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.

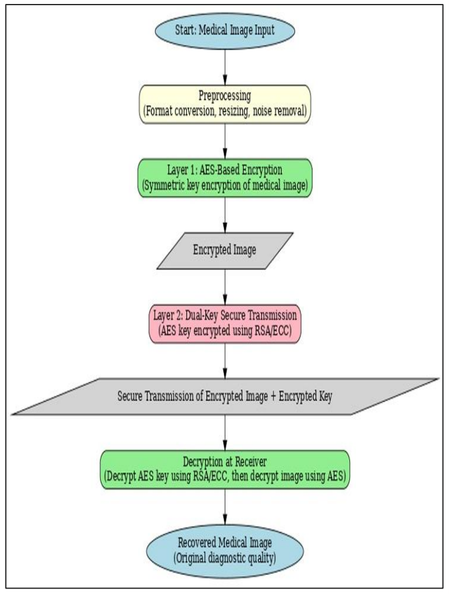


**Fig 1. Flow Chart**

## 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:

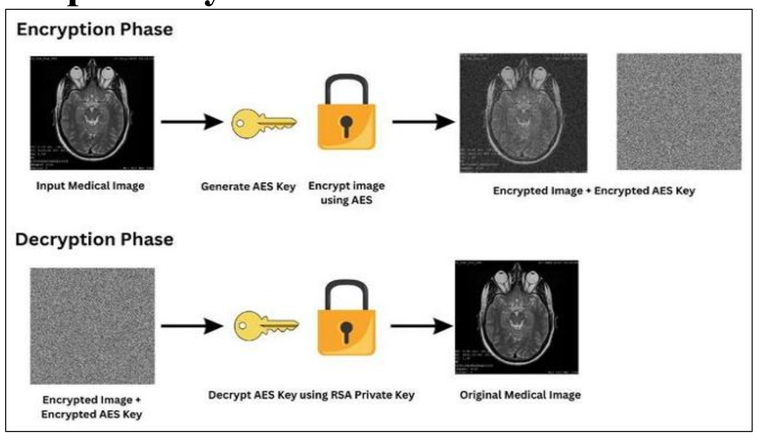


**Fig 2. System Architecture**

## Result:

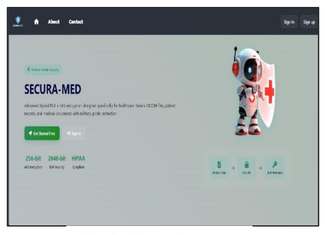


**Fig 3. Home Page**

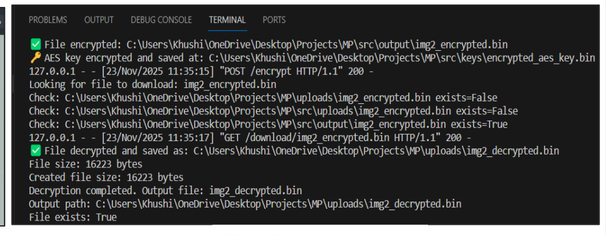


**Fig 4. Key Generation**

**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.