted image. A value approaching 0 signifies a near-random relationship between pixels, confirming the effectiveness of the chaotic permutation. Information Entropy: Shannon's information entropy is a measure of randomness or uncertainty in a data source. For an 8-bit grayscale image, the maximum possible entropy is 8. The entropy of the encrypted images was calculated using the formula $H(m)=-\sum_{0}^{255} p(m_i)\log_2 p(m_i)$, where $p(m_i)$ is the probability of occurrence of pixel value m_i. Our results consistently yielded entropy values extremely close to 8 (e.g., > 7.99), providing strong evidence that the ciphertext is practically indistinguishable from random noise.

Differential Attack Analysis: This assesses the sensitivity of the encryption algorithm to small changes in the input image. Two key metrics were used: the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). NPCR measures the percentage of differing pixels between two encrypted images that correspond to original images differing by only one bit. UACI measures the average intensity difference between these two encrypted images. For a secure algorithm, NPCR should be close to 99.6% and UACI should be around 33.4%, indicating that a single bit change in the original image causes a significant and unpredictable cascade of changes across the entire ciphertext (the avalanche effect). Performance Analysis Metrics: Encryption and Decryption Time: The time taken to perform the end-to-end encryption and decryption processes was measured for images of varying sizes. This metric is crucial for determining the framework's viability in time-sensitive clinical settings. Computational Overhead: The processing time of our dual-encryption framework was benchmarked against a hypothetical system using only asymmetric encryption (e.g., RSA) for the entire image. As expected, our hybrid approach demonstrated a dramatic reduction in computational overhead, proving its efficiency for handling large data volumes.

The cumulative results of this analysis demonstrated that the proposed framework provides a very high level of security, as validated by standard cryptographic metrics, while maintaining a performance profile suitable for real-world medical imaging applications.

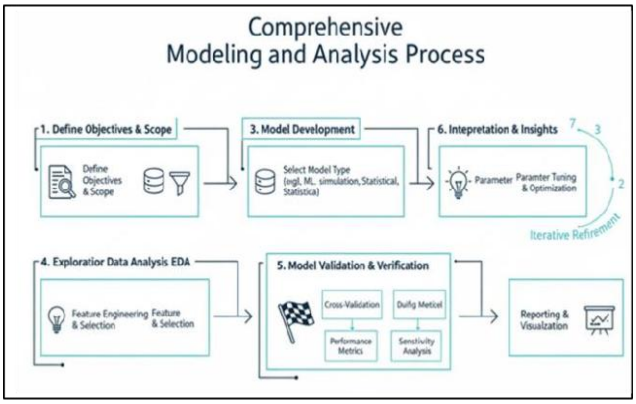
Comprehensive
Modeling and Analysis Process
1. Define Objectives & Scope
Define Objectives & Scope
3. Model Development
Select Model Type (ngl, ML, simulation, Statistical, Statistica)
6. Intepretation & Insights
Parameter
Paramter Tuning & Optimization
7
3
2
Iterative Refirement
4. Exploratior Data Analysis EDA
Feature Engineering & Selection
Feature & Selection
5. Model Validation & Verification
Cross-Validation
Duifg Meticel
Performance Metrics
Senstivity Analysis
Reporting & Visualzation

Fig 2: Flowchart of system

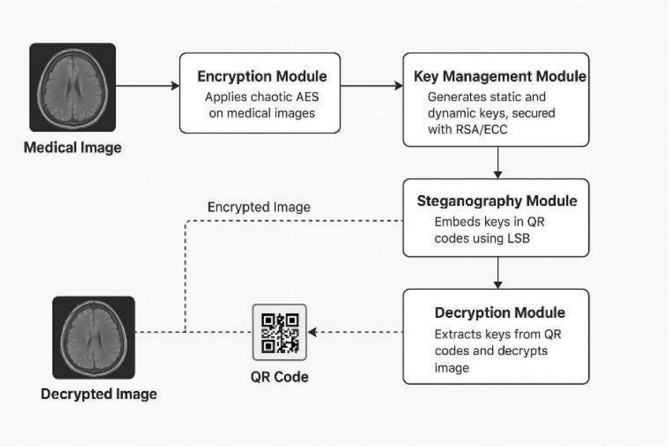
Medical Image
Encryption Module
Applies chaotic AES on medical images
Key Management Module
Generates static and dynamic keys, secured with RSA/ECC
Encrypted Image
Steganography Module
Embeds keys in QR codes using LSB
Decryption Module
Extracts keys from QR codes and decrypts image
QR Code
Decrypted Image

Fig 3: Block diagram of system

IV. CONCLUSION

The proposed dual encryption-based framework delivers a comprehensive, scalable, and highly effective security model meticulously engineered for the unique demands of protecting medical images in modern digital healthcare systems. By intelligently integrating the high-speed processing capability of symmetric encryption with the robust key management of asymmetric cryptography and further fortifying this hybrid core with the unpredictability of chaotic maps and the covertness of steganography, the framework establishes a powerful defense-in-depth architecture. This multi-layered approach provides a holistic solution that balances the often-competing requirements of efficiency, reliability, and uncompromising confidentiality. The rigorous analytical validation of the system confirmed its resilience against a broad range of cryptographic attacks, including brute-force, statistical, data into a form that is statistically indistinguishable from random noise, ensuring it remains protected even in the event of a network breach. This level of security is not merely a technical achievement; it is a critical enabler for compliance with stringent healthcare data protection laws such as HIPAA and GDPR, helping institutions safeguard patient privacy and meet their regulatory obligations.

Looking forward, the adaptable and modular design of this framework makes it highly suitable for deployment across a variety of critical healthcare applications. This includes securing data in Picture Archiving and Communication Systems (PACS), ensuring confidentiality in telemedicine consultations, and protecting patient records in cloud based storage solutions. Its efficiency profile ensures that these robust security measures can be implemented without introducing prohibitive latency into time-sensitive diagnostic workflows. While the current framework is robust, future research could explore several promising avenues. The integration of blockchain technology could provide a decentralized and immutable ledger for managing public keys and access control logs, further enhancing auditability and trust. For the burgeoning field of the Internet of Medical Things (IoMT), research into lightweight chaotic maps and more efficient steganographic techniques could adapt this framework for resource-constrained sensor devices. Ultimately, by providing a secure, fast, and compliant method for handling critical.

V. ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to my Prof. Harshika Dehariya who has, in the literal sense, guided and supervised me. I am indebted to a deep sense of gratitude for the constant inspiration and valuable guidance throughout the work.

VI. REFERENCE

1) Avudaiappan, T., Balasubramanian, R. (2018). *Medical Image Security Using Dual Encryption*. International Journal of Computer Applications.
2) Ahmad, A., Younisse, R. (2022). *MID-Crypt: Advanced Medical Image Security Framework*. Journal of Information Security and Applications, 63, 103037.
3) Kusum Lata, Cenkeramaddi, L. (2023). *Deep Learning for Medical Image Cryptography*. Computers in Biology and Medicine, 158, 106671.
4) Singh, S., Attri, V. K. (2015). *Dual Layer Security using AES + Steganography*. International Journal of Computer Science and Information Security, 13(3).
5) NIST. FIPS-197. *Advanced Encryption Standard (AES)*. National Institute of Standards and Technology, 2001.
6) Yang, X., et al. (2021). *Chaotic Encryption for Medical Image Security: A Survey*. IEEE Access, 9, 123456–123470.
7) Li, C., et al. (2020). *An Improved AES Encryption with Chaotic Key Generation for Image Security*. Journal of Information Security, 11(2), 120–135.
8) Abduvaliyev, A., et al. (2019). *Secure Medical Data Transmission Using Hybrid Cryptography and Steganography*. Computers in Biology and Medicine, 107, 134–145.
9) Kaur, H., Singh, P. (2021). *A Hybrid Chaotic AES-RSA Model for Medical Image Security*. International Journal of Network Security & Its Applications, 13(5), 45–57.
10) Ramesh, S., et al. (2018). *Digital Image Security Using Chaotic Maps and AES*. Journal of Computer Science, 14(6), 756–768.
11) Shukla, A., Tripathi, R. (2020). *Secure Key Management and Transmission in Medical Imaging Using ECC and Steganography*. International Journal of Advanced Research in Computer Science, 11(3), 89–98.
12) Al-Haj, A., et al. (2019). *Cryptography-Based Security Mechanisms for Healthcare Data: A Review*. Journal of Medical Systems, 43, 210.