# Medical Image Security and Anomaly Detection

KUMARAGURU SCHOOL OF INNOVATION
"Innovating Education and Educating for Innovation"

S.R. Vidhyambika (23MDS011), Final year MTech-Data Science student, Department of IT

## ABSTRACT


- With the increasing reliance on digital healthcare, safeguarding medical images is crucial for patient privacy, trust and preventing data tampering.
- This paper proposes hybrid encryption,hashing algorithms including RSA+AES+SHA-256, ECC+AES+SHA-256, AES+SHA-256, DNA Cryptography+AES, Blowfish+SHA-256, Chaotic Maps+AES & DES+AES+MD5.
- Evaluated using metrics such as MSE, PSNR, SSIM, entropy, edge preservation, and encryption time, the results show that these algorithms enhance security while preserving image quality and minimizing encryption time, making them ideal for real-time telemedicine.
- All algorithms achieve SSIM of 1.0, PSNR as infinity, MSE as 0, entropy > 7, and encryption times under 1 ms.


## OBJECTIVE OF THE PROJECT

- **Confidentiality:** Protects patient data from unauthorized access, ensuring privacy.
- **Integrity:** Ensures that medical images remain accurate and untampered in transmission.
- **Authenticity:** Verifies the source and integrity of medical images.
- **Reliability:** Ensures consistent availability and accuracy of images.
- **Anomaly Detection:** Monitors images for unauthorized changes, ensuring security.

## BACKGROUND OF THE STUDY

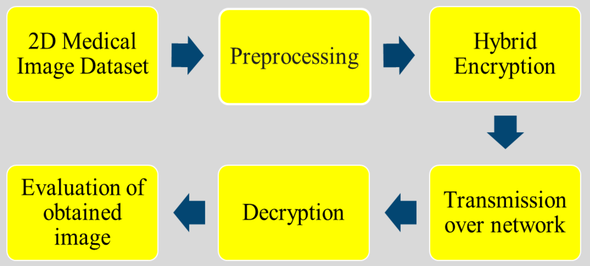
- Medical images like X-rays and MRIs are vital for diagnosis but contain sensitive data, making them prone to breaches and tampering that compromise patient privacy & care.
- Significance: Ensuring medical image security is crucial for diagnostic accuracy and compliance with HIPAA, GDPR. ML and DL enhance anomaly detection for real-time tamper identification.
- Gap identified: Existing solutions focus on either encryption or anomaly detection. This project integrates hybrid encryption with AI-driven anomaly detection for security and reliability.

## EXISTING SYSTEM

Watermarking, steganography, weak encryption (e.g., DES), and other encoding techniques are vulnerable to attacks like cryptanalysis and brute force, causing visible changes, overfitting, low PSNR, and distortion, compromising security and accuracy.

## DESIGN/PROPOSED SYSTEM

1. Medical images are collected from the Cancer Imaging Archive and Kaggle, pre-processed, and stored in DICOM and JPEG formats for encryption.
2. Seven hybrid algorithms namely: ChaoticMaps+AES, RSA+AES+SHA-256, Blowfish+SHA-256, ECC+AES+SHA-256, DES+AES+MD5, AES+SHA-256, and DNA Cryptography+AES are implemented to enhance security, speed, accuracy & resilience against attacks.




3. These are assessed using six metrics: PSNR, SSIM, MSE, entropy, edge preservation, and encryption time.

## SDG/DOMAIN

**SDG Goals:**

- **Goal 3:** Good Health and Well-being
- **Goal 4:** Quality Education
- **Goal 9:** Industry, Innovation, and Infrastructure
- **Goal 12:** Responsible Consumption and Production
- **Goal 16:** Peace, Justice, and Strong Institutions
- **Goal 17:** Partnerships for the Goals

**Domain:** Healthcare

**Cohort:** Cybersecurity

## PROPOSED MODULES

1) **Admin Module:**
   i. User & data management
   ii. Encryption settings
2) **User Module:**
   i. User authentication
   ii. Image upload and view
3) **Dataset Collection And Preprocessing**
4) **Image Encryption/ Decryption Using Algorithms**

## FUTURE WORK

- Future research could focus on encrypting 3D medical images, addressing unique challenges in data handling and security.
- Development of lightweight yet robust hybrid encryption algorithms to optimize the balance between security and performance for modern healthcare applications.

## REFERENCES

[1] Magdy, M., Hosny, K. M., Ghali, N. I., & Ghoniemy, S. (2022). Security of medical images for telemedicine: a systematic review. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-022-11956-7

**GUIDE/MENTOR DETAILS:**

Dr. N. Rajathi,
Professor,
Department of Information Technology,
Kumaraguru College of Technology