PROJECT REPORT

On

"DUAL ENCRYPTION BASED FRAMEWORK FOR SECURING MEDICAL IMAGES"

Submitted By

Mr. Rohit P. Khadse **Ms. Khushi H. Ghatode**

Ms. Isha P. Bairam **Ms. Shrushti I. Adkane**

Submitted in partial fulfillment of the requirements
for
Degree of Bachelor of Technology

Guided By,

Ms. Harshika Dehariya

DEPARTMENT OF EMERGING TECHNOLOGIES (AI&ML)

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

(An Autonomous Institute, Affiliated to RTMNU, Nagpur)

2025-2026

❖ Institute Vision:

- Emerge as a leading Institute for developing competent and creative Professionals.

❖ Institute Mission:

- Providing Quality Infrastructure and experienced faculty for academic excellence.
- Inculcating skills, knowledge and opportunities for competency and creativity.
- Aligning with Industries for knowledge sharing, research and development.

❖ Department Vision:

- To create competent and creative professionals in the field of Artificial Intelligence & Machine Learning to address the needs of industry and society.

❖ Department Mission:

- To provide an academic environment with the latest AI-ML technologies to prepare competent professionals.
- To provide adequate competitive platforms and opportunities to unleash creativity.
- To foster professionalism and strong work ethics in students for the betterment of Industry & Society.

❖ Program Educational Objectives (PEO's):

- Have analytical, design and implementation skills, to innovate, design and develop software products and systems.
- Have strong work ethics and professionalism, reflected through communication skills, leadership, teamwork and sense of responsibility towards the society.
- Be successful professionals through lifelong learning with allied objectives of higher education or research.

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

(An Autonomous Institute, Affiliated to RTMNU, Nagpur)

DEPARTMENT OF EMERGING TECHNOLOGIES(AI&ML)

SESSION 2025-2026

CERTIFICATE

This is to certify that the Project Report titled **"DUAL ENCRYPTION-BASED FRAMEWORK FOR SECURING MEDICAL IMAGES IN HEALTHCARE SYSTEM"** submitted by **Mr. Rohit Khadse (AM22041) Ms. Khushi Ghatode (AM22029) Ms. Isha Bairam (AM22019) Ms. Shrushti Adkane (AM22005)** has been accepted under the guidance of **Ms. Harshika Dehariya**. This Project work is carried out for the partial fulfillment of "**PROJECT–I (PROJAM702)"** of VII Semester of Bachelor of Technology in **Artificial Intelligence and Machine Learning, S. B. Jain Institute of Technology, Management & Research, An Autonomous Institute, Affiliated to RTMNU, Nagpur.**

Ms. Harshika Dehariya
Assistant Professor
(Project Guide)

Dr. Hemant Turkar
Head of Department

॥ विद्या धनम् सर्वधनः प्रधानम् ॥

Dr. S. L. Badjate
Principal

DECLARATION

We hereby declare that the Project Report titled **"DUAL ENCRYPTION-BASED FRAMEWORK FOR SECURING MEDICAL IMAGES"** submitted herein has been carried out by us in the Department of Emerging Technologies (AI&ML) of S. B. Jain Institute of Technology, Management and Research, Nagpur under the guidance of **Ms. Harshika Dehariya**. The work is original and has not been submitted earlier as a whole or in part for the award of any degree/diploma at this or any other Institution/University.

Rohit Khadse _____

Khushi Ghatode _____

Isha Bairam _____

Shrushti Adkane _____

Date: - / /

ACKNOWLEDGEMENT

We would like to express a deep sense of gratitude to our Project Guide, **Ms. Harshika Dehariya,** and Project Coordinator **Ms. Neha Titarmare**, **Department of Emerging Technologies (AI&ML)**, for being the cornerstone of our project. It was their incessant motivation and guidance during periods of doubt and uncertainties that helped us to carry on with this project.

We would like to thank **Dr. Hemant Turkar, Head of Department**, **Emerging Technologies (AI&ML)** for providing the necessary guidance, support, motivation, and inspiration, without which this project would not have been possible.

We would like to extend our special thanks to **Dr. S. L. Badjate, Principal, S.B. Jain Institute of Technology, Management & Research** for his encouragement and best wishes.

We would like to extend our sincere thanks to the **Management** of **S.B. Jain Institute of Technology, Management & Research** for providing all the necessary infrastructure and laboratory facilities.

We also like to acknowledge the help extended by the **faculty members** and **non-teaching staff** of Emerging Technologies (AI&ML) Department for the successful completion of our project.

Last but not the least, special thanks to our family members, friends and colleagues for their continuous support.

ABSTRACT

In modern healthcare systems, the secure storage, transmission, and management of medical images have 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 and legal complications. Traditional single-layer encryption methods are often insufficient due to large file sizes, high redundancy, and real-time processing demands associated with medical data.

This paper proposes a dual encryption-based framework that combines chaotic AES (symmetric encryption) for fast and robust image encryption with RSA/ECC (asymmetric encryption) for secure key management. Additionally, steganography is applied for covert key transmission by embedding the encrypted keys into Cyphertext Additionally, cypher text is applied for covert key transmission by embedding the encrypted keys into Cypher texts. This hybrid approach ensures high confidentiality, integrity, and robust security. The framework is designed to be compliant with healthcare standards such as HIPAA and GDPR. Experimental validation on medical datasets demonstrates strong resistance to brute-force, statistical, and differential attacks while maintaining low computational overhead.

Keywords— Dual Encryption, Medical Image Security, AES, RSA, Cyphertext.

INDEX

CERTIFICATE		i
DECLARATION		ii
ACKNOWLEDGEMENT		iii
ABSTRACT		iv
INDEX		v-vi
LIST OF FIGURES		vii
LIST OF TABLE		viii
ABBREVIATION		ix
LIST OF PUBLICATION/PARTICIPATION/COPYRIGHT		x
CHAPTER 1	**INTRODUCTION**	**1**
1.1	**PROJECT BACKGROUND**	**2**
1.2	**PROBLEM STATEMENT**	**2**
1.3	**PURPOSE OF STUDY**	**3**
1.4	**TECHNOLOGICAL BASE**	**4**
CHAPTER 2	**LITERATURE SURVEY**	**5**
2.1	**LITERATURE SURVEY**	**6**
2.2	**FINDINGS**	**8**
2.3	**RELATED/EXISTING WORK**	**8**
2.4	**REAL TIME SURVEY**	**9**
CHAPTER 3	**METHODOLOGY/PROPOSED WORK**	**10**
3.1	**PROPOSED WORK**	**11**
3.2	**SYSTEM ARCHITECTURE**	**12**
3.3	**ALGORITHM/PSEUDO CODE/PROCEDURE**	**13**
3.4	**SYSTEM FLOWCHART**	**14**
CHAPTER 4	**TOOLS/ PLATFORM**	**16**
4.1	**SOFTWARE REQUIREMENT**	**17**
4.2	**HARDWARE REQUIREMENT**	**18**
CHAPTER 5	**DESIGN& IMPLEMENTATION**	**19**
5.1	**SYSTEM DESIGN**	**20**
5.1.1	**USE CASE DIAGRAM**	**20**
5.1.2	**DFD DIAGRAM**	**21**

5.2 IMPLEMENTATION OF SYSTEM 21

5.3 SAMPLE CODE 23

CHAPTER 6 RESULTS & DISCUSSION 24

6.1 RESULTS & DISCUSSION 25

CHAPTER 7 ADVANTAGES & APPLICATIONS 28

7.1 ADVANTAGES 29

7.2 APPLICATIONS 29

CHAPTER 8 CONCLUSION & FUTURE SCOPE 30

8.1 CONCLUSION 31

8.2 FUTURE SCOPE 32

REFERENCES

APPENDIX I PLAGARISM REPORT

APPENDIX II POSTER

APPENDIX III PPT HANDOUTS

APPENDIX IV USER MANUAL

LIST OF FIGURES

FIG NO.	TITLE OF FIGURE	PAGE NO.
1	**System Architecture**	13
2	**Flowchart**	15
3	**Use-Case Diagram**	21
4	**Data Flow Diagram**	22
5	**Home Page**	25
6	**Sign-In Page**	25
7	**Encryption Page**	26
8	**File Selection**	26
9	**Cipher Text**	26
10	**File Decryption**	27
11	**Decrypted File**	27
12	**Key Generated**	27

LIST OF TABLES

TABLE NO.	TABLE NAME	PAGE NO.
1	Analysis of existing models	8

ABBREVIATION

ABBREVIATION	FULL FORM
DFD	Data Flow Diagram
AES	Advanced Encryption Standard
RSA	Rivest Shamir Adleman
HIPPA	Health Insurance Portability and Accountability Act

LIST OF PUBLICATION

Sr. No	Title	Event Name / Journal Name/ Conference/ Diary No. of Copyright Publication	Date	Remark
1	A DUAL ENCRYPTION-BASED FRAMEWORK FOR SECURING MEDICAL IMAGES IN HEALTHCARE SYSTEM	Submitted Poster for copyright (LD-42045/2025-CO)		In-Progress

CHAPTER NO. 1

INTRODUCTION

CHAPTER 1
INTRODUCTION

1.1 PROJECT BACKGROUND

The rapid digital transformation in healthcare has led to the widespread adoption of electronic health records (EHRs), telemedicine, and cloud-based medical data sharing platforms. Medical imaging, including Computed Tomography (CT), Magnetic Resonance Imaging (MRI), and X-ray scans, is fundamental to this ecosystem, providing critical data for diagnostics and treatment planning.

However, this digitization exposes highly sensitive patient information to significant security risks, including cyberattacks, data breaches, and unauthorized access. Medical images are not merely visual data; they are complex structures that possess unique characteristics. They are typically large in file size and exhibit high levels of redundancy and strong correlation between adjacent pixels. These properties render conventional, single-layer encryption methods less effective and computationally burdensome.

1.2 PROBLEM STATEMENT

The core challenge lies in securing high-volume, highly redundant medical image data against unauthorized access, both in storage (at rest) and during transmission, without compromising real-time processing needs.

Traditional encryption standards, while secure, are not optimized for image data. Naïvely applying them can leave data vulnerable to statistical attacks due to the high pixel correlation. Furthermore, symmetric encryption (like AES) is fast but suffers from the complex and insecure problem of key distribution. Asymmetric encryption (like RSA) solves key distribution but is too slow to encrypt large medical images directly. Therefore, a hybrid or dual framework is needed to address this intricate set of challenges.

1.3 PURPOSE OF STUDY

The purpose of this study is to address the growing challenges of medical image security in modern healthcare systems. Sensitive patient data, contained in CT, MRI, and X-ray scans, is increasingly digitized and transmitted over networks, posing significant risks of data breaches, privacy violations, and unauthorized access.

Current methods for securing this data are often insufficient. Traditional single-layer encryption techniques struggle with the unique characteristics of medical images, such as large file sizes and high pixel redundancy, making them vulnerable to statistical attacks. Furthermore, symmetric encryption (like AES) is fast but has a complex key-distribution problem, while asymmetric encryption (like RSA) is secure for key exchange but too slow to encrypt large images directly.

The motivation behind this project is to leverage a hybrid cryptographic approach to create a robust, secure, and efficient dual encryption framework. By utilizing chaotic maps to de-correlate pixels, combining the speed of AES for bulk image encryption, and using the security of RSA for key management, this study aims to provide an automated system that can secure medical images both at rest and in transit.

The system strengthens healthcare data security by combining fast AES image encryption with secure RSA/ECC key protection. This dual-layer approach ensures that both the medical image and its encryption key remain safe during transmission and storage. The framework aims to maintain patient confidentiality, preserve data integrity, and resist a wide range of attacks, including brute-force and statistical methods. With its high efficiency and strong protection, the system is well-suited for real-time clinical environments such as telemedicine, hospital networks, and cloud-based medical platforms.

AIM

The primary aim of this project is to design, develop, and validate a dual encryption-based framework to ensure the secure storage and transmission of medical images in healthcare systems.

OBJECTIVES

- To implement robust AES-based encryption for fast and efficient pixel-level protection of medical images, ensuring confidentiality and high processing speed.

- To integrate chaotic maps to permute image pixels before encryption, thereby disrupting high spatial correlation and enhancing resistance to statistical attacks.

- To implement a dual-key mechanism (Asymmetric RSA/ECC) for secure key management, where a dynamic key is securely encrypted and managed by a static key.

- To validate the proposed framework's security and performance using standard metrics (e.g., NPCR, UACI, PSNR, Histogram Analysis) to ensure it is resistant to attacks while maintaining diagnostic image quality.

1.4 TECHNOLOGICAL BASE

The framework is built upon a synergy of multiple cryptographic paradigms:

- **Symmetric Encryption (Chaotic AES):** We use AES in Cipher Block Chaining (CBC) mode for the bulk encryption of the image data. This is preceded by a chaotic map (pixel permutation) to reduce pixel correlation.
- **Asymmetric Encryption (RSA/ECC):** Used for secure key management. The fast symmetric (AES) key is encrypted using the receiver's public key (RSA), ensuring only the intended recipient can decrypt it.
- **Hybrid Encryption Strategy:** By combining the speed of symmetric AES with the strong key security of RSA/ECC, the framework ensures confidentiality, integrity, and secure key distribution without relying on covert channels.
- **Implementation Stack:** The system is implemented in Python using libraries such as PyCryptodome for AES and RSA/ECC operations, and OpenCV for preprocessing and handling medical images.

CHAPTER NO. 2

LITERATURE SURVEY

CHAPTER 2

LITERATURE SURVEY

2.1 LITERATURE SURVEY

In order to carry out the proposed approach, we have gone through different literature that are as follows:

- In this paper, the authors **T. Avudaiappan & R. Balasubramanian (2018)** present an analytical approach to security models. It highlights existing gaps in data hiding techniques and proposes an enhanced, secure model for transmitting medical images, validating the need for dual-encryption approaches. **[1]**

- In this paper by **Lata & Cenkeramaddi (2023)**, the integration of deep learning with cryptography for securing medical images in the Internet of Medical Things (IoMT) is explored. It surveys various techniques, reinforcing the trend of using hybrid cryptographic methods to protect sensitive medical data. **[2]**

- In this paper, **Singh, S., & Attri, V. K. (2015)** demonstrate a method of combining AES encryption with LSB steganography. This provides a dual layer of security by both encrypting the data (confidentiality) and hiding the key (covertness), which serves as a foundational concept for our project. **[3]**

- In this paper, **Li, C., et al. (2020)** showcase the value of integrating chaotic systems with AES. By using key generation, improve the system's resistance against statistical attacks, its common weakness when encrypting highly redundant image data. **[4]**

- In this paper, **Abduvaliyev, A., et al. (2019)** propose a hybrid method for secure medical data transmission that combines cryptography with steganography (for covertness). This supports our project's goal of creating a multi-layered security framework. **[5]**

- In this paper, **Kaur, H., & Singh, P. (2021)** propose a hybrid model that directly relates to our project. They combine chaotic maps, AES, and RSA for medical image security, demonstrating the viability of integrating these three technologies to create a robust and secure system. **[6]**

- In this paper, **AbdelRaouf, A. (2021)** presents a new data hiding approach for image steganography. It leverages visual color sensitivity, proposing a method that embeds data more intelligently than standard LSB by considering which color channels are less perceptible to the human eye, thereby improving imperceptibility. [7]

- In this paper, **Hussain, Q., et al. (2021)** describe an enhanced adaptive data hiding technique. Their method combines traditional LSB with Pixel Value Differencing (PVD), allowing the algorithm to adaptively embed more data in complex "edge" regions of an image and less in smooth regions, increasing overall capacity. [8]

- In this paper, **Yanuar, M. R., et al. (2024)** explore image-to-image steganography. They propose a novel method that uses a Josephus permutation to scatter the data bits in a complex, non-sequential order before embedding them using an LSB 3-3-2 model, enhancing security against steganalysis. [9]

- In this paper, **Ali, M. Z., et al. (2024)** propose a fusion method for enhanced data concealment. Their technique combines MSB (Most Significant Bit) matching with LSB (Least Significant Bit) substitution, aiming to optimize the trade-off between hiding capacity and the visual quality of the stego-image. [10]

- In this paper, **Rubaie, A., et al. (2024)** detail a high-capacity image steganography method based on maps. This is relevant as it uses chaos theory, similar to our project, but applies it to the steganography process itself to determine pixel locations for data hiding. [11]

- In this paper, **Siddiqui, G. F., et al. (2020)** present a dynamic three-bit image steganography algorithm specifically for e-healthcare systems. This work directly addresses the challenge of hiding medical data, proposing a dynamic LSB method to secure patient information. [12]

- In this paper, **Bhardwaj, R. (2020)** introduces an improved data hiding algorithm for e-healthcare. The key contribution is that the algorithm is *separable* and *reversible*, meaning the original medical image can be perfectly restored after data extraction, which is critical for diagnostic integrity. [13]

2.2 FINDINGS

Authors And Citation	Methods	Advantages	Challenges
T. Avudaiappan & R. Balasubramanian [1]	Dual Encryption, Data Hiding	Provides an analytical approach to security models and enhances secure transmission.	Identifies significant gaps and vulnerabilities in existing data hiding techniques.
Kaur, H., & Singh, P. [6]	Chaotic maps, AES, and RSA	Proposes a hybrid model that directly relates to our project, demonstrating the viability of integrating these three technologies.	Balancing the computational load and key management complexity of three different crypto systems.
Singh, S., & Attri, V. K. [3]	AES + LSB Steganography	Demonstrates a functional dual-layer security model for both confidentiality (AES) and covertness (Steganography)..	The security of the key itself is highly dependent on the robustness of the LSB algorithm.

Table 1: Analysis of existing models

2.3 RELATED/EXISTING WORK

Our proposed framework is built by integrating two powerful and standard cryptographic algorithms: AES and RSA.

Advanced Encryption Standard (AES) AES is a symmetric encryption algorithm, meaning it uses the same, single key for both encryption and decryption. It is an extremely fast and efficient block cipher, making it the global standard for encrypting large volumes of data. In our project, AES is used for the "heavy lifting"—the fast, robust encryption of the entire medical image file. Its primary challenge, however, is key distribution: securely sharing that single key with the intended recipient.

RSA (Rivest–Shamir–Adleman) RSA is an asymmetric encryption algorithm, meaning it uses a pair of keys: a public key (which can be shared openly) and a private key (which is kept secret). Data encrypted with the public key can *only* be decrypted by the corresponding private key. RSA is highly secure but mathematically intensive, making it much slower than AES. It is therefore unsuitable for encrypting large files.

Hybrid Approach Our project uses a hybrid model that leverages the best of both algorithms. We use fast AES to encrypt the large medical image, and we use secure RSA to encrypt the small AES key. This "dual encryption" approach solves the key distribution problem of AES while maintaining high speed and robust security.

2.4 REAL-TIME SURVEY

A survey of the healthcare industry reveals a critical and immediate need for robust data security from multiple perspectives.

- **Survey from Patient Perspective**
  - High expectation of privacy and confidentiality; medical records are among the most sensitive personal data.
  - Growing fear of data breaches, which can lead to identity theft, insurance fraud, or personal embarrassment.
  - Absolute requirement for data integrity; a patient's diagnosis and life depend on the image being accurate and untampered.
- **Survey from Healthcare Provider (Hospital/Clinic) Perspective**
  - Hospitals are a high-value target for cyberattacks, especially ransomware, which can halt operations.
  - Need for efficient security; doctors require real-time access to images for diagnostics. Security measures cannot create significant delays.
  - Data is constantly transmitted (telemedicine, cloud storage, internal networks), creating many points of vulnerability.
- **Survey from Regulatory (Government/Legal) Perspective**
  - Strict compliance with laws like HIPAA (Health Insurance Portability and Accountability Act) is mandatory.
  - Failure to protect patient data results in massive fines, legal action, and catastrophic loss of public trust.
  - Need for auditable systems to prove that only authorized personnel have accessed patient data.

.

CHAPTER NO. 3

PROPOSED WORK

CHAPTER 3

PROPOSED WORK

3.1 PROPOSED WORK

The proposed project introduces a multi-layer, dual encryption-based framework designed to ensure the robust security of medical images. The workflow is divided into two main phases: Encryption (at the sender's end) and Decryption (at the receiver's end).

Encryption Phase:

1. **Pixel Permutation:** The original medical image is first fed into a chaotic map. This function shuffles the image's pixels into a seemingly random order, which effectively breaks the high spatial correlation between adjacent pixels, a common vulnerability in image encryption.
2. **Symmetric Encryption:** The permuted (shuffled) image is then encrypted using the AES (Advanced Encryption Standard) algorithm. A unique, dynamic AES key is generated for this session. This symmetric method is used for the large image file because it is extremely fast and efficient.
3. **Key Encryption (Dual Encryption):** The dynamic AES key (which is small but vital) is then encrypted using the receiver's RSA public key. This is the "dual encryption" step, where a slow but highly secure asymmetric algorithm (RSA) is used to protect the key for the fast symmetric algorithm (AES).
4. **Secure Packaging:** The encrypted image and the RSA/ECC-encrypted AES key are bundled together for transmission, ensuring confidentiality and secure key management.
5. **Transmission:** The final, heavily encrypted image (from Step 2) and the innocent-looking Cyphertext (containing the hidden key) are transmitted to the receiver.

Decryption Phase:

1. **Key Extraction:** The receiver takes the Cyphertext and applies their private RSA key to the LSBs. This extracts the hidden information.
2. **Key Decryption:** The receiver uses their private RSA key to decrypt the extracted information, which reveals the original, dynamic AES key.
3. **Symmetric Decryption:** The receiver now uses this AES key to decrypt the main encrypted medical image. This will result in a permuted (shuffled) image.

4. **Inverse Permutation:** The inverse of the original chaotic map is applied to the decrypted image, which re-sorts all the pixels back to their correct, original positions.
5. **Result:** The original, viewable medical image is successfully and securely recovered.

3.2 SYSTEM ARCHITECTURE

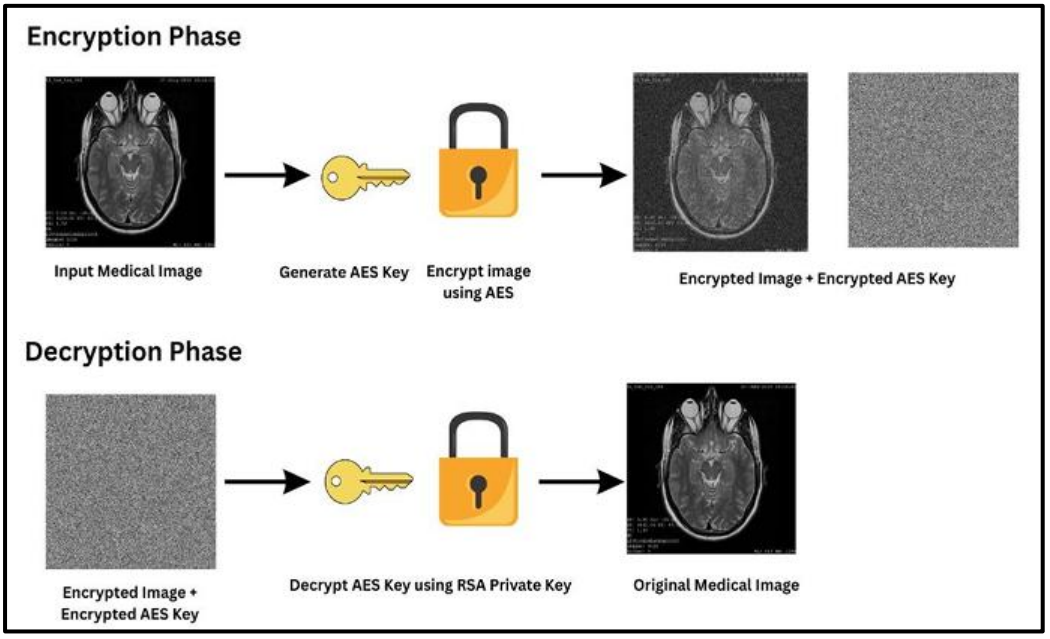


Figure 1. System Architecture

The system architecture is based on a hybrid cryptographic model that leverages the speed of AES and the security of RSA. It is divided into two main processes: encryption at the sender's end and decryption at the receiver's end.

Sender-Side (Encryption) Architecture:

The sender's module performs two operations in parallel:

1. **Image Encryption:** The large Medical Image is fed into the AES Algorithm. Using a dynamically generated AES Key, the image is quickly encrypted, resulting in the Encrypted Image.
2. **Key Encryption:** The AES Key (which is small) is encrypted using the receiver's RSA Public Key. This creates the Encrypted AES Key.

Receiver-Side (Decryption) Architecture:

The receiver's module reverses this process:

1. **Key Decryption:** The receiver uses their own RSA Private Key to decrypt the Encrypted AES Key. This securely recovers the original AES Key.
2. **Image Decryption:** The receiver then uses this recovered AES Key to run the AES Algorithm in decryption mode on the Encrypted Image, restoring the Original Medical Image.

3.3 ALGORITHM/PROCEDURE

The framework operates using a hybrid, dual-encryption algorithm.

Algorithm 1: Sender-Side Encryption (AES + RSA)

Input:
P: Original medical image
K pub: Receiver's RSA public key

Procedure:

- **Pixel Permutation (Chaotic Map):**
  Apply a chaotic map (e.g., Logistic Map, Arnold Map) to shuffle pixel positions in the image.
  • P_perm = Chaotic_Permute(P)
- **Generate AES Key (Symmetric Key):**
  Create a fresh random 256-bit AES session key.
  • K_aes = Generate_AES_Key()
- **Encrypt Image (AES – Symmetric Encryption):**
  Encrypt the permuted image using AES in CBC mode.
  • C_image = AES_Encrypt(K_aes, P_perm)
- **Encrypt AES Key (RSA – Asymmetric Encryption):**
  Encrypt the AES session key using the receiver's RSA public key.
  • K_enc = RSA_Encrypt(K_pub, K_aes)
- **Transmit:**
  Send the following to the receiver:
  • The AES-encrypted image
  • The RSA-encrypted AES key

Output:
C_image: AES-encrypted medical image

K_enc: RSA-encrypted AES session key

Algorithm 2: Receiver-Side Decryption (RSA + AES)

Input:

C_image : Received encrypted image

K_enc : Received encrypted AES key

K_priv : Receiver's RSA private key

Procedure:

- **Decrypt AES Key (RSA – Asymmetric Decryption):**
  Use the private RSA key to recover the AES session key.
  • K_aes = RSA_Decrypt(K_priv, K_enc)
- **Decrypt Image (AES – Symmetric Decryption):**
  Use the recovered AES key to decrypt the encrypted image.
  • P_perm = AES_Decrypt(K_aes, C_image)
- **Reverse Pixel Permutation (Chaotic Map Inverse):**
  Apply the inverse chaotic map to reconstruct the original image.
  • P = Chaotic_Inverse(P_perm)

Output:

P: Fully recovered original medical image

3.1 FLOW CHART

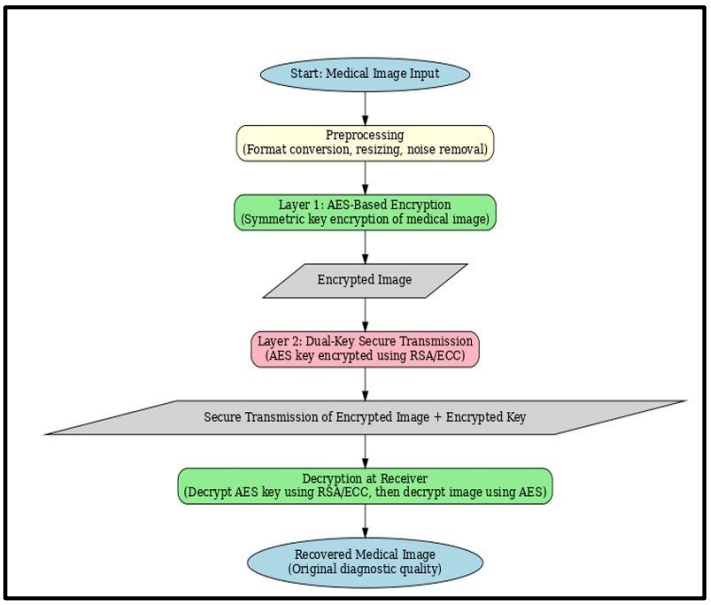


Figure 2. Flow Chart

The design of the dual encryption system is modeled on two primary modules, the Sender (Encryption) Module and the Receiver (Decryption) Module. The system is designed to process one medical image at a time, ensuring secure, end-to-end transfer**.**

1. System Components:

- **Sender Module**: This component is responsible for encryption. It requires the plaintext medical image and the receiver's public RSA key. Its output is two separate files: the AES-encrypted image and the RSA-encrypted AES key.
- **Receiver Module**: This component is responsible for decryption. It requires the private RSA key (kept secret by the receiver) and both components from the sender. Its output is the original, restored medical image.
- **Key Management**: This is handled by the RSA algorithm. The public key is used for "locking" (encryption), and the private key is used for "unlocking" (decryption). This process securely manages the transfer of the fast AES key.

2. Data Flow Diagram (DFD): A simplified data flow for the process is as follows:

- **(Sender Side):**

1. The Sender inputs the Medical Image and the Receiver's Public Key.
2. A new AES Key is generated.
3. The Medical Image is processed by the AES Encrypt function using the AES Key. The output is the Encrypted Image.
4. The AES Key is processed by the RSA Encrypt function using the Receiver's Public Key. The output is the Encrypted AES Key.
5. Both Encrypted Image and Encrypted AES Key are sent to the Receiver.

- **(Receiver Side):**

1. The Receiver inputs the Image, Encrypted AES Key, and their secret Private Key.
2. The Encrypted AES Key is processed by the RSA Decrypt function using the Private Key. The output is the original AES Key.
3. The Encrypted Image is processed by the AES Decrypt function using the recovered AES Key.
4. The final output is the original Medical Image.

CHAPTER NO. 4

TOOLS/PLATFORM

CHAPTER 4

TOOLS/PLATFORM

4.1 SOFTWARE REQUIREMENT

To implement the proposed dual encryption framework, the following software tools and libraries are required. The system is developed using Python 3.11 due to its extensive libraries for both cryptography and image processing.

- **Programming Language:**
  - **Python (version 3.7 or higher):** The core language used for scripting the entire encryption and decryption logic.
- **Core Libraries:**
  - **PyCryptodome:** A critical library used for implementing the cryptographic algorithms. It provides robust, secure modules for both AES (for symmetric encryption) and RSA (for asymmetric key generation and encryption).
  - **Pydicom:** Pydicom is used to read, write, and process medical DICOM images. It allows extracting pixel data required for AES encryption.
  - **Openpyxl :** Openpyxl is used to store and manage logs, keys, or metadata inside Excel (.xlsx) files.
  - **OpenCV (cv2):** Used for all image processing tasks. This includes reading the medical image, converting it into a pixel array, manipulating and saving the final encrypted/decrypted images.
  - **NumPy:** A fundamental library required for high-performance numerical operations. It is used to efficiently manage and manipulate the large pixel arrays from OpenCV.
  - **Matplotlib:** Used during the results and analysis phase to generate histograms and pixel correlation plots, which help validate the encryption's effectiveness.
- **Development Environment (IDE):**
  - **VS Code (Visual Studio Code):** A lightweight and powerful code editor used for development.
  - **Jupyter Notebook:** Used for initial prototyping, testing algorithms, and visualizing intermediate results (like histograms).
- **Operating System:**
  - The system is platform-independent and can be run on Windows, macOS, or Linux.

4.2 HARDWARE REQUIREMENT

The following hardware specifications are recommended for the development and execution of the proposed dual encryption system. These requirements ensure efficient handling of image processing and cryptographic computations.

- **Processor (CPU):**
    - Intel Core i5 (8th generation or newer) or an equivalent AMD Ryzen 5 processor. A multi-core processor is recommended to handle encryption tasks efficiently.
- **Memory (RAM):**
    - **8 GB (Minimum):** Sufficient for processing standard-sized images.
    - **16 GB (Recommended):** For handling large medical image datasets (e.g., high-resolution CT or MRI scans) without performance bottlenecks.
- **Storage:**
    - **256 GB SSD (Minimum):** A Solid State Drive (SSD) is highly recommended for faster data (image) read/write speeds, which significantly speeds up the process of loading and saving encrypted files.
- **Operating System:**
    - A system capable of running Windows 10/11, macOS (11.0 or later), or a modern Linux distribution (e.g., Ubuntu 20.04).

.

CHAPTER NO. 5

DESIGN & IMPLEMENTATION

CHAPTER 5

DESIGN & IMPLEMENTATION

5.1 SYSTEM DESIGN

5.1.1 USE-CASE

DIAGRAM Actors –

1. Sender
2. Receiver

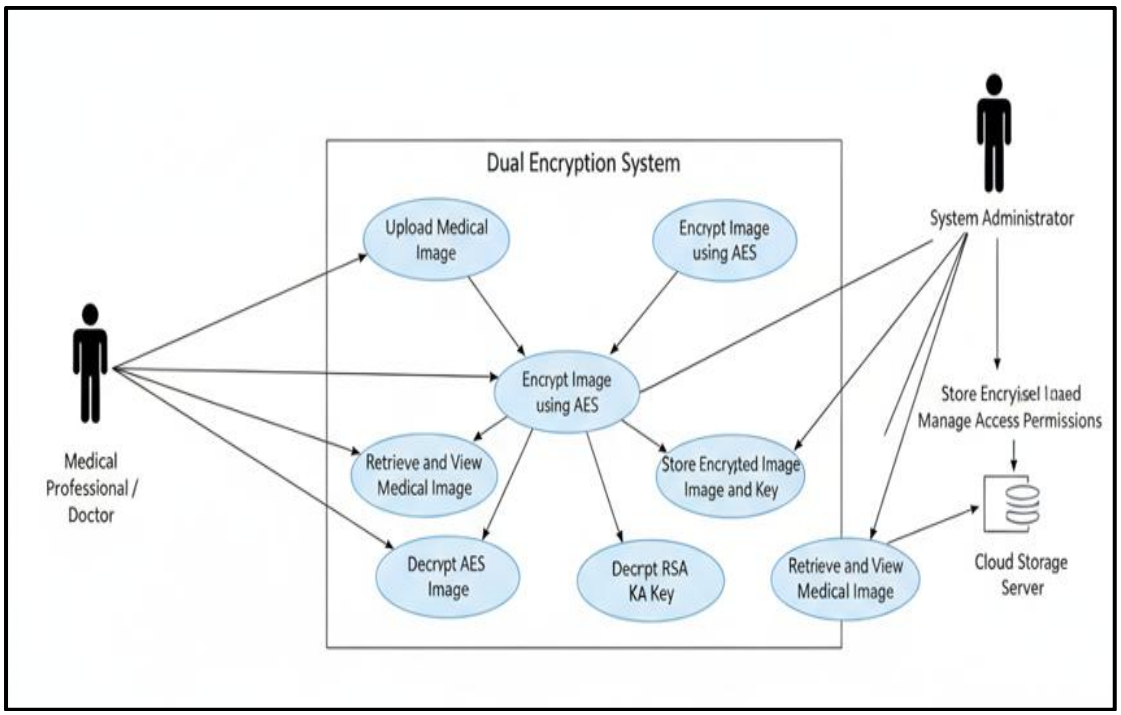


Figure 3. Use-Case Diagram

In Use-Case diagram, the tasks performed by the users are listed below,

1. Sender (Doctor/Medical Professional)– Uploads the medical image and encrypts it using AES before securely sending it to cloud storage. Ensures patient data confidentiality by using strong encryption.
2. Receiver (Authorized Doctor/User)– Retrieves the encrypted medical image from the cloud and decrypts it using the correct key. Can safely view the original medical image only after successful decryption.

5.1.2. DFD DIAGRAM

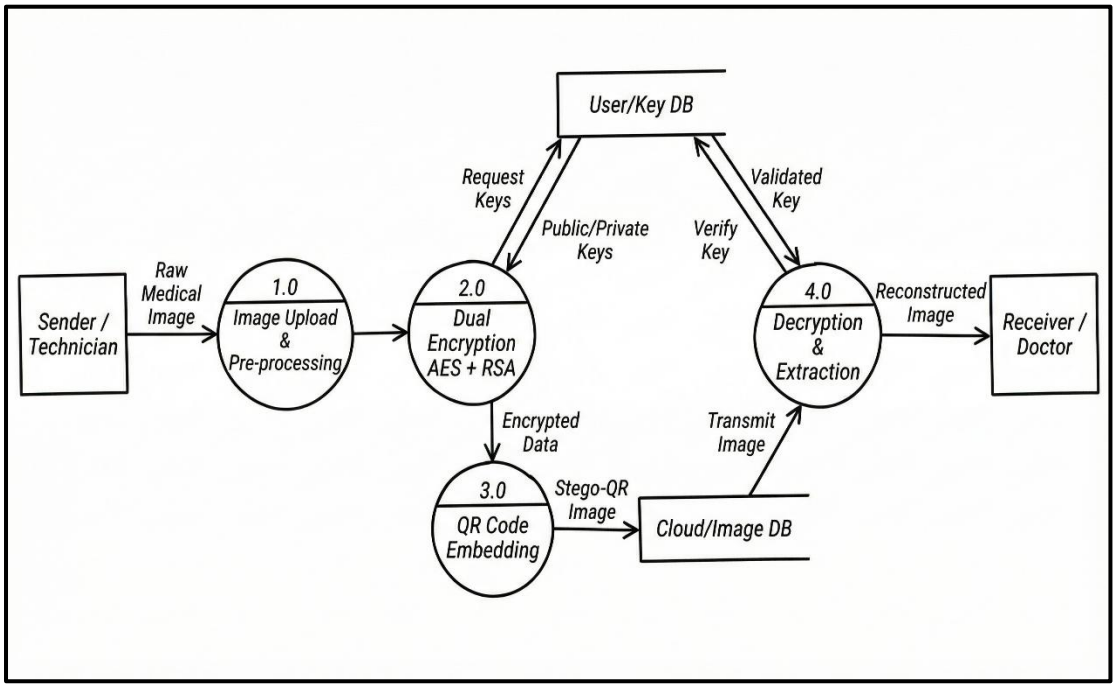


Figure 4. DFD Diagram

This diagram shows a secure medical-image transmission workflow using crypto-stego techniques. First, a raw medical image is uploaded and pre-processed. Then, dual encryption (AES for data, RSA for keys) is applied using keys fetched from a user/key database. The encrypted data is embedded into a Cyphertext to form a stego-QR image, which is stored or sent through a cloud/image database. At the receiver's side, the doctor retrieves the image, verifies the key with the key database, and performs decryption and extraction. Finally, the reconstructed medical image is delivered securely to the intended medical professional.

5.2 Implementation of System

5.2.1 Completed Module

The encryption module is the core component executed on the sender's side. Its purpose is to take a plaintext medical image and the receiver's public key as inputs, and output two secure files: the encrypted image and the encrypted key. This process was implemented in Python using the PyCryptodome library.

AES Image Encryption:

1. **Session Key Generation:** First, a cryptographically secure, random 16-byte (128-bit) symmetric key is generated using Crypto.Random.get_random_bytes(16). This key, K_aes, is used only for this single encryption session.
2. **Image Data Reading:** The target medical image (e.g., image.png) is read into the script in binary-read mode ('rb').
3. **AES Cipher Initialization:** An AES cipher object is created using the AES.new() function. We use AES.MODE_EAX, as this mode provides both confidentiality (encryption) and authenticity (a MAC tag) in one package.
    - cipher_aes = AES.new(K_aes, AES.MODE_EAX)
4. **Encryption and Tagging:** The encrypt_and_digest() method is called on the image data. This returns two items: the encrypted image data (ciphertext) and an authentication tag.
    - ciphertext, tag = cipher_aes.encrypt_and_digest(image_data)
5. **Output:** The nonce (a random value used by EAX mode), the tag, and the ciphertext are saved together into a single binary file (e.g., encrypted_image.bin).

RSA Key Encryption:

1. **Public Key Import:** The receiver's public key is read from its file (public_key.pem) and imported using RSA.import_key().
2. **RSA Cipher Initialization:** An RSA cipher object is created from the imported public key using the PKCS1_OAEP padding scheme for high security.
    - cipher_rsa = PKCS1_OAEP.new(public_key)
3. **Key Encryption:** The cipher_rsa.encrypt() method is called on the 16-byte K_aes. The RSA cipher securely encrypts the AES session key.
4. **Output:** The resulting encrypted key is saved to a separate file (e.g., encrypted_aes_key.bin).

5.3 Sample Code

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import AES, PKCS1_OAEP
import os

encrypted_image_file = "encrypted_image.bin"
encrypted_key_file = "encrypted_aes_key.bin"

private_key_file = "private_key.pem"

decrypted_image_file = "decrypted_medical_image.png"

try:
    with open(private_key_file, "rb") as f:
        private_key = RSA.import_key(f.read())
except FileNotFoundError:
    print(f"Error: Private key file '{private_key_file}' not found.")
    exit()

with open(encrypted_key_file, "rb") as f:
    encrypted_aes_key = f.read()

cipher_rsa = PKCS1_OAEP.new(private_key)
aes_key = cipher_rsa.decrypt(encrypted_aes_key)

print("Step 1: AES session key successfully decrypted using RSA.")

try:
    with open(encrypted_image_file, "rb") as f:
        nonce = f.read(16)
        tag = f.read(16)
        ciphertext = f.read()
except FileNotFoundError:
    print(f"Error: Encrypted image file '{encrypted_image_file}' not found.")
    exit()

cipher_aes = AES.new(aes_key, AES.MODE_EAX, nonce=nonce)

try:
    decrypted_data = cipher_aes.decrypt_and_verify(ciphertext, tag)
    print("Step 2: Image data successfully decrypted using AES.")
    print("Step 3: Data integrity verified. The file was not tampered with.")
except (ValueError, KeyError):
    print("Error: Decryption failed. The data or key is corrupt, or the file was
tampered with.")
    exit()

with open(decrypted_image_file, "wb") as f:
    f.write(decrypted_data)

print(f"Success! Original image saved as '{decrypted_image_file}'.")
```

CHAPTER NO. 6

RESULTS & DISCUSSION

CHAPTER 6

RESULTS & DISCUSSION

6.1 RESULTS AND DISCUSSIONS

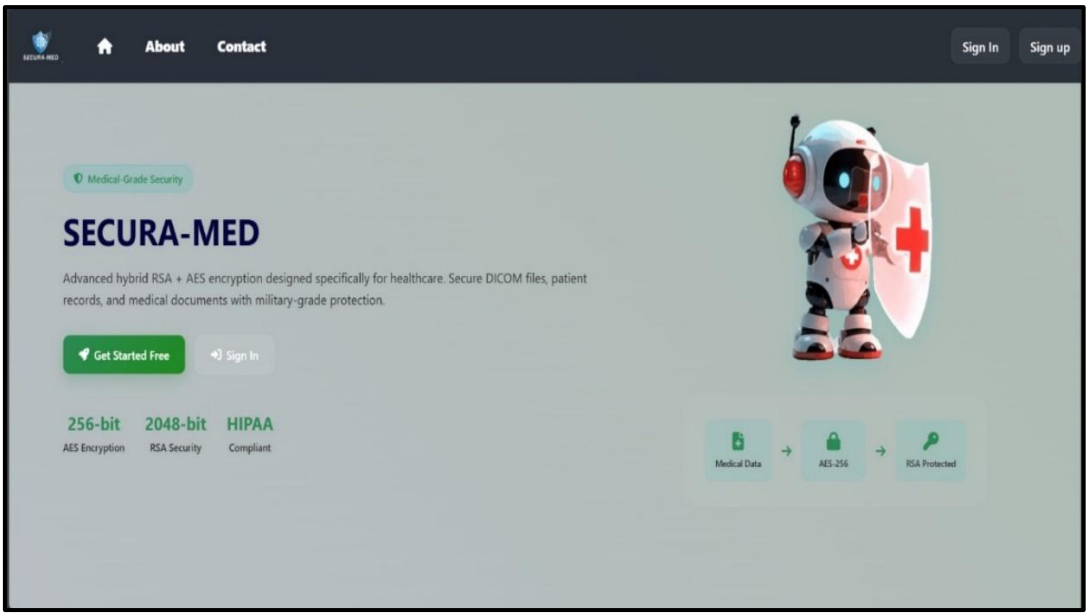


Figure 5. Home Page

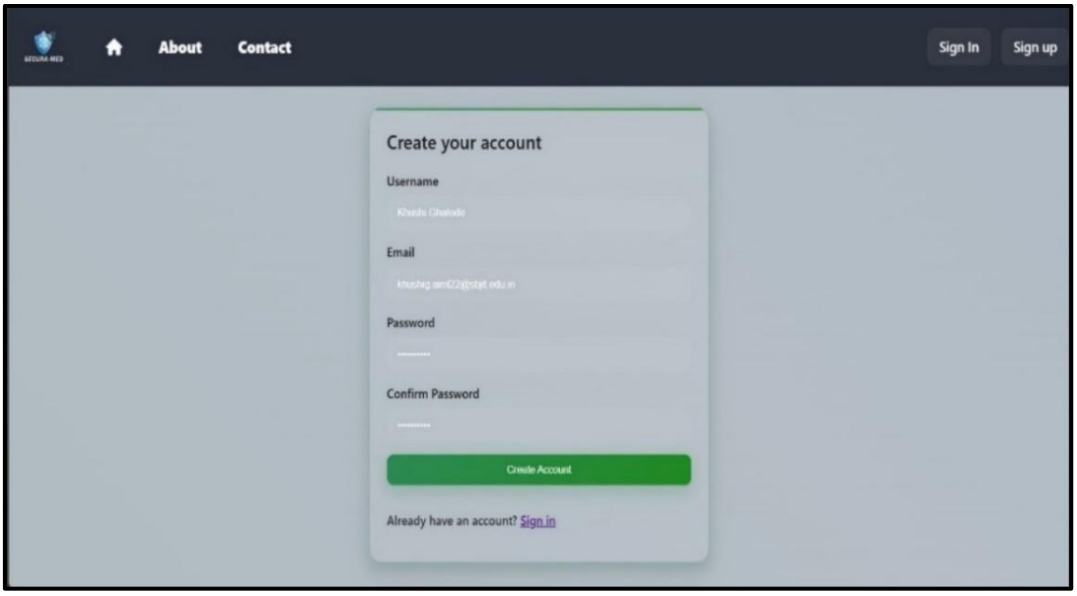


Figure 6. Sign In Page

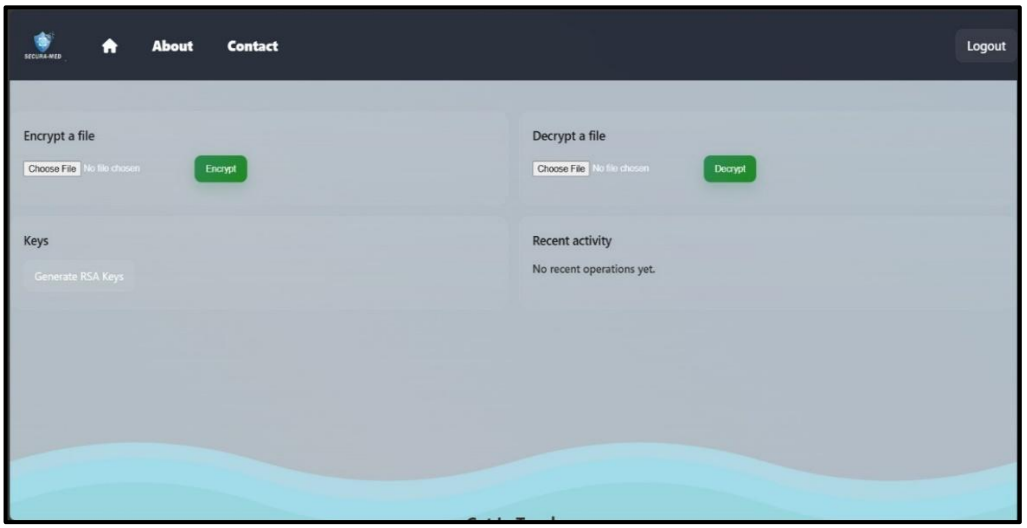


Figure 7. Encryption Page

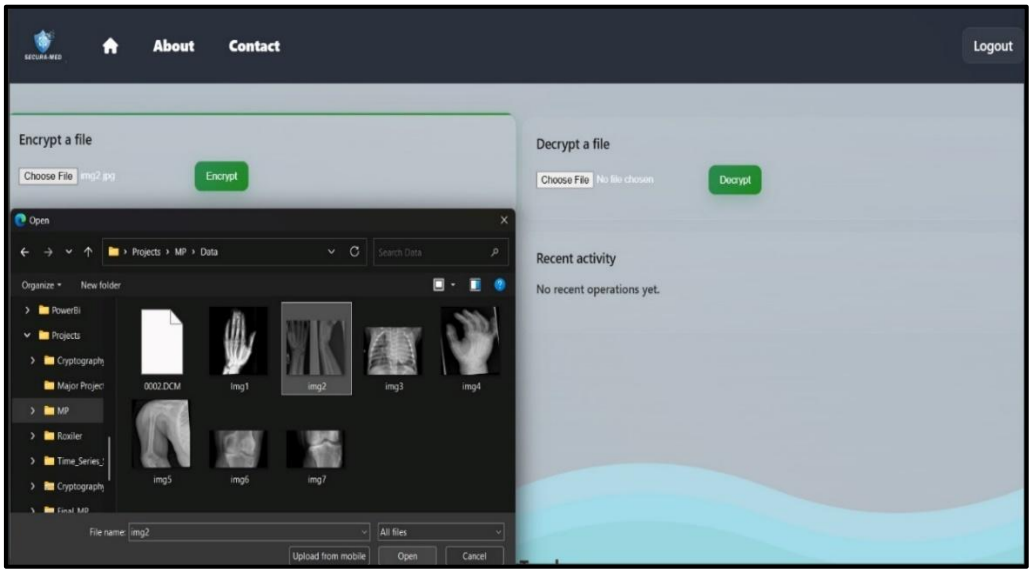


Figure 8. File Selection

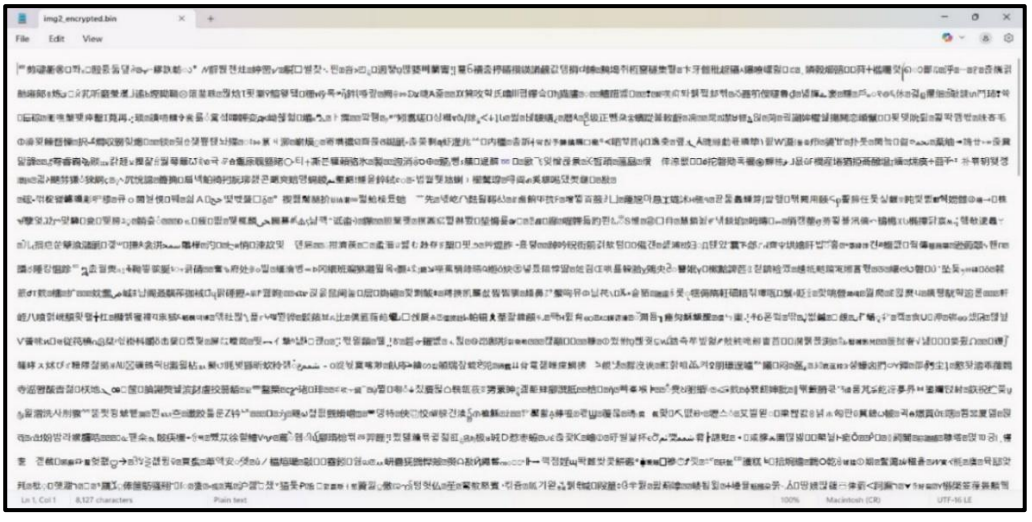


Figure 9. Cipher Text

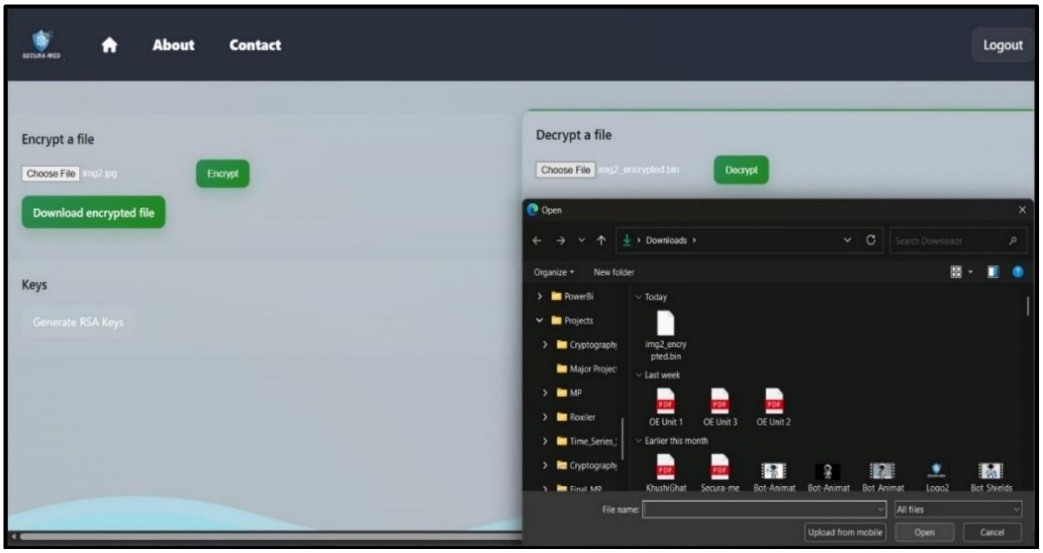


Figure 10. File Decryption

Figure 11. Decrypted File

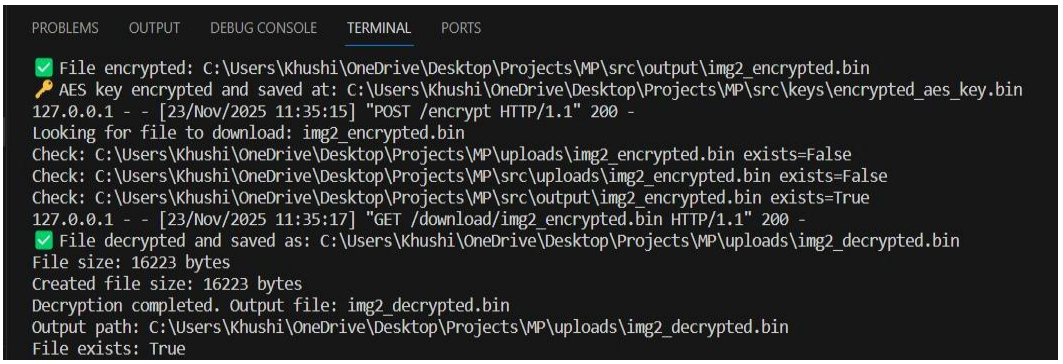


Figure 12. Key Generated

CHAPTER NO. 7

ADVANTAGES AND APPLICATIONS

CHAPTER 7

ADVANTAGES AND APPLICATIONS

7.1 ADVANTAGES

The proposed dual encryption framework offers several significant advantages over traditional, single-layer security methods:

- **Dual-Layer Security:** The system combines the high speed of symmetric (AES) encryption for the large image file with the high security of asymmetric (RSA) encryption for key management. This hybrid model provides the best of both worlds.
- **High Resistance to Attacks:** By using a chaotic map to permute (shuffle) image pixels before encryption, the system destroys the high statistical correlation between pixels.
- **Guaranteed Data Integrity and Quality:** The encryption process is lossless, ensuring that the decrypted medical image is bit-for-bit identical to the original, which is critical for maintaining diagnostic accuracy.
- **Compliance with Healthcare Standards:** This robust security framework directly helps healthcare organizations in meeting the strict technical safeguard requirements for data privacy and security mandated by regulations like HIPAA (Health Insurance Portability and Accountability Act).

7.2 APPLICATIONS

- **Telemedicine and Remote Diagnosis:** Securely transmitting patient images (e.g., X-rays, MRIs, dermatology photos) from a patient's home to a hospital or between specialists in different geographical locations for consultation.
- **Electronic Health Record (EHR) Systems:** Encrypting medical images stored in hospital databases (data-at-rest).
- **Cloud-Based Medical Archives (IoMT):** Securing images before they are uploaded to third-party cloud storage. This is essential for the Internet of Medical Things (IoMT) where data is constantly moved between devices and the cloud.
- **Medical Research:** Protecting the privacy of subjects in clinical trials or research studies by encrypting large datasets of medical images that are shared between institutions..

CHAPTER NO. 8

CONCLUSION & FUTURE SCOPE

CHAPTER 8

CONCLUSION & FUTURE SCOPE

8.1 CONCLUSION

In modern healthcare, ensuring the security and confidentiality of digital medical images is essential, as these images carry highly sensitive diagnostic information and are frequently exchanged across networks and storage platforms. This project successfully developed and validated a dual encryption-based security framework that significantly strengthens protection compared to traditional single-layer approaches. The primary objective was to address the inherent vulnerabilities of medical images, which include large file sizes, high pixel correlation, and susceptibility to statistical and differential attacks. The core strength of the proposed system lies in its integration of AES and RSA encryption**,** creating a layered, highly resilient security mechanism. AES (Advanced Encryption Standard) serves as the symmetric encryption component and is responsible for encrypting the bulk medical image data. Complementing AES, RSA (Rivest Shamir Adleman) is employed as the asymmetric encryption mechanism to protect and manage the AES key itself.

This dual-encryption approach often referred to as hybrid or layered encryption leverages the strengths of both algorithms: AES ensures fast, robust data encryption, while RSA provides secure key exchange and eliminates the risk of key interception. Overall, this dual encryption framework offers a practical, high-strength, and compliance-ready solution capable of meeting modern healthcare security demands.

8.2 FUTURE SCOPE

While the proposed framework provides a comprehensive security solution, there are several avenues for future research and enhancement:

- **Integration with Deep Learning:** Explore the use of deep learning models for generating more complex, unpredictable chaotic maps, which could further enhance the security of the permutation step.
- **Hardware Implementation (IoMT):** The algorithms could be optimized and implemented on specialized hardware, such as FPGAs (Field-Programmable Gate Arrays) or embedded directly into Internet of Medical Things (IoMT) sensors. This would allow for secure, real-time encryption at the point of image capture.
- **Blockchain for Access Control:** Integrate a blockchain-based system to create an immutable, decentralized ledger for managing access logs. This would provide a tamper-proof audit trail, tracking exactly who accessed, decrypted, or shared a medical image and when.
- **Digital Watermarking for Provenance:** In addition to encryption (which provides confidentiality), a robust digital watermarking technique could be embedded. This would not be for security, but for *provenance*, allowing a hospital to trace the origin of an image and verify its authenticity.
- **Elliptic Curve Cryptography (ECC):** Investigate the replacement of RSA with **ECC** for the asymmetric key exchange. ECC provides the same level of security as RSA but with significantly smaller key sizes, making it more efficient and suitable for low-power mobile or wearable medical devices.

REFERENCES:

[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.

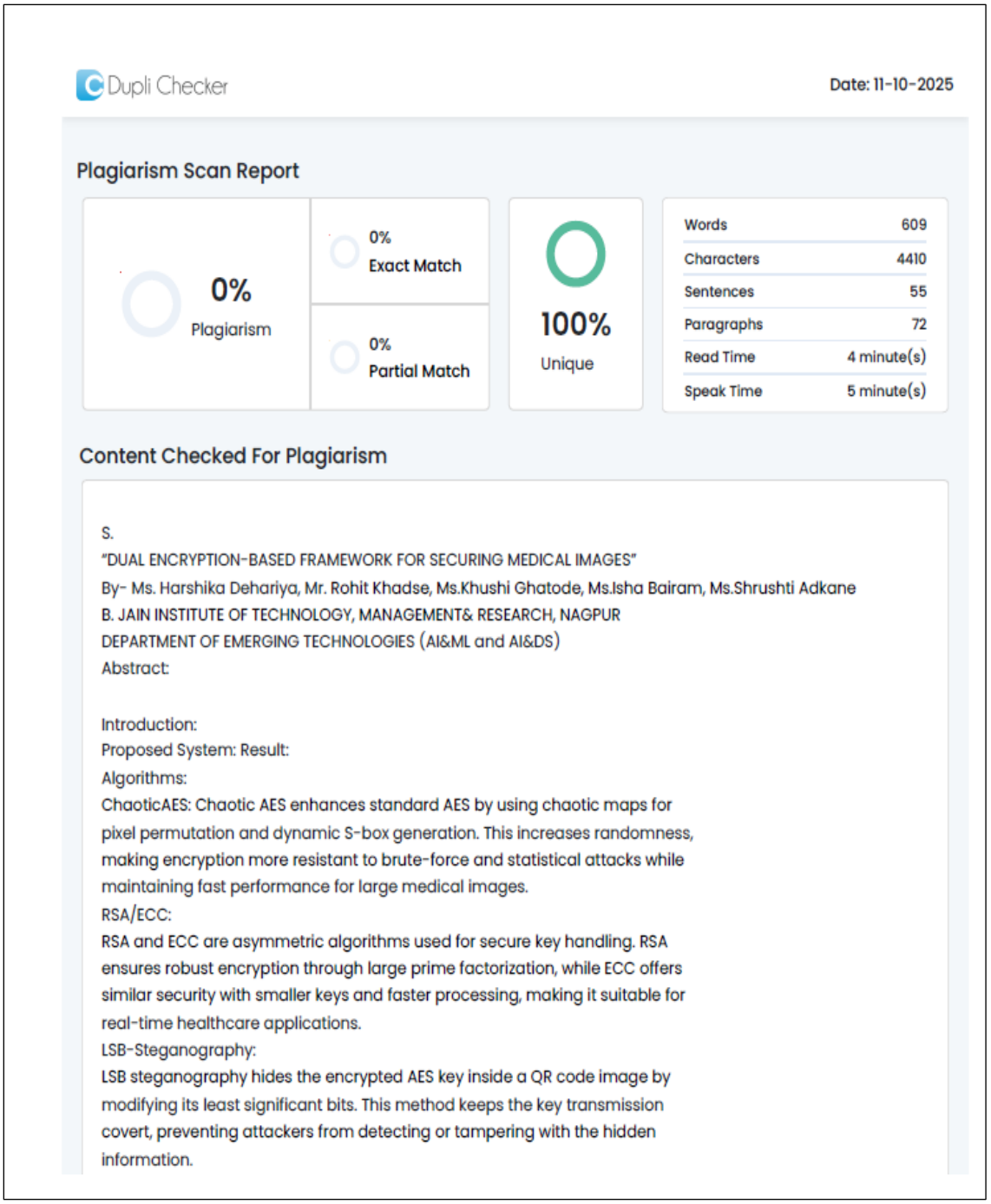
[11] Shukla, A., Tripathi, R. (2020). Secure Key Management and Transmission in Medical Imaging Using ECC and Steganography. *International Journal of Advanced Research in Computer Science, 11(3)*, 89–98.

[12] Al-Haj, A., et al. (2019). Cryptography-Based Security Mechanisms for Healthcare Data: A Review. *Journal of Medical Systems, 43*, 210.

APPENDIX I

PLAGIARISM REPORT

PLAGIARISM REPORT



Dupli Checker

Date: 11-10-2025

Plagiarism Scan Report

0% Plagiarism	0% Exact Match
	0% Partial Match
100% Unique	

Words	609
Characters	4410
Sentences	55
Paragraphs	72
Read Time	4 minute(s)
Speak Time	5 minute(s)

Content Checked For Plagiarism

S.
"DUAL ENCRYPTION-BASED FRAMEWORK FOR SECURING MEDICAL IMAGES"
By- Ms. Harshika Dehariya, Mr. Rohit Khadse, Ms.Khushi Ghatode, Ms.Isha Bairam, Ms.Shrushti Adkane
B. JAIN INSTITUTE OF TECHNOLOGY, MANAGEMENT& RESEARCH, NAGPUR
DEPARTMENT OF EMERGING TECHNOLOGIES (AI&ML and AI&DS)
Abstract:

Introduction:
Proposed System: Result:
Algorithms:
ChaoticAES: Chaotic AES enhances standard AES by using chaotic maps for pixel permutation and dynamic S-box generation. This increases randomness, making encryption more resistant to brute-force and statistical attacks while maintaining fast performance for large medical images.
RSA/ECC:
RSA and ECC are asymmetric algorithms used for secure key handling. RSA ensures robust encryption through large prime factorization, while ECC offers similar security with smaller keys and faster processing, making it suitable for real-time healthcare applications.
LSB-Steganography:
LSB steganography hides the encrypted AES key inside a QR code image by modifying its least significant bits. This method keeps the key transmission covert, preventing attackers from detecting or tampering with the hidden information.

Tool used for plagiarism check: Duplichecker

APPENDIX II
POSTER

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

DEPARTMENT OF EMERGING TECHNOLOGIES (AI&ML and AI&DS)

"DUAL ENCRYPTION-BASED FRAMEWORK FOR SECURING MEDICAL IMAGES"

By- Ms. Harshika Dehariya, Mr. Rohit Khadse, Ms. Khushi Ghatode, Ms. Isha Bairam, Ms. Shrushti Adkane

Abstract:

Medical images such as MRI, CT, and X-ray scans carry confidential patient information that must be securely stored and transmitted. With the increasing use of digital healthcare systems, these images are at risk of data theft and unauthorized access. To address this issue, a dual encryption-based framework is developed that combines the speed of chaotic AES with the key security of RSA/ECC algorithms. The encrypted keys are safely transmitted using cypher text, which hides the key information within an image. This approach provides two layers of protection and ensures secure communication between sender and receiver. The framework is efficient, resistant to common cryptographic attacks, and suitable for real-time healthcare applications such as telemedicine, hospital databases, and cloud-based medical systems while maintaining compliance with data protection standards.

Introduction:

With the growth of digital healthcare systems and telemedicine, medical images such as CT, MRI, and X-ray scans are frequently shared and stored online for diagnosis and treatment. However, this digital transition has also increased the chances of data leakage, cyberattacks, and unauthorized access to sensitive patient information. Traditional single-layer encryption methods like AES or RSA alone cannot fully meet the need for both speed and secure key management.

To overcome these challenges, a dual encryption approach is proposed, combining chaotic AES for fast image encryption and RSA/ECC for secure key handling. The encrypted keys are further protected using cypher texts. This combination provides a balance between efficiency and strong data security, making it suitable for real-time medical systems such as telemedicine, hospital networks, and cloud storage platforms.

Algorithms:

Chaotic AES:

Chaotic AES enhances standard AES by using chaotic maps for pixel permutation and dynamic S-box generation. This increases randomness, making encryption more resistant to brute force and statistical attacks while maintaining fast performance for large medical images.

RSA/ECC:

RSA and ECC are asymmetric algorithms used for secure key handling. RSA ensures robust encryption through large prime factorization, while ECC offers similar security with smaller keys and faster processing, making it suitable for real-time healthcare applications.

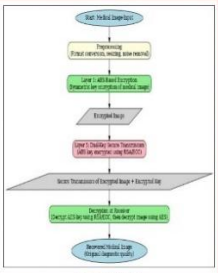


Fig 1. Flow Chart

Conclusion:

The proposed dual encryption framework ensures secure transmission and storage of medical images by combining Chaotic AES and RSA/ECC. This approach provides both speed and strong key protection while maintaining data confidentiality and integrity. The system is efficient, resistant to attacks, and compliant with healthcare standards like HIPAA and GDPR, making it suitable for real-time use in telemedicine and cloud-based medical systems.

Future Scope:

The framework can be enhanced by integrating blockchain for tamper-proof audit trails and using AI-based key generation for adaptive security. Quantum-resistant encryption can prepare it for future threats, while edge-based encryption enables protection on IoMT devices. These improvements will make medical image security more robust, scalable, and suitable for emerging healthcare technologies.

Proposed System:

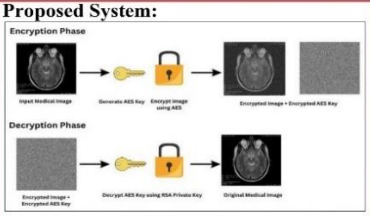


Fig 2. System Architecture

Result:

Fig 3. Home Page

Fig 4. Key Generation

Fig 5. Sample X-Ray

Fig 6. Image Encrypted Cypher Text

Fig 7. Decrypted Image

References:

1. Avudaiappan, S., & Ramachandran, S. (2018). *Dual Encryption Technique for Securing Medical Images*. International Journal of Computer Applications.

2. Ahmad, M., Khan, S., & Sharma, R. (2022). *MID-Crypt: A Hybrid Medical Image Encryption Framework*. Journal of Biomedical Informatics.

3. Kusum Lata, & Cenkeramaddi, S. (2023). *Deep Learning Approaches for Medical Image Cryptography*. Procedia Computer Science.

4. Singh, P., & Attri, R. (2015). *AES Combined with Steganography for Medical Image Security*. International Journal of Engineering Research & Technology.

FORM XIV

APPLICATION FOR REGISTERATION OF COPYRIGHT

[SEE RULE 70]

Diary Number: LD-42045/2025-CO

To

The Registrar of Copyrights,
Copyright Office,
Department of Industrial Policy & Promotion,
Ministry of Commerce and Industry,
Boudhik Sampada Bhawan,
Plot No. 32, Sector 14, Dwarka,
New Delhi-110075
Email Address: copyright@nic.in
Telephone No.: (Office) 011-28032496, 08929474194

Sir,

In Accordance with Section 45 of the Copright Act, 1957 (14 of 1957), I hereby apply for registration of Copyright and request that enteries may be made in the Register of Copyrights as in the enclosed Statement of Particulars.

1. I also send herewith duly completed the Statement of further Particulars relating to the work. (for Literary/Dramatic, Musical, Artistic works only) **Literary/ Dramatic works**

2. In accordance with rule 16 of the Copyright Rules, 1958, I have sent by prepaid registered post copies of this letter and of the Statement of Particulars and Statement of Further Particulars to other parties concerned as shown below:

[See columns 7,11,12, and 13 of the Statement of Particulars and party referred in col.2 (e) of the Statement of Further Particulars.]

3. The prescribed fee has been paid, as per details below: **500/-**

Payment ID	Payment Date	Amount	Bank Name	Payment Mode
429516	16/10/2025	500		

4. Communications on this subject may be addressed to:

HARSHIKA DEHARIYA
S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501
7389977552

5. I hereby declare that to the best of my knowledge and belief, no person, other than to whom a notice has been sent as per paragraph 2 above any claim or interest or dispute to my copyright of this work or its use by me.

6. I hereby verify that the particulars given in this Form and the Statement of Particulars and Statment of Further Particulars are true to the best of my knowledge, belief and information and nothing has been concealed there from.

List of Enclosures:

1. 2 Copies of Work
2. DD/IPO of Rs.500 Per Work
3. Authorization from author/publisher
4. If the application is being filed through attorney , a specific Power of Attorney in original duly signed by the applicant and accepted by the attorney

Place:

Date: **16/10/2025**

For : HARSHIKA DEHARIYA

STATEMENT OF PARTICULARS

Diary Number: LD-42045/2025-CO

1.	Registration Number	
2.	Name, Address and Nationality of the Applicant	NAME: HARSHIKA DEHARIYA, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian NAME: ROHIT KHADSE, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian NAME: KHUSHI GHATODE, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian NAME: ISHA BAIRAM, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian NAME: SHRUSHTI ADKANE, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian
3.	Nature of the Applicant's interest in the Copyright of the work	Author
4.	Class and description of the work	Literary/ Dramatic Work
5.	Title of the work	DUAL ENCRYPTION BASED FRAMEWORK FOR SECURING MEDICAL IMAGES
6.	Language of the work	English
7.	Name, Address and Nationality of the Author and if the Author is deceased, the date of decease.	NAME: HARSHIKA DEHARIYA, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian, NAME: ROHIT KHADSE, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian, NAME: KHUSHI GHATODE, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian, NAME: ISHA BAIRAM, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian, NAME: SHRUSHTI ADKANE, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian,
8.	Whether the work is Published or Unpublished	Unpublished
9.	Year and Country of first publication, and Name, Address and Nationality of the publisher	N/A
10.	Year and Countries of subsequent publications, if any, and Name, Address and Nationality of the publisher	N/A
11.	Name, Address and Nationality of the Owners of the various rights comprising the copyright in the work and extent of rights held by each, together with particulars of assignments and licence. If any	NAME: HARSHIKA DEHARIYA, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian NAME: ROHIT KHADSE, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian NAME: KHUSHI GHATODE, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian NAME: ISHA BAIRAM, ADDRESS: S.B. JAIN INSTITUTE OF TECHNOLOGY MANAGEMENT AND RESEARCH,KATOL ROAD,NAGPUR-441501, Indian NAME: SHRUSHTI ADKANE, ADDRESS: S.B. JAIN

APPENDIX III
PPT HANDOUTS

S. B. JAIN INSTITUTE OF TECHNOLOGY, MANAGEMENT & RESEARCH, NAGPUR.
(An Autonomous Institute, Affiliated to RTMNU, Nagpur)
DEPARTMENT OF EMERGING TECHNOLOGIES (AI&ML and AI&DS)
"Become an excellent center for Emerging Technologies in Computer Science to create competent professionals"

Project Review I

College Name: S. B. Jain Institute of Technology, Management and Research, Nagpur

Department Name: Emerging Technologies

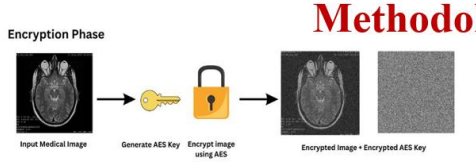
Project Title: A Dual Encryption-Based Framework for Medical Images

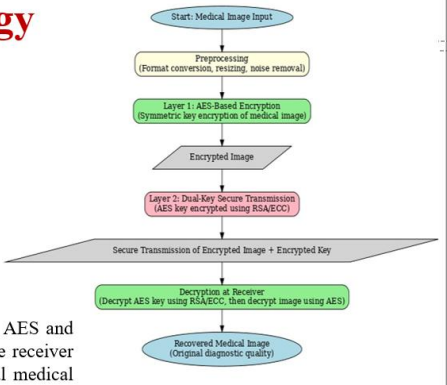
Group Members: **Mr. Rohit Khadse (Team Leader),** Ms. Khushi Ghatode, Ms. Isha Bairam, Ms. Shrushti Adkane

Guide Name: Ms. Harshika Dehariya

S. B. JAIN INSTITUTE OF TECHNOLOGY, MANAGEMENT & RESEARCH, NAGPUR.
(An Autonomous Institute, Affiliated to RTMNU, Nagpur)
DEPARTMENT OF EMERGING TECHNOLOGIES (AI&ML and AI&DS)
"Become an excellent center for Emerging Technologies in Computer Science to create competent professionals"

Methodology





This securely protects medical images by first encrypting them with AES and then encrypting the AES key using RSA for safe transmission. At the receiver end, the AES key is decrypted and used to fully recover the original medical image without loss of diagnostic quality.

S. B. JAIN INSTITUTE OF TECHNOLOGY, MANAGEMENT & RESEARCH, NAGPUR.
(An Autonomous Institute, Affiliated to RTMNU, Nagpur)
DEPARTMENT OF EMERGING TECHNOLOGIES (AI&ML and AI&DS)
"Become an excellent center for Emerging Technologies in Computer Science to create competent professionals"

Future Scope

Background Work

Previous studies mainly used single-layer AES or RSA, which were either fast but weak in key management or secure but slow for large medical images. Hybrid models were attempted, but many lacked pixel-level permutation or proper validation using medical-grade datasets.

Future Work:

The system can be extended by adding lightweight chaotic encryption, QR-code–based secure key packaging, and OTP-verified access for real-time telemedicine environments. Future versions may also integrate blockchain-based audit trails and cloud deployment for secure, large-scale medical image sharing.

APPENDIX IV

USER MANUAL

User Manual
On

"DUAL ENCRYPTION BASED FRAMEWORK FOR SECURING MEDICAL IMAGES"

Submitted By

Mr. Rohit Khadse

Ms. Khushi Ghatode

Ms. Isha Bairam

Ms. Shrushti Adkane

Under the Guidance of

Ms. Harshika Dehariya

Department of Emerging Technologies

S. B. Jain Institute of Technology Management & Research Nagpur

(An Autonomous Institute, Affiliated to RTMNU, Nagpur)

2025-2026

1. Introduction

This document provides instructions for setting up and operating the Dual Encryption Framework for securing medical images. This software uses a hybrid cryptographic approach, combining the speed of AES (for image encryption) with the security of RSA (for key encryption).

This manual is divided into three parts:

- **First-Time Setup:** For the *Receiver* to generate their keys.
- **Encryption:** For the *Sender* to securely encrypt an image.
- **Decryption:** For the *Receiver* to securely open the image.

2. System Requirements

Before use, ensure your system meets the following requirements:

- **Operating System:** Windows, macOS, or Linux.
- **Software:**
    - Python 3.7 or higher.
    - PyCryptodome library. (Install via pip install pycryptodomex or pip install pycryptodome).

3. First-Time Setup (Receiver Only)

This step only needs to be performed once by the person who will be *receiving* the images.

1. **Run Key Generation:**
    - Execute the generate_keys.py script in your terminal:
    - python generate_keys.py
2. **Verify Files:**
    - The script will create two files in the folder:
        - private_key.pem (Your secret key. DO NOT SHARE THIS.)
        - public_key.pem (Your public key.)
3. **Share Public Key:**
    - Securely send the `public_key.pem` file to the person who will be sending you images (the Sender).

4. How to Encrypt an Image (Sender)

Follow these steps to securely encrypt a medical image.

1. **Prepare Files:**
    - Create a folder for the operation.
    - Place the medical image you want to encrypt in this folder (e.g., medical_image.png).
    - Place the public_key.pem file (which you received from the Receiver) in the *same* folder.
2. **Run Encryption Script:**

    1. **Input File**
    - Execute the encrypt.py script:
    - python encrypt.py
2. **Get Output Files:**
    - The script will run and, when finished, you will find two new files in the folder:
        - encrypted_image.bin (The encrypted image file).
        - encrypted_aes_key.bin (The encrypted session key).
3. **Send Files:**
    - Send **both** of these new files (encrypted_image.bin and encrypted_aes_key.bin) to the Receiver.

5. How to Decrypt an Image (Receiver)

Follow these steps to securely decrypt the files you receive.

1. **Prepare Files:**
    - Create a folder for the operation.
    - Place the two files you received from the Sender in this folder:
        - encrypted_image.bin
        - encrypted_aes_key.bin
    - Place your secret private_key.pem file (from the First-Time Setup) in the *same* folder.

2. **Run Decryption Script:**
    - Execute the decrypt.py script:
    - python decrypt.py
3. **View Image:**
    - The script will run and, if successful, will output the original, viewable image:
        - decrypted_medical_image.png
    - You can now open this file normally.

6. Troubleshooting

If you encounter an error, check the following common issues:

- **Error: "Private key file not found."**
    - **Solution:** The Receiver must place their private_key.pem file in the same directory as the decrypt.py script.
- **Error: "Public key file not found."**
    - **Solution:** The Sender must place the public_key.pem (received from the Receiver) in the same directory as the encrypt.py script.
- **Error: "ValueError: Incorrect decryption."**
    - **Solution:** This means the private key does not match the public key used for encryption. Ensure you are using the correct `private_key.pem` file that corresponds to the `public_key.pem` the sender used.
- **Error: "ValueError: MAC check failed."** (or similar "data tampered" message)
    - **Solution:** This is a critical security warning. It means the encrypted image file or the key file is corrupt, incomplete, or was modified after encryption.

Conclusion

This Dual Encryption Framework represents a remarkable innovation in terms of technology for healthcare data security, as it provides an effective, multi-layered solution for monitoring and protecting sensitive medical images. By combining the speed of AES with the security of RSA, the system ensures patient confidentiality and data integrity, helping to prevent unauthorized access and data breaches. For further support or queries, feel free to contact our support team.