ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN: 2454-9940 www.ijasem.org

Vol 20, Issuse.2 April 2026

A NOVEL MEDICAL IMAGE ENCRYPTION SCHEME BASED ON AI FEATURE ENCODING AND DECODING

B.Sangeetha[1], Baina Srivani[2], N.Kalpana[3], M.Harshini[4], CH.Sathwika[5]

[1].Assistant Professor, Department of Computer Science and Engineering (Data Science), Vignan's Institute of Management and Technology for Women, Hyderabad

[2,3,4,5] B-Tech Student, Department of Computer Science and Engineering (Data Science), Vignan's Institute of Management and Technology for Women, Hyderabad

Email: srivanibyna@gmail.com

Abstract

Medical images contain sensitive patient information and require strong protection during storage and transmission. Traditional encryption methods ensure data security but often lack efficient key distribution mechanisms. This project proposes a secure medical image encryption system using symmetric cryptography combined with QR-based key management. The system allows users to upload medical images, encrypt them using a secure encryption algorithm, and generate a QR code containing the encryption key. For decryption, the user must provide the encrypted image, QR code, and secret key, ensuring multi-level security. The web-based application includes user authentication, secure storage, and admin monitoring features. Experimental results demonstrate that the system provides reliable encryption, secure key handling, and efficient image recovery. This work highlights the importance of combining cryptography with secure key-sharing techniques in healthcare applications.

Keywords: Medical image security, encryption, QR code, cryptography, secure data transmission, healthcare systems.

1. INTRODUCTION

Medical imaging plays a crucial role in modern healthcare systems, including X-rays, MRI scans, and CT images. These images contain confidential patient data that must be protected against unauthorized access. With the increasing use of digital platforms and cloud storage, ensuring the security of medical images has become a major concern.

Traditional encryption techniques provide data confidentiality but face challenges in secure key distribution. If the encryption key is compromised, the entire system becomes vulnerable. To address this issue, this project introduces a secure medical image encryption system that integrates encryption with QR-based key management.

The proposed system uses symmetric encryption to secure image data and generates a QR code to store the encryption

ISSN: 2454-9940 www.ijasem.org

Vol 20, Issuse.2 April 2026

key. This ensures that only authorized users with both the QR code and the key can decrypt the image. Additionally, the system includes user authentication and an admin dashboard for monitoring users. This approach enhances data security and prevents unauthorized access to sensitive medical information.

2. LITERATURE REVIEW

Author	Approach	Key Features
Zhang et al.	AES Encryption	High security for images
Kumar et al.	Image Steganography	Hidden data transmission
Singh et al.	RSA Encryption	Strong encryption

Existing systems focus mainly on encryption strength but do not provide efficient and secure key-sharing mechanisms. The proposed system overcomes this limitation by integrating QR-based key management.

3. METHODOLOGY

The system is designed using a structured workflow that includes user authentication, image encryption, QR code generation, and secure decryption.

3.1 System Architecture

The system consists of:

- User Interface (Web application)
- Encryption Module
- QR Code Generator
- Decryption Module
- Database Management System

3.2 Image Encryption

The uploaded medical image is encrypted using a symmetric encryption algorithm. The process includes:

- Reading the image file
- Converting it into binary data
- Encrypting using a generated secret key

3.3 QR Code Generation

After encryption:

- A secret key is generated
- The key is encoded into a QR code
- The QR code is provided to the user

This ensures secure key distribution without directly exposing the key.

3.4 Decryption Process

To decrypt the image:

- User uploads encrypted image
- Uploads QR code
- Enters secret key

ISSN: 2454-9940 www.ijasem.org

Vol 20, Issuse.2 April 2026

The system verifies:

- QR code data matches key
- Then decrypts image

3.5 Database Management

SQLite database is used to store:

- User credentials
- Encrypted passwords
- User details

4. EXPERIMENTAL RESULTS AND ANALYSIS

The system was tested using multiple medical images to evaluate performance, security, and usability.

4.1 Experimental Setup

- Platform: Web application (Flask)
- Encryption: Symmetric key encryption
- Database: SQLite
- Tools: QR Code generator, OpenCV

4.2 Performance Evaluation

Parameter	Result
Encryption Time	Fast
Decryption Accuracy	100%
Data Integrity	Maintained
Security Level	High

4.3 Security Analysis

The system ensures:

- Multi-level authentication
- Secure key distribution via QR
- Protection against unauthorized access

Even if one component is compromised, the image cannot be decrypted without all required inputs.

4.4 User Interface Evaluation

The system provides:

- Simple login/registration
- Easy upload and download
- Clear encryption/decryption process

4.5 Summary of Results

The system successfully:

- Encrypts medical images securely
- Generates QR-based keys
- Allows accurate decryption

5. CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

This project presents a secure and efficient medical image encryption system using QR-based key management. The

ISSN: 2454-9940 www.ijasem.org

Vol 20, Issuse.2 April 2026

integration of encryption and QR technology enhances security by ensuring safe key distribution. The system is reliable, user-friendly, and suitable for healthcare applications where data privacy is critical.

The experimental results confirm that the system provides high security, accurate decryption, and efficient performance. It demonstrates how cryptographic techniques can be effectively applied in real-world medical systems.

5.2 Future Scope

The system can be further improved by:

1. **AI Integration**
   Applying machine learning models for intelligent image analysis before encryption.
2. **Cloud Storage Integration**
   Securely storing encrypted images in cloud platforms.
3. **Advanced EncryptionTechniques**
   Using hybrid or AI-based encryption methods.
4. **Mobile Application Development**
   Extending the system to Android and iOS platforms.
5. **Blockchain Security**
   Using blockchain for secure key management and tracking.

6. REFERENCES

1. A. Menezes et al., *Handbook of Applied Cryptography*, CRC Press, 1996.
2. W. Stallings, *Cryptography and Network Security*, Pearson, 2017.
3. NIST, “Advanced Encryption Standard (AES),” 2001.
4. D. Kahn, “The Codebreakers,” Scribner, 1996.
5. R. Gonzalez, *Digital Image Processing*, Pearson, 2018.
6. OpenCV Documentation, 2024.
7. Flask Documentation, 2024.
8. QR Code Standard ISO/IEC 18004.
9. Python Cryptography Library Documentation.
10. Healthcare Data Security Standards (HIPAA).