International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

AES Encryption System for Secure Medical Image Processing

Dr.R.Girija[1], Aaditya Raj Kuwar[2], Shivam Kumar Jha[3], Ashish Dhayal[4], Aryan Parashar[5]

[1]Associate Professor, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana
[2,3,4,5,]Manav Rachna International Institute of Research and Studies, Faridabad, Haryana

Abstract
In today's digital era where cyber attacks and security breaches are increasing rapidly, encryption of medical images in essential. The confidentiality, authenticity, and integrity of this data must be maintained. This is the research proposal for the Advanced Encryption Standard (AES)-based Web-based Medical Image Encryption and Decryption System. AES is a commonly used encryption system that works on symmetric key cryptography and is most effective against attacks like Brute Force attacks. Performance can be measured on the basis of usability, security strength and encryption/decryption time. The results clearly state that the AES is much more efficient then the traditional techniques (like DES and RSA) and hence is much more compatible with medical information system.

Keywords: Medical image encryption, Advanced Encryption Standard (AES), RSA cryptography, Chaos-based encryption, Healthcare data security, Patient privacy protection, Symmetric Key Cryptography, Cloud based Medical Image Storage

1. Introduction:
Medical reports are personal and sometime may contain confidential or sensitive patient information. The cloud storage had always been a major concern in terms of privacy while transmission of the data weather they occur in public networks or private networks.

Problem Statement:
- Medical Image contain sensitive information that needs to be secured.
- Unauthorized users may access unencrypted images while they are being transmitted and can manipulate it.
- Traditional encryption methods are not fit for the job.

Motivation:
Protection of patient confidentiality is a legal requirement also as per healthcare regulations like **HIPAA (Health Insurance Portability and Accountability Act, USA)** and **Indian IT Act 2000 (Amended 2008)**.

Proposed Solution:
A **Medical Image Encryption and Decryption System using AES algorithm** integrated into a **website** that:
- Encrypts medical images before storage or transfer.

- Allows authorized users to decrypt them with a valid key.
- Provides a user-friendly interface for doctors and medical staff.

2. Background Study

It doesn't matter if it's a simple X-Ray or an advanced MRI/CT scan they all are a vital part of the patient treatment. As a large number of images are being transferred to the medical institute servers the chances of transfer being intercepted by an unauthorized user are also high.
Medical images are not just some data with numbers and text. They contain sensitive information like address, Phone Number, Policy Numbers, etc. Such information should not be used without authentication and cause big issues like identity theft, insurance scam and many more.
Over the past years many methods for image encryption are being introduced such as DES (Data Encryption Standard) and Triple-DES but as time passed by they become outdated and vulnerable the attacks. Major reason behind vulnerability of this has always being there short key length, while RES encryption has better security it's flow is it's slower processing rate and incompatibility with large image files.
AES is likely the best option available at current time because of it's speed, security and reliability. It has endurance against many currently known cryptographic attacks such as Brute Force attack. It is also compataible with both software and hardware implementation.
Medical encryption has two major factors that should be considered while encryption and decryption: security and preservation of quality of image. Decrypted image are checked using tests like Peak Signal-to-Noise Ratio(PSNR) and Structured Similarity Index(SSIM), which is a crucial step for checking the integrity of the image. Here this is a concern of grave importance because the lifesaving judgements are dependent on the quality of the image. Hence, medical images are needed to be processed without compromising the quality of the image.

3. Literature Review

Several research studies have been conducted on medical image encryption:

- **DES(Data Encryption Standard)** is an early encryption system that uses key of 56 bit and can be easily broken using Brute Force attack
- **Public-key cryptography, based on the RSA algorithm (Rivest-Shamir-Adleman),** is reliable in terms of security but in terms of efficiency it falls behind while dealing with large image files.
- **Chaos-based encryption** is more like a random shuffle of pixels and thus is not widely accepted due to its very complex implementation process.
- **AES (Advanced Encryption Standard) is** adopted by the US government in 2001 as a standard encryption protocol. It uses key of length 128/192/256 bit and provide strong security and reliability.

Comparison Table:

Algorithm	**Key Size**	**Security Strength**	**Speed**	**Suitability for Images**
DES	56-bit	Weak	Fast	Not suitable
RSA	1024–4096 bits	Very Strong	Slow	Not efficient
AES	128–256 bits	Strong	Fast	Highly suitable

Algorithm	**Key Size**	**Security Strength**	**Speed**	**Suitability for Images**
Chaos Based	Depends on Chaotic Map Parameter	High	Moderate to Fast	Not reliable

AES emerges as the best choice for **medical image encryption** due to its balance of speed and strength.

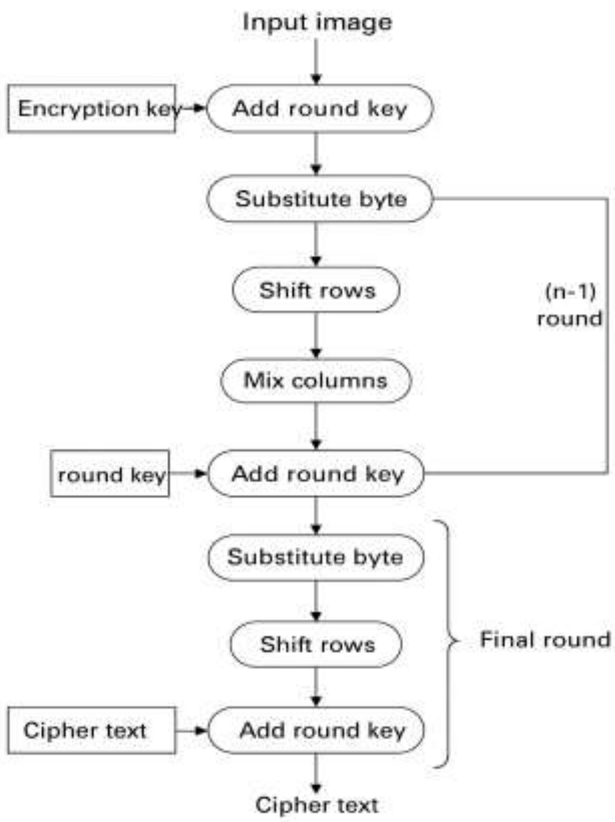
4. Objective

The objectives of this research are:
1. To study the AES encryption for its application and implementation.
2. To design a **web-based system** that enables secure image processing.
3. To analyze the performance of all encryption methods in terms of speed, memory, security .
4. To compare AES with other traditional cryptographic techniques (RSA, DES, Chaos).
5. To propose future enhancements for integration into healthcare IT systems.

5. Methodology

5.1 AES Algorithm Overview

AES is a symmetric encryption algorithm working on 128/192/256-bit blocks and does so across several rounds (10, 12, or 14 depending upon the key size). Each round consist of 4 primary operations:
- Sub Bytes: Substitution of bytes using a nonlinear substitution table.
- Shift Rows: Rows of the block are then cyclically shifted.
- Mix Columns: Each column is then mixed by using some arithmetic transformation.
- Add Round Key: A round key, derived from the secret key, is Xored with the block.



5.2 System Architecture

Steps:

1. **Image Upload:** User uploads the medical image to the portal weather it's a X-Ray or MRI.
2. **Image Conversion:** As for being processed by computer the image is needed to be in binary the image is then converted into a binary image.
3. **AES Encryption:** The data is encrypted using AES encryption algorithm and a secret key.
4. **Secure Transmission/Storage:** The encrypted image is stored or transmitted.
5. **AES Decryption:** Authorized users can enter the key for the image decryption.
6. **Image Restoration: The original image is restored for medical diagnosis.**

5.3 Website Implementation

- Frontend: HTML with CSS and JavaScript is used for the interface.
- Backend: Python-based Flask or Django for AES implementation else use Node.js.
- Database: Uses MongoDB/MySQL to store encrypted images

6. Results and Analysis

6.1 Security Analysis

- AES uses **key lengths up to 256 bits**, making brute-force practically impossible.
- Encrypted images appear as **noise-like making it** visually unrecognizable.

6.2 Performance Evaluation

- **Encryption Time:** AES is faster RSA for large size images.
- **Decryption Accuracy:** Almost 100% recovery of original image when key is correct.

6.3 Experimental Example

- Input: Medical Image of size 1 MB.
- AES-128 encryption time: 0.35 seconds.
- AES-256 encryption time: 0.65 seconds.
- RSA encryption time: ~5.2 seconds.

7. Advantages of Proposed System

- It is faster and more secured than DES/3-DES.
- Compatible with Cloud integration and hospital databases.
- Friendly web interface for doctors and patients.
- Fully ensure the patient confidentiality.

8. Limitations and Future Work

- The whole system work around the key if it is lost the data become unretrievable and data is lost for forever.
- Large image datasets can cause processing delays.
- Future Enhancements:
  - Integration with **cloud computing platforms**.
  - **Blockchain-based audit trails** for tamper-proof logging.
  - Hybrid encryption (AES + RSA) for key exchange.
  - Image watermarking for copyright protection.

9. Conclusion

AES is more convenient and secured to be used in medical image encryption and decryption and it's compatibility make it easier to implement on the web platform for a wider range of use. It is superior to all other methods in terms of speed, reliability, and security.

It can be deployed on the hospital or medical institutes information system assuring that the patient confidentiality is fully secured.

10. References

1. Arab, Alireza, Mohammad Javad Rostami, and Behnam Ghavami. "An image encryption method based on chaos system and AES algorithm." *Journal of Supercomputing* 75.10 (2019).
2. Zeghid, Medien, et al. "A modified AES based algorithm for image encryption." International Journal of Computer Science and Engineering 1.1 (2007): 70-75.
3. Zhang, Qi, and Qun Ding. "Digital image encryption based on advanced encryption standard (AES)." *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*. IEEE, 2015.
4. Singh, Amandeep, Praveen Agarwal, and Mehar Chand. "Image encryption and analysis using dynamic AES." *2019 5th international conference on optimization and applications (ICOA)*. IEEE, 2019.
5. Wadi, Salim Muhsin, and Nasharuddin Zainal. "High definition image encryption algorithm based on AES modification." *Wireless personal communications* 79.2 (2014): 811-829.
6. Hafsa, Amal, et al. "Image encryption method based on improved ECC and modified AES algorithm." *Multimedia Tools and Applications* 80.13 (2021): 19769-19801.