Medical Image Encryption System Using QR-Based Key Management

CH.Navaneetha[1], S.Sharanya[2], P.Anjali[3], P.Sharanya[4], P.Deekshasree[5]
Department of Computer Science and Engineering, Vignan's Institute of Management and Technology for Women (VMTW) Hyderabad, India

Abstract - **The increasing adoption of digital healthcare systems has significantly improved the efficiency of medical services, but it has also raised serious concerns regarding the security and privacy of sensitive patient data. Medical images such as X-rays, MRI scans, and CT scans contain critical diagnostic information that must be protected from unauthorized access, tampering, and data breaches. Ensuring secure transmission and storage of such data is therefore essential in modern healthcare environments. This project proposes a Medical Image Encryption System that combines a lightweight encryption technique with an efficient key management mechanism. The system utilizes the XOR (Exclusive OR) encryption algorithm to encrypt image data at the byte level using a randomly generated key. The encrypted image is stored securely, while the key is indirectly managed through a QR code that encodes a unique identifier associated with the encrypted image in a database. During the decryption process, the QR code is scanned and decoded using image processing techniques, allowing the system to retrieve the corresponding encryption key and encrypted file from the database. This eliminates the need for manual key memorization and reduces the risk of key mismanagement. The system is developed as a web-based application using the Flask framework, incorporating user authentication, secure file handling, and database integration for efficient data storage and retrieval. The proposed approach offers several advantages, including simplicity, low computational complexity, fast processing, and improved usability. While XOR encryption alone may not provide high-level security against advanced attacks, its combination with QR-based access control and structured database storage enhances the overall reliability of the system. This makes the solution suitable for small-scale healthcare applications, academic projects, and prototype-level implementations.**

Keywords: **Medical Image Encryption, XOR Algorithm, QR Code, Data Security, Healthcare Systems, Image Processing, Flask Web Application, Database Management, Information Security, Secure Data Transmission**

I. INTRODUCTION

The rapid advancement of digital technologies has transformed the healthcare industry, enabling efficient storage, transmission, and analysis of medical data. Among various forms of healthcare data, medical images such as X-rays, Magnetic Resonance Imaging (MRI), and Computed Tomography (CT) scans play a crucial role in diagnosis and treatment planning. However, the digital handling of such sensitive information has raised significant concerns regarding data security, privacy, and unauthorized access.

Medical images often contain confidential patient information, and any breach can lead to serious ethical, legal, and financial consequences. With the increasing use of cloud storage, telemedicine, and electronic health records, the risk of cyberattacks and data leakage has grown substantially. Therefore, ensuring secure transmission and storage of medical images has become critical requirement in modern healthcare systems.

Encryption techniques are widely used to protect sensitive data by converting it into an unreadable format that can only be accessed by authorized users. Traditional encryption algorithms, such as AES and RSA, provide strong security but may involve higher computational complexity and resource requirements. In contrast, lightweight encryption methods offer faster processing and are suitable for applications where speed and simplicity are essential. In this project, a Medical Image Encryption System is proposed using a simple yet effective XOR-based encryption technique combined with a QR code-based key management mechanism. The system encrypts image data at the byte level using a randomly generated key, ensuring that the original image cannot be interpreted without proper authorization. To address the challenge of key management, a QR code is generated to store a

unique identifier linked to the encrypted image and its corresponding key in a database.

The integration of QR code technology simplifies the process of secure key sharing and retrieval, eliminating the need for users to manually remember encryption keys. Additionally, the system is implemented as a web-based application using the Flask framework, providing user authentication, secure file handling, and efficient database management.The primary objective of this work is to develop a secure, user-friendly, and efficient solution for protecting medical images while maintaining low computational complexity. This approach demonstrates how combining basic encryption techniques with modern tools such as QR codes and web technologies can enhance data security in practical applications.

II. LITERATURE SURVEY

Traditional Encryption Techniques

Traditional encryption algorithms such as the Advanced Encryption Standard (AES) are widely used for securing medical images due to their strong security features. These methods ensure high confidentiality and protection against unauthorized access. However, they involve complex computations and require more processing time, which may not be suitable for real-time or lightweight applications.

Asymmetric Encryption Methods

Asymmetric encryption techniques like RSA are used for secure data transmission and key exchange. These methods provide a high level of security by using public and private keys. However, they are computationally intensive and slower when applied to large image files, making them less efficient for handling high-resolution medical images.

Hybrid Encryption Approaches

To overcome the limitations of individual encryption techniques, hybrid methods combining AES and RSA have been proposed. These approaches aim to provide both high security and better performance. While effective, they increase the complexity of the system and require more resources for implementation and maintenance.

Image Steganography Techniques

Steganography involves hiding sensitive information within images to enhance confidentiality. In medical applications, patient data can be embedded within image files. Although this method improves data hiding, it has limitations such as low data capacity and vulnerability to certain detection techniques.

Chaos-Based Encryption Methods

Chaos-based encryption techniques use mathematical chaotic systems to encrypt image data. These methods offer high randomness and strong security features. However, they are difficult to implement and may not be suitable for simple or resource-constrained systems.

QR Code-Based Security Systems

Recent research has explored the use of QR codes for secure data sharing and key management. QR codes provide a user-friendly way to transfer encrypted information or keys. However, they have limitations in terms of storage capacity and may require additional security measures to prevent misuse.

Research Gap Identified

From the above studies, it is observed that most existing systems focus either on strong encryption or ease of use. There is a lack of systems that provide a balance between security, simplicity, and usability, especially for small-scale applications.

Proposed System Approach

To address these limitations, the proposed system utilizes a lightweight XOR-based encryption technique combined with QR code-based key management and database integration. This approach ensures faster processing, ease of use, and structured data handling while maintaining a reasonable level of security for medical image protection.

III. METHODOLOGY

System Overview

The proposed system is a web-based application designed to securely encrypt and decrypt medical images. It integrates image processing, encryption techniques, QR code generation, and database management to ensure secure storage and controlled access to sensitive medical data.

User Authentication

The system begins with a user authentication module where users must register and log in using valid credentials. This ensures that only authorized users can access the encryption and decryption

functionalities, thereby adding an additional layer of security.

Image Upload and Preprocessing
After successful login, the user uploads a medical image such as an X-ray, MRI, or CT scan. The uploaded image is stored temporarily on the server, and its binary data is prepared for encryption. The system ensures that only valid image formats are accepted.

Key Generation
A random encryption key is generated using system-level randomness. The key is typically a value between 1 and 255, which is used in the XOR encryption process. This key is unique for each image, ensuring variability in encryption.

XOR-Based Image Encryption
The core encryption process uses the XOR (Exclusive OR) operation. Each byte of the image data is combined with the generated key using the XOR operation. This transforms the original image into an encrypted format that appears as random data and cannot be interpreted without the correct key.

Database Storage
After encryption, the encrypted image is stored in the system's storage, and the corresponding key along with a unique image identifier is saved in the database. This structured storage ensures efficient retrieval during the decryption process.

QR Code Generation
A QR code is generated that encodes the unique image identifier. This QR code acts as a secure reference to retrieve the encryption key and encrypted image from the database. It eliminates the need for users to manually remember the key.

QR Code Scanning and Data Retrieval
During decryption, the user uploads the QR code. The system decodes the QR code using image processing techniques to extract the image identifier. Using this identifier, the system retrieves the corresponding encrypted image and key from the database.

Image Decryption
The decryption process uses the same XOR operation with the retrieved key. Since XOR is a reversible operation, applying the same key restores the original image from the encrypted data.

Output Generation
After successful decryption, the original medical image is reconstructed and provided to the user as a downloadable file. This ensures that the user regains access to the exact original image without any data loss.

System Implementation
The entire system is implemented using the Flask web framework, with SQLite database integration for data storage. OpenCV is used for QR code decoding, and standard Python libraries are used for file handling and encryption operations.

IV. SYSTEM ARCHITECTURE

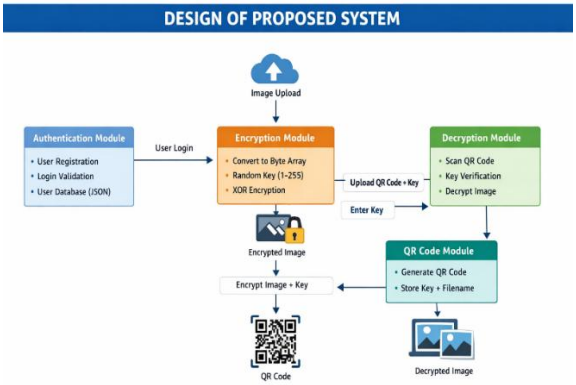


Fig. 1: System Architecture

The proposed system is designed as a modular web-based architecture that ensures secure encryption and decryption of medical images. It consists of four major modules: Authentication Module, Encryption Module, QR Code Module, and Decryption Module. Each module performs a specific function to maintain security, usability, and efficiency throughout the system.

Authentication Module
The authentication module is responsible for managing user access to the system. It includes user registration, login validation, and storage of user credentials in the database. Only authorized users can access the system functionalities, ensuring restricted access to sensitive medical data. This module acts as the first layer of security.

Image Upload Process
After successful authentication, the user uploads a medical image such as an X-ray or MRI scan. The uploaded image is passed to the encryption module,

where it is prepared for further processing. This step ensures that only valid image files enter the system.

Encryption Module

The encryption module performs the core functionality of securing the image. Initially, the uploaded image is converted into a byte array format. A random key within the range of 1 to 255 is generated. Using this key, XOR encryption is applied to each byte of the image, producing an encrypted image that appears as unreadable data. This ensures confidentiality of the medical image.

Encrypted Image Generation

Once encryption is completed, the encrypted image is generated and stored. This encrypted file cannot be accessed or understood without the correct key, thereby protecting sensitive information from unauthorized users.

QR Code Module

The QR code module is responsible for secure key management. Instead of directly sharing the encryption key, the system generates a QR code that stores a unique reference (such as image ID linked with key and filename). This QR code simplifies key sharing and eliminates the need for users to manually remember the key. The key and file details are securely stored in the database.

Decryption Module

The decryption module allows users to recover the original image. The user uploads the QR code, which is scanned and decoded to extract the stored information. The system retrieves the corresponding encrypted image and key from the database.

Key Verification and Decryption

After retrieving the key, the system verifies its correctness and applies the XOR operation again on the encrypted image. Since XOR is reversible, the original image is successfully reconstructed without any data loss.

Final Output Generation

The decrypted image is generated and provided to the user as output. This ensures that only authorized users with the correct QR code can access the original medical image.

V. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental Setup

The proposed system was implemented as a web-based application using the Flask framework. The system was tested on a standard computing environment with typical medical image formats such as JPG and PNG. Various images, including X-rays and MRI scans, were used to evaluate the performance of the encryption and decryption .

Encryption Results

The uploaded medical images were successfully encrypted using the XOR-based encryption technique. The encrypted images appeared completely distorted and unreadable, ensuring that the original content could not be visually interpreted. This demonstrates that the encryption process effectively protects sensitive medical data from unauthorized access.

Decryption Results

The decryption process was performed by uploading the corresponding QR code. The system successfully decoded the QR code, retrieved the correct key and image details from the database, and reconstructed the original image. The decrypted images were identical to the original images, confirming the correctness and reliability of the decryption .

Performance Analysis

The proposed system demonstrated fast processing speed due to the lightweight nature of the XOR operation. Both encryption and decryption processes were completed within a short time, making the system suitable for real-time applications. Compared to complex encryption algorithms, the computational overhead is significantly reduced.

Security Analysis

The system ensures a basic level of security through XOR encryption combined with QR code-based key management and user authentication. The use of a randomly generated key for each image increases variability and reduces predictability. Additionally, storing the key in the database and accessing it via QR code improves key management and reduces human error.

However, it is observed that XOR encryption alone is vulnerable to brute-force attacks due to its limited key size. The security of the system is enhanced by

restricting access through authentication and QR-based retrieval, but it may not be sufficient for high-security applications.

Usability Analysis

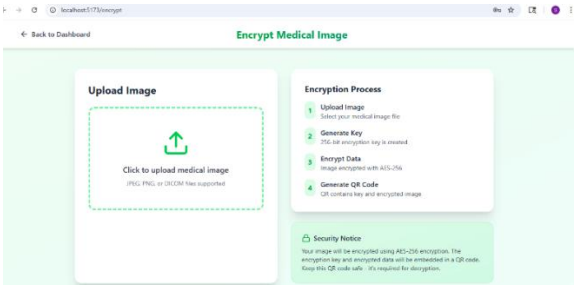
The system provides a user-friendly interface for both encryption and decryption processes. The integration of QR code technology eliminates the need for users to manually remember or share encryption keys. This improves usability and reduces the chances of key loss, making the system more practical for real-world usage.

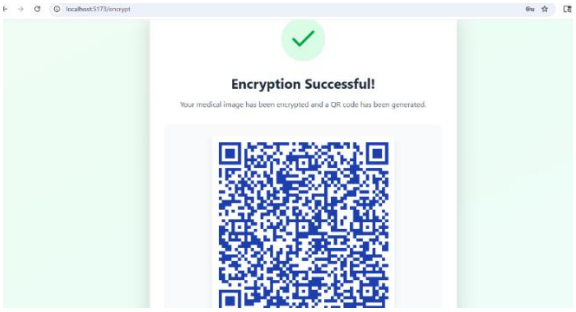
Comparison with Existing Methods

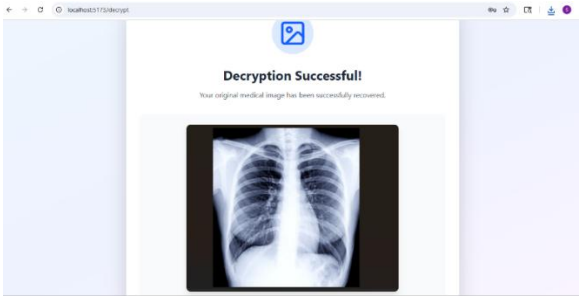
Compared to traditional encryption methods such as AES and RSA, the proposed system offers faster execution and lower computational complexity. While advanced algorithms provide higher security, they require more resources and complex implementation. The proposed approach achieves a balance between simplicity, efficiency, and usability.

Overall Analysis

The experimental results show that the proposed system successfully encrypts and decrypts medical images while maintaining data integrity. The combination of XOR encryption, QR code-based key management, and database storage provides a practical and efficient solution for secure image handling. Although the system is not designed for highly sensitive environments, it performs effectively for academic and small-scale healthcare applications.







VI. DISCUSSIONS

Effectiveness of the Proposed System

The proposed system successfully demonstrates the secure encryption and decryption of medical images using a lightweight XOR-based technique. The experimental results confirm that the encrypted images are completely unreadable, while the decryption process accurately reconstructs the original image without any loss of data. This validates the correctness and functionality of the system.

Role of QR Code in Key Management

One of the key contributions of the system is the use of QR codes for key management. Instead of requiring users to manually remember or share

encryption keys, the system encodes a unique identifier within a QR code. This approach simplifies the key retrieval process and reduces the risk of human error. It also enhances usability, making the system more practical for real-world applications.

Performance Considerations

The XOR encryption technique used in the system is computationally efficient and requires minimal processing time. This makes the system suitable for real-time applications and environments with limited computational resources. Compared to traditional encryption methods, the proposed approach achieves faster execution with lower complexity.

Security Implications

While the system provides a basic level of security, it is important to note that XOR encryption alone is not highly secure against advanced attacks such as brute-force or known-plaintext attacks. However, the integration of user authentication, QR code-based access, and database storage enhances overall system security. These additional layers make unauthorized access more difficult.

Usability and Practicality

The system is designed with a user-friendly web interface that allows easy interaction for both encryption and decryption processes. The use of QR codes improves convenience, as users do not need to manually handle encryption keys. This makes the system accessible even to non-technical users, increasing its practical applicability.

Limitations of the System

Despite its advantages, the system has certain limitations. The use of a small key size in XOR encryption reduces its resistance to brute-force attacks. Additionally, the system relies on the availability of the QR code for decryption, and loss of the QR code may result in inability to retrieve the original image. The system is therefore more suitable for academic and small-scale applications rather than highly secure environments.

Scope for Improvement

The current system can be enhanced by integrating advanced encryption algorithms such as AES for stronger security. Additional features such as secure key storage, multi-factor authentication, and cloud integration can further improve the robustness and scalability of the system. Incorporating artificial intelligence techniques for anomaly detection could also strengthen system security.

VII. CONCLUSIONS

The proposed Medical Image Encryption System presents a simple and efficient approach for securing sensitive healthcare data. By utilizing the XOR-based encryption technique, the system successfully converts medical images into an unreadable format, ensuring confidentiality during storage and transmission. The integration of QR code-based key management provides a user-friendly solution for handling encryption keys, eliminating the need for manual memorization and reducing the risk of key loss.The system also incorporates user authentication and database storage, which enhances overall security and ensures controlled access to encrypted data. Experimental results demonstrate that the system is capable of accurately encrypting and decrypting images without any loss of information, while maintaining low computational complexity and fast processing speed.Although the use of XOR encryption offers simplicity and efficiency, it provides only a moderate level of security compared to advanced encryption algorithms. However, the combination of encryption, QR-based access, and structured data management makes the system reliable for academic purposes and small-scale applications.

In conclusion, the proposed system achieves a balance between security, performance, and usability, demonstrating a practical solution for medical image protection. It highlights how basic encryption techniques can be effectively enhanced with modern technologies to address real-world challenges in data security.

VIII. FUTURE SCOPE

Integration of Advanced Encryption Algorithms

The current system uses XOR encryption, which is simple and efficient but offers limited security. In the future, the system can be enhanced by integrating advanced encryption techniques such as AES or hybrid encryption methods to provide stronger protection against cyberattacks.

Multi-Layer Security Implementation

Additional security layers such as multi-factor authentication, biometric verification, or OTP-based

login can be incorporated to further restrict unauthorized access and improve overall system security.

Cloud-Based Storage Integration
The system can be extended to support cloud storage, enabling secure storage and remote access to encrypted medical images. This would make the system more scalable and suitable for real-time healthcare environments.

Secure QR Code Enhancement
The QR code mechanism can be improved by encrypting the data stored within the QR code itself or by adding time-based validity. This would prevent misuse in case the QR code is lost or accessed by unauthorized users.

AI-Based Security and Monitoring
Artificial Intelligence techniques can be integrated to detect suspicious activities, unauthorized access attempts, or anomalies in the system. This would significantly enhance the security and intelligence of the system.

Support for Multiple File Formats
Future versions of the system can be designed to support a wider range of medical file formats such as DICOM, which is widely used in healthcare systems for storing medical imaging data.

Mobile Application Development
A mobile application version of the system can be developed to allow users to encrypt, decrypt, and scan QR codes directly from smartphones, improving accessibility and usability.

Performance Optimization
The system can be optimized further to handle large datasets and high-resolution images efficiently, making it suitable for large-scale hospital environments.

REFERENCES

[1] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2018.
[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th Edition, Pearson, 2017.
[3] N. Provos and D. Mazieres, “A Future-Adaptable Password Scheme,” *USENIX Annual Technical Conference*, 1999.
[4] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 4th Edition, Pearson, 2018.s