Medical Data Encryption

[1]**Sanjeev Kumar R V M,** PG Student, Dept of CSE, AMCEC

[2]**Dr. Ramesh Shahabadkar (Prof,)** Dept. of CSE AMCEC

Abstract - The growing use of digital health records and medical imaging has improved healthcare delivery but also intensified concerns over data security and patient privacy. Sensitive images such as MRI, CT, and X-rays, if compromised, can result in identity theft and unauthorized access. Traditional encryption methods often struggle to balance security, speed, and preservation of diagnostic quality. This study introduces a Rubik's algorithm–based encryption technique that applies complex pixel permutations inspired by the Rubik's cube. The method achieves strong non-linear transformations, ensuring confidentiality while maintaining diagnostic integrity. Results highlight its effectiveness for secure storage and transmission of medical images, providing a robust solution for healthcare data protection.

***Key Words*:** Medical image encryption, Rubik's algorithm, Digital health records security, MRI, CT, X-ray protection, Pixel permutation, Non-linear transformation, Data confidentiality, Healthcare cybersecurity, Image integrity preservation, Secure data transmission.

1. INTRODUCTION

The digitization of health records and medical imaging has revolutionized healthcare by improving diagnosis, treatment, and research. However, it has also raised serious concerns regarding data security and patient privacy. Medical images such as MRI, CT scans, and X-rays contain highly sensitive information that, if compromised, may result in identity theft, unauthorized access, and severe privacy violations.

Traditional encryption techniques, while effective for general data, are not fully suited for medical imaging. They often face challenges in maintaining diagnostic quality, ensuring real-time accessibility, and preserving data integrity. To address these issues, this study introduces a Rubik's algorithm-based encryption technique, inspired by the permutations of the Rubik's cube. By applying complex non-linear pixel rearrangements, the method provides strong security while safeguarding diagnostic accuracy and accessibility for authorized users.

1.1 Motivation

The growing threat of cyberattacks in healthcare makes securing medical images essential. Advanced encryption ensures patient privacy, prevents unauthorized access, and maintains clinical reliability in an increasingly digital environment.

1.1 Problem Statement

Conventional algorithms such as AES and RSA are not optimized for medical imaging. They may introduce delays, compromise image clarity, and fail to support real-time healthcare applications. A specialized encryption approach is therefore required.

1.2 Existing System and Drawbacks

Current systems use AES, RSA, and similar linear encryption techniques. Their limitations include:

- Possible degradation of diagnostic image quality
- High computational overhead and slow access
- Vulnerability to pattern recognition in linear structures

1.3 Proposed System

The Rubik's algorithm-based encryption applies non-linear pixel permutations to overcome these drawbacks, offering:

- Strong resistance against cryptographic attacks
- Preservation of diagnostic image integrity
- Fast access for authorized users

1.4 Objectives

- Enhance Security: Design encryption tailored to medical images
- Preserve Diagnostic Quality: Maintain image clarity for accurate interpretation
- Enable Rapid Access: Reduce computational delays in real-time use
- Apply Non-Linear Techniques: Use Rubik's cube- inspired transformations to strengthen security

2. LITERATURE SURVEY

1. Chaotic Map-Based Encryption (Smith & Lee, 2022)

Utilizes chaotic maps for pixel diffusion and permutation, producing strong non-linear encryption patterns.

Pros: High security, preserves diagnostic quality.

Cons: Computationally intensive, unsuitable for low-resource devices.

2. Hybrid AES–ECC Encryption (Brown & White, 2023)

Integrates AES for speed and ECC for key management, ensuring layered security in IoT healthcare.

Pros: Strong protection, real-time suitability.

Cons: Complex implementation, larger encrypted files.

1. Genetic Algorithm with DES (Green, 2021)

Applies genetic operators (crossover, mutation) with DES for pixel scrambling.

Pros: Strong randomness, adaptable to diverse image types.

Cons: Time-intensive, requires fine-tuning of parameters.

3. Lightweight IoT Encryption (Parker, 2022)

Uses segmentation and scrambling for secure medical image transmission in low-resource settings.

Pros: Low computation, clarity preserved.

Cons: Lower security, vulnerable to sophisticated attacks.

4. Rubik's Cube-Based Technique (Wilson & Martinez, 2023)

Employs cube-like rotations with randomized keys for pixel permutation.

Pros: High complexity, maintains diagnostic quality.

Cons: Sensitive to key management, complexity grows with resolution

3. SYSTEM REQUIREMENTS

Functional Requirements

Image Encryption: Secure medical images (MRI, CT, X-rays) using Rubik's algorithm with pixel permutation.

Image Decryption: Authorized users decrypt images with keys while preserving diagnostic quality.

Key Management: Generate and securely manage unique keys per image.

User Authentication: Restrict access to authorized personnel only.

Image Integrity: Verify encrypted/decrypted images to prevent corruption or loss.

Data Logging: Record user activities, timestamps, and operations for audit.

Error Handling: Provide alerts for failed operations or unauthorized access.

Format Compatibility: Support medical image formats (DICOM, JPEG, PNG).

Non-Functional Requirements

Security: Ensure confidentiality, integrity, and compliance with HIPAA/GDPR.

Performance: Enable real-time processing with minimal delay.

Reliability & Availability: Ensure continuous system uptime.

Scalability: Handle large medical datasets across small clinics to large hospitals.

Usability: Intuitive interface requiring minimal training.

Maintainability: Support easy updates and upgrades.

Data Quality: Preserve diagnostic clarity of medical images.

Interoperability: Integrate with PACS and EMR systems.

4. METHODOLOGY AND IMPLEMENTATION

4.1 System Design

The system ensures confidentiality of medical images through Rubik's algorithm-based encryption.

Functional Requirements: Strong encryption, fast processing, support for DICOM/JPEG/PNG.

Non-Functional Requirements: Scalability, usability, healthcare compliance (HIPAA, GDPR).

Architecture: Modules for image input, encryption/decryption, key management, authentication, storage, and access control.

4.2 Data Collection & Pre-processing

A dataset of anonymized MRI, CT, and X-ray images was used. Images were resized and converted for uniformity while preserving diagnostic quality.

4.3 Encryption (Rubik's Algorithm)

Pixel Permutation: Sub-blocks rotated randomly like cube movements.

Combinatorial Encryption: Pixel values altered via key-based transformation.

Key Generation: Keys record all permutations, ensuring secure decryption.

4.4 Decryption

Reverses permutations using the original key. Validation confirmed decrypted images retained diagnostic clarity.

3.1 Authentication & Access Control

Secure login with two-factor/biometric authentication. Role-Based Access Control (RBAC) restricts operations to authorized users.

3.2 Key & Metadata Management

Keys, logs, and metadata stored in an encrypted database with audit trails, backup, and recovery mechanisms.

3.3 Testing & Validation

Functional: Verified encryption, decryption, and key management.

Quality: Decrypted images matched originals.

Performance: Encryption speed met clinical requirements.

Security: Penetration tests confirmed resistance to attacks.

3.4 Deployment & Training

Deployed in secure healthcare cloud/network. Staff trained with user manuals and hands-on sessions.

3.5 Maintenance

Continuous monitoring, regular patches, compliance updates, and user feedback integration.

3.6 Evaluation

Metrics: encryption strength, decryption accuracy, processing speed, user satisfaction, and regulatory compliance.

System Components

User Interface: Login, image upload, encryption access.

Authentication Module: Identity verification & RBAC.

Encryption/Decryption: Rubik's algorithm execution.

Key Management: Secure generation & storage.

Database & Storage: Credentials, logs, encrypted images.

Applications

Secure hospital and radiology imaging.

Telemedicine & remote diagnosis.

Confidential medical research data sharing.

Cloud storage for large-scale imaging.

Pharmaceutical clinical trial security.

Advantages

High security with Rubik's algorithm.

Preserved diagnostic quality.

Secure key management + RBAC.

Scalable & cross-platform adaptable.

Compliance with healthcare laws.

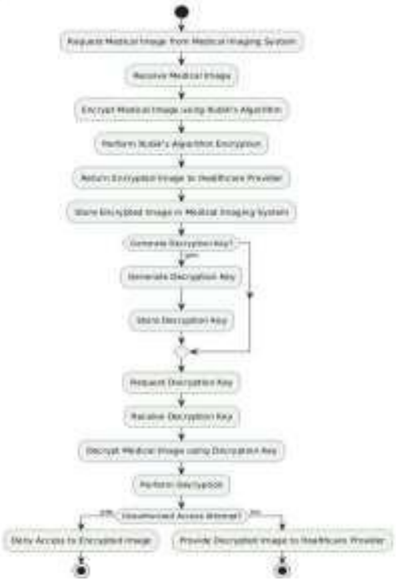
Request Medical Image from Medical Imaging System
Receive Medical Image
Encrypt Medical Image using Rubik's Algorithm
Perform Rubik's Algorithm Encryption
Return Encrypted Image to Healthcare Provider
Store Encrypted Image in Medical Imaging System
Generate Decryption Key?
yes
Generate Decryption Key
Store Decryption Key
Request Decryption Key
Receive Decryption Key
Decrypt Medical Image using Decryption Key
Perform Decryption
Unauthorized Access Attempt?
yes
no
Deny Access to Encrypted Image
Provide Decrypted Image to Healthcare Provider

Fig 1. Methodology

CONCLUSION

The proposed Rubik's algorithm-based encryption system ensures secure, efficient medical image protection without compromising quality. Testing validated robustness, speed, and compliance, making it suitable for real-world healthcare applications.

FUTURE SCOPE

Real-time enhanced Rubik's variants.

AI-assisted encrypted image analysis.

Blockchain for immutable access control.

Cloud and multi-platform expansion.

Decentralized key management.