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 Seminar – I

"Dual encryption based framework for medical images"

1. ROHIT P..KHADSE (AM22041)
2. ISHA P.BAIRAM(AM22019)
3. KHUSHI H.GHATODE(AM22029)
4. SHRUSHTI I.ADKANE (AM22005)

Guided By: **Asst.Prof.** Ms.HARSHIKA DEHARIYA

Content

1) Introduction
2) Problem Statement
3) Objectives of the Project
4) Literature Review
5) Proposed Work
6) Methodology
7) Expected Outcomes
8) Project Plan & Timeline
9) References

Introduction

The project focuses on addressing growing security challenges in medical imaging due to digital transformation. With rising threats like cyberattacks and data breaches, traditional single-layer encryption proves insufficient. The framework integrates symmetric encryption (AES) for efficient large-scale image protection and asymmetric cryptography (RSA/ECC) for secure key management. Inspired by studies using optimization, deep learning, and hybrid methods, it aims to ensure confidentiality, robust key distribution, and system efficiency. This solution targets storage and transmission security, adaptability to emerging threats, and real-time healthcare needs, strengthening trust and patient data integrity.

Problem Statement

"**A Dual Encryption-Based Framework for Securing Medical Images in Healthcare Systems**"

In healthcare, medical images like X-rays and MRIs often contain private patient information. If this data is not properly protected, it can be stolen, changed, or misused.

Using only encryption keeps the data safe, but it still looks suspicious and can attract hackers. Using only steganography hides the data but may not fully protect it if someone finds it.

So, there is a need for a better method that both hides the data and protects it with encryption.

This project aims to build a dual encryption-based framework that uses both cryptography and steganography to securely hide and protect medical images in healthcare systems.

Objectives of the Project

To ensure confidentiality, integrity, and privacy of patient data embedded within medical images.

To prevent unauthorized access, data leaks, and tampering during storage or transmission.

To maintain image quality and diagnostic usability after data embedding.
The framework supports embedding various patient data (name, ID, diagnosis) into medical images.
Uses symmetric/asymmetric encryption (e.g., AES, RSA) for strong data protection

Literature Review

Sr.No	Title of Paper	Author	Major Observations
1	MID-Crypt: A Cryptographic Algorithm for Advanced Medical Images Protection	Ashraf Ahmad , Yousef AbuHour , Remah Younisse , Yasmeen Alslman , Eman Alnagi and Qasem Abu Al-Haija	combining cryptography and steganography offers stronger security for medical images by protecting both the content and its presence. Techniques like AES, RSA, LSB, and DWT ensure data confidentiality and imperceptibility, while advanced methods like chaos-based encryption, DNA coding, and signcryption improve resistance to attacks. The study also notes a need for lightweight, scalable solutions for real-time healthcare and telemedicine systems.

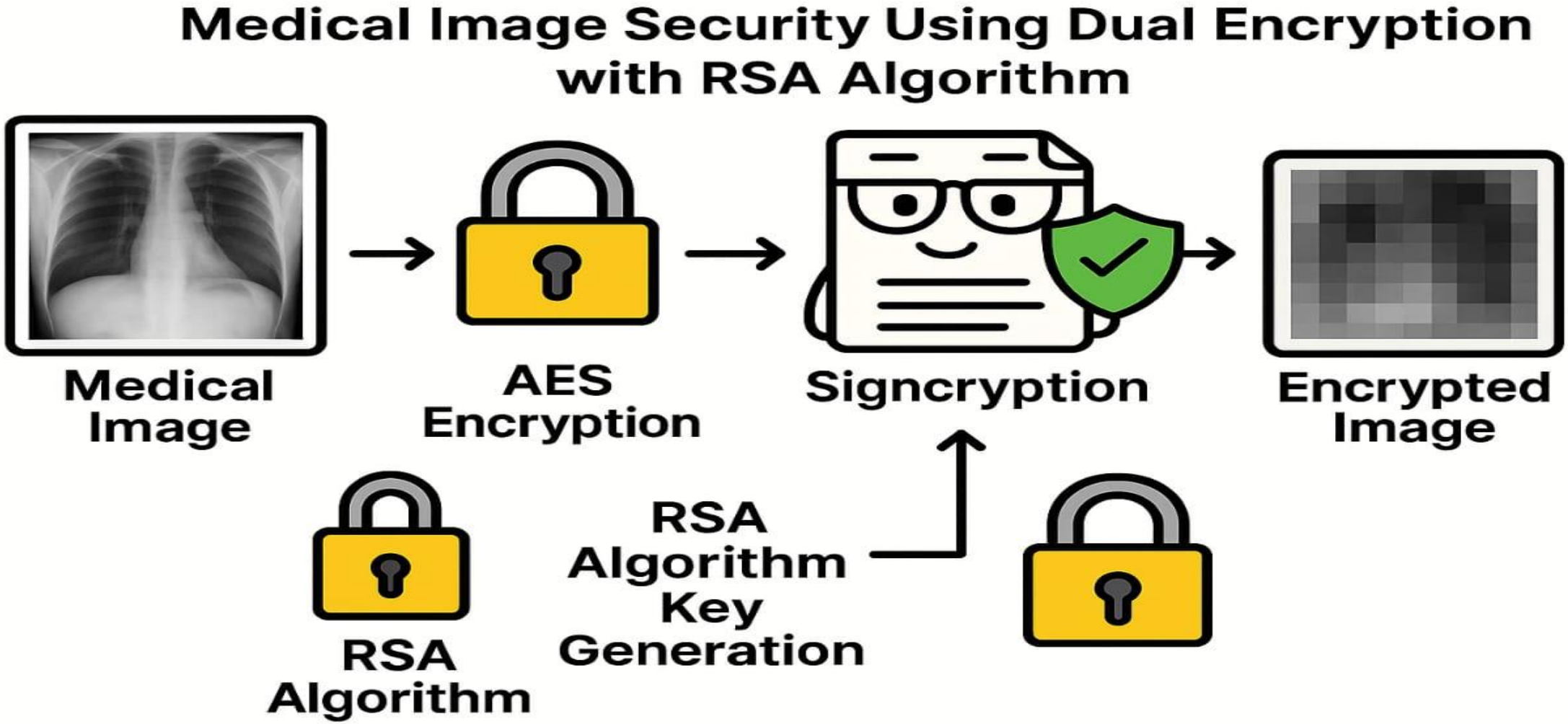
Literature Review

Sr.No	Title of Paper	Author	Major Observations
2	Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm	T. Avudaiappan & R. Balasubramanian & S. Sundara Pandiyan & M. Saravanan & S. K. Lakshmanaprabu& K. Shankar	dual encryption method using Blowfish and Signcryption, enhanced by an optimization algorithm to secure medical images. It ensures high security, image quality, and resistance to attacks while reducing computational cost. The method outperforms traditional techniques and is well-suited for protecting medical data in healthcare systems.

Proposed Work

- **Layer 1 – Chaos-enhanced AES:** Encrypt medical images using AES with pixel permutation, dynamic S-boxes, XOR diffusion, and CBC mode for high security.
- **Layer 2 – Dual-key system:** Use static and dynamic keys; static key slightly modified for extra security.
- **Secure key exchange:** Protect keys with RSA/ECC and encrypt bit-flip position using ElGamal.
- **Steganography:** Embed keys in a QR code using LSB steganography for covert transmission.
- **Technology stack:** Python, Streamlit, Flask, AES, RSA, pydicom; designed for HIPAA/GDPR compliance and real-time healthcare use

Methodology



Expected Outcomes

- **High security:** Strong protection of medical images using chaos-enhanced AES and asymmetric cryptography.
- **Efficient key management:** Secure and covert distribution of keys through dual-key and steganography techniques.
- **Compliance:** Framework aligned with HIPAA/GDPR standards.
- **Performance:** Low computational overhead for real-time healthcare applications like telemedicine.
- **Robustness:** Resistance to brute-force, statistical, differential, and quantum-era attacks with strong entropy and sensitivity metrics.

Project Plan & Timeline

Sr. No	Duration of Week	Work Done by projectees
1	16 June – 15July	Search Project Topic
2	15July – 18 July	Analysis on project
3	18 July – 31 July	Divide task module
4	1 Aug – 18 Aug	Start working on project
5	19 Aug – 15 Sept	1st module will be completed

References

•**T. Avudaiappan and R. Balasubramanian (2018).** *Medical Image Security Using Dual Encryption.* International Journal of Computer Sciences and Engineering, 6(5), 230–238.

•**Ahmad, A., Younisse, R. (2022).** *MID-Crypt: A Cryptographic Algorithm for Advanced Medical Images Protection.*

•**Kusum Lata, Linga Reddy Cenkeramaddi (2023).** *Deep Learning for Medical Image Cryptography: A Comprehensive Review.*