MEDICAL IMAGE SECURITY AND ANOMALY DETECTION

A PROJECT REPORT

Submitted by

VIDHYAMBIKA S R

in partial fulfillment for the award of the degree of

MASTER OF TECHNOLOGY

in

DATA SCIENCE

KUMARAGURU COLLEGE OF TECHNOLOGY
(An Autonomous Institution affiliated to Anna University, Chennai)
Post Box No: 2034, Coimbatore - 641049

NOVEMBER 2024

ABSTRACT

With the growing reliance on digital healthcare, safeguarding medical images is crucial to protect patient privacy, ensure trust, and prevent data tampering. This project enhances medical image security using hybrid encryption and hashing algorithms, including RSA+AES+SHA-256, ECC+AES+SHA-256, AES+SHA-256, DNA Cryptography+AES, Blowfish+SHA-256, Chaotic Maps+AES, and DES+AES+MD5. Medical images in formats like DICOM and JPEG are encrypted, ensuring compliance with HIPAA, GDPR, and India's Digital Personal Data Protection Act. These algorithms are evaluated using metrics like PSNR, SSIM, MSE, entropy, edge preservation, and encryption time, achieving SSIM of 1.0, PSNR as infinity, MSE as 0, entropy > 7, and encryption times under 1 ms (per image). Additionally, deep learning-based anomaly detection analyzes large datasets to identify unauthorized alterations and transmission errors, enabling real-time detection of compromised images. This approach ensures robust security, preserves image quality, minimizes encryption time, and protects against attacks like brute-force, cryptanalysis, and data breaches.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

RSA	Rivest–Shamir–Adleman
AES	Advanced Encryption Standard
SHA-256	Secure Hash Algorithm 256-bit
ECC	Elliptic Curve Cryptography
DNA	Deoxyribonucleic Acid
MD5	Message Digest Algorithm 5
DES	Data Encryption Standard
SSIM	Structural Similarity Index Measure
PSNR	Peak Signal-to-Noise Ratio
MSE	Mean Squared Error
DICOM	Digital Imaging and Communications in Medicine
JPEG	Joint Photographic Experts Group
RAM	Random Access Memory
OS	Operating System
SSD	Solid State Drive
2D	Two-Dimensional
3D	Three-Dimensional
CT	Computed Tomography
MRI	Magnetic Resonance Imaging
OCT	Optical Coherence Tomography
PET	Positron Emission Tomography
E2EE	End-to-End Encryption
SVD	Singular Value Decomposition
DWT	Discrete Wavelet Transform

DCT	Discrete Cosine Transform
CPU	Central Processing Unit
GPU	Graphics Processing Unit
HD	High Definition
WIFI	Wireless Fidelity
USB	Universal Serial Bus
HDD	Hard Disk Drive
NumPy	Numerical Python
Matplotlib	Mathematical Plotting Library
GHz	Gigahertz
SciPy	Scientific Python
AMD	Advanced Micro Devices
RX	Radeon X
LTS	Long-Term Support
Hashlib	Hashing Library
Skimage	Scikit-Image
Sklearn	Scikit-Learn
PyCryptodome	Python Cryptography Domain Extension
TPU	Tensor Processing Unit

CHAPTER 1
INTRODUCTION

1.1 BACKGROUND OF THIS PROJECT

In recent years, the field of medical imaging has seen tremendous growth and advancements. Medical images such as X-rays, MRIs, CT scans, and ultrasounds are vital tools in diagnosing and monitoring various diseases and medical conditions. These images contain highly sensitive patient information and are often shared between medical professionals, hospitals, and research institutions. However, the sharing of medical data raises significant concerns about privacy, security, and the risk of unauthorized access, manipulation, or leakage of sensitive information. Medical images not only contain visual data but also identifiable patient information, making them vulnerable to cyberattacks. As a result, protecting patient privacy and ensuring diagnostic accuracy are paramount in healthcare.

The security of medical images is particularly critical because any breach or tampering with these images can lead to misdiagnosis, compromised patient care, and legal consequences. Unauthorized alterations can undermine the integrity of diagnoses, potentially leading to inappropriate treatments and endangering patient health. Ensuring the confidentiality, integrity, and authenticity of medical images is thus of the utmost importance. With the increasing reliance on digital technologies for healthcare services, the need for robust security mechanisms to protect these images has become more critical than ever.

Furthermore, advancements in artificial intelligence (AI), machine learning (ML), and deep learning (DL) have revolutionized anomaly detection in medical imaging. These technologies enhance diagnostic accuracy by analyzing vast datasets to identify subtle patterns, detect unauthorized alterations, and flag transmission errors. AI-driven systems can automatically recognize deviations from expected image characteristics, enabling real-time identification of tampered or compromised images. By integrating AI-powered anomaly detection, healthcare providers can not only strengthen image security but also enable earlier interventions and more effective treatment strategies. This integration ensures the continued integrity, availability, and utility of medical images in modern healthcare systems, ultimately supporting better patient outcomes.

To address these concerns, regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and the General Data Protection Regulation (GDPR) in the European Union, and the Digital Personal Data Protection Act in India set guidelines for data protection, including the encryption and secure management of medical images. To comply with these regulations, healthcare organizations must implement security measures to protect sensitive patient data from cybersecurity risks and illegal access. Consequently, healthcare organizations must prioritize image security to safeguard patient data from unapproved access, data leaks, and cyberattacks. Implementing encryption, secure access controls, and conducting regular audits are critical steps to ensure compliance with these frameworks, maintain diagnostic accuracy and protect sensitive information.

1.2 PROBLEM STATEMENT

“Inadequate encryption and access control for medical images jeopardize patient data security and regulatory compliance, especially as digital imaging grows and cyber threats evolve. Existing security measures often fail to protect against modern, complex threats and lack effective anomaly detection, leaving medical images vulnerable to tampering and unauthorized access. This could compromise diagnostic accuracy, violate healthcare regulations, and undermine patient privacy and trust.”

1.3 PURPOSE

The motto of this project is to design a more comprehensive security framework that integrates advanced hybrid encryption techniques, secure access control, role-based authentication, and real-time anomaly detection to protect medical images and ensure compliance with privacy regulations.

1.4 OBJECTIVES OF THE PROJECT

The objective of this project is to develop a robust framework for ensuring the integrity, confidentiality, authenticity, and reliability of medical imaging data during the encryption and decryption processes. This framework will focus on protecting sensitive patient data while ensuring that medical images remain unaltered, accurate, and available for clinical use. The project aims to achieve secure transmission of medical images by implementing encryption techniques, secure communication protocols, and authentication mechanisms. Additionally, it will introduce role-based access control to ensure that only authorized personnel can access or modify medical image data, thus reducing the risk of unauthorized access and ensuring compliance with regulations. Furthermore, the framework will include advanced anomaly detection systems to identify and address any irregularities or unauthorized modifications in medical images, ensuring continuous protection throughout the image’s lifecycle.

Key Objectives:

- Confidentiality: Protects sensitive patient data from unauthorized access, ensuring privacy and compliance with regulations.
- Integrity: Guarantees that medical images remain unaltered and accurate throughout their lifecycle, from creation to storage and transmission. This involves using cryptographic techniques to detect and prevent tampering or

unauthorized modifications to the data.

- Authenticity: Verifies that medical images are genuine, ensuring that they originate from trusted sources and have not been altered or falsified during transmission or storage. This will be achieved through digital signatures, certificates, and other authentication methods to confirm the source and integrity of the images.
- Reliability: Ensures that the medical image data is consistently available, accurate and accessible when needed by authorized personnel, supporting clinical decisions and patient care. This includes robust data storage solutions, backup protocols, and ensuring that images are retrievable for timely clinical decision-making.
- Anomaly Detection: Implements advanced anomaly detection techniques to continuously monitor medical images for any irregularities or unauthorized changes, ensuring that the images remain accurate and secure throughout their lifecycle.

1.5 SCOPE

To develop a solution for encryption of medical images, authorized access control and detection of irregularities or anomalies in medical scans.

Deliverables:

- End-to-End Encryption (E2EE) using Advanced Encryption Techniques
- Access control
- Accompanied by Deep learning-based real-time anomaly detection for 2D and 3D images (phase II)
- Role-based authentication

Components:

- Medical images:

  2D:

  1. X-ray
  2. Mammography
  3. Optical Coherence Tomography (OCT)
  4. Ultrasound
  5. Fluoroscopy

  3D: (For Phase II)

  1. Computed Tomography (CT) scan
  2. Magnetic Resonance Imaging (MRI)
  3. Positron Emission Tomography (PET)
- Encryption algorithms for security
- Deep learning algorithms for anomaly detection (phase II)

CHAPTER 2
LITERATURE SURVEY

The increasing prevalence of data breaches in the medical field has underscored the urgent need for advanced encryption algorithms to protect sensitive patient information. Medical data breaches often expose confidential details, leading to identity theft, financial fraud, and compromised healthcare outcomes. This growing threat has driven researchers to develop and refine encryption techniques that ensure the confidentiality, integrity, and authenticity of medical data [1].

Ali Alzahrani et al. [2] proposed a robust watermarking framework for securing medical images by leveraging a hybrid domain approach involving Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD). The technique embeds watermarks into the Regions of Non-Interest (RONI) after segmenting the image, ensuring that critical diagnostic regions remain unaffected and minimizing reduction in image quality. By combining frequency and spatial domain transforms, the scheme achieves superior imperceptibility and resilience against various attacks.

Sujarani Rajendran and Manivannan Doraipandian [3] proposed a chaos-based secure medical image transmission model specifically designed for IoT-powered healthcare systems. The cryptosystem ensures both the confidentiality and integrity of medical images through a three-phase security architecture. Initially, the MD5 algorithm generates seed keys for a 3D Lorenz chaotic map, and the Lorenz map is iterated to produce the chaotic key series, which is then applied in the encryption process. This is followed by dual confusion (row- and column-wise scrambling) and dual diffusion (binary reverse and XOR operations) processes. Experimental results confirm high resistance to statistical attacks and robustness against unauthorized modifications, validating its effectiveness in safeguarding medical image transmission and storage.

Ding et al. [4] proposed DeepKeyGen, which leverages a generative adversarial network (GAN) to derive a private key from the original image. The network consists of a generator, which creates the private key, and a discriminator, which distinguishes between the generated key and real data from the transformation domain. The transformation domain defines the "style" of the private key, guiding the network in the key generation process. DeepKeyGen aims to learn mapping from the initial image to the private key. Evaluation on datasets like the Montgomery County chest X-ray, Ultrasonic Brachial Plexus, and BraTS18 shows that the system achieves high security in generating private keys.

Saleh Ali Alshehri [5] introduced a neural network-based image compression technique that primarily focuses on the decompression stage. This method involves dividing the image into several matrices, with neural networks trained to predict the missing pixel values, aiding in the restoration of the original image from compressed data. The system achieved an impressive compression ratio of 81%, with a peak signal-to-noise ratio (PSNR) of 29.5 dB for certain tests. The network was trained using a combination of image samples, initially derived from one image, and later extended to a larger dataset of 30 images.

Alan et al. [6] developed a two-step steganography technique aimed at enhancing image quality and the undetectability of embedded messages. The first step involves a Secret Image Size Reduction (SISR) algorithm that minimizes the size of the secret image without any loss of information. The second step employs a Fibonacci-based embedding mechanism with bit-plane mapping, which significantly improves the quality of the stego image compared to traditional methods.

T. Yuvaraja and R. S. Sabeenian [7] proposed a steganography technique leveraging fuzzy logic to enhance the security of medical images by embedding secret medical images within cover images. The method employed fuzzy rules for edge detection in both cover and secret images, categorizing edges as thin or thick to optimize the embedding process. Utilizing the Discrete Wavelet Transform (DWT) for image transformation, the algorithm achieved multi-resolution analysis, improving robustness. The approach demonstrated superior performance with an average PSNR of 45.87 dB, indicating high-quality stego images and effective concealment. Comparisons with traditional methods highlighted reduced Mean Square Error (MSE) and enhanced entropy, showcasing the technique's capability to secure sensitive patient data and prevent unauthorized access in healthcare applications.

The paper presented by Kester et al. [8] focuses on the integration of medical imaging data within health information systems, emphasizing the critical aspects of data security, privacy, and regulatory compliance. It highlights advancements in medical imaging technologies and their significant applications in healthcare, proposing a comprehensive framework that includes a novel algorithm for secure data transmission and access control in medical imaging systems. The findings suggest that implementing this framework can enhance the effectiveness and reliability of healthcare delivery, ultimately improving patient outcomes through better data management practices.

The algorithm proposed by Yang et al. [9] uses a BP neural network for image compression, followed by Zigzag confusion and chaotic pseudo-random sequences for encryption. The original image is first compressed using the BP neural network, and then the compressed image is encrypted using the Zigzag algorithm and XOR operation. Numerical simulations demonstrate that this approach provides effective image compression and encryption with strong security, making it suitable for information security and secure communication applications.

The method introduced by Ying Niu and Xuncai Zhang [10] utilizes an Isolation Forest, combining multiple binary trees to identify outliers. To improve the discriminative power of the binary trees, the Otsu-based splitting criterion is applied, splitting subsamples into anomalies and backgrounds. This method enhances the ability of the encryption system to resist plaintext and differential attacks by improving the sensitivity of the cipher image to the plaintext and reducing the iteration count of chaotic system-generated index sequences. Additionally, the use of Josephus traversing with pixel value-based step sizes, along with bit XOR and crossover operations, achieves enhanced confusion and diffusion in the image. Experimental results demonstrate that the scheme effectively resists various attacks, such as selective-plaintext and exhaustive attacks, and offers high potential for real-time and secure image encryption.

Priyadharshini et al. [11] proposed a method to secure medical images by integrating one-time pad encryption with LSB steganography. In this approach, medical images are encrypted using a randomly generated key through XOR operation (one-time pad), ensuring robust confidentiality. The encrypted data is then embedded into the least significant bits of a cover image, maintaining its visual quality while concealing sensitive information. Experimental results demonstrated improved performance, achieving lower mean squared error (MSE) and higher peak signal-to-noise ratio (PSNR) compared to traditional LSB techniques, thereby enhancing the security of medical data during transmission.

Shankar et al. [12] proposed a robust encryption algorithm for medical image security, leveraging chaotic functions optimized through an Adaptive Grasshopper Optimization (AGO) algorithm. The study introduced a dual-key mechanism to enhance confusion and diffusion phases, using chaotic maps to generate randomized key streams, addressing challenges in existing one-dimensional chaotic cryptosystems. The AGO algorithm ensured optimal key selection, maximizing Peak Signal-to-Noise Ratio (PSNR) and Correlation Coefficient (CC). Experimental results demonstrated superior encryption quality, resistance to statistical and differential attacks, and computational efficiency. The proposed model safeguards sensitive medical images effectively, requiring only one encryption round while maintaining high-security standards.

Jolfaei et al. [13] conducted a comprehensive analysis of the security vulnerabilities inherent in permutation-only image encryption schemes, revealing significant weaknesses against chosen-plaintext attacks. Their research demonstrated that these ciphers can be entirely compromised with a minimal number of chosen plain-images, specifically a number that scales with the logarithm of the product of the image dimensions and the number of color intensities. The proposed cryptanalysis method exhibits a computational complexity that is proportional to the product of the number of chosen images and the total number of pixels, highlighting that current pseudo-random permutations fail to provide sufficient security, thereby necessitating the development of more robust encryption techniques.

Koppu et al. [14] proposed a Self-Adaptive Grey Wolf Optimization (GWO) algorithm to enhance the security of medical image encryption through optimized 2D Logistic Chaotic Mapping (2DCM). Their findings demonstrated that the proposed method achieved superior key sensitivity, with percentage differences of 1%, 2.29%, and 2.07% for ultrasound images compared to standard, Genetic Algorithm (GA), and GWO methods, respectively. Additionally, the GWO method outperformed existing techniques in terms of noise sensitivity, achieving better performance in Chi-square tests and showing less deviation from uniform histograms, ultimately providing a more secure and efficient encryption process against various attacks.

Sun et al. [15] developed a robust method for medical image authentication that utilizes wavelet reconstruction and fractal dimension analysis to enhance security in telemedicine. The proposed scheme involves obtaining low-frequency detail regions through discrete wavelet transform, reconstructing approximate data, and analyzing the fractal dimension of stable feature regions to construct a feature matrix. This method effectively reduces redundancy in medical images while extracting key features, demonstrating strong resistance to various attacks, including JPEG compression, noise, and rotation. The findings highlight the method's ability to ensure the authenticity and integrity of medical images without introducing additional noise, thereby significantly improving security in E-health applications.

Thanki et al. [16] proposed a robust and hybrid watermarking scheme to enhance the security of medical images in telemedicine by combining techniques such as finite ridgelet transform (FRT), singular value decomposition (SVD), and Arnold scrambling-based encryption. This multifaceted approach integrates confidential patient information into medical images, ensuring identification and authentication while preserving visual integrity. The scheme demonstrates superior imperceptibility, with PSNR values ranging from 35 dB to 59 dB, and strong resistance to watermarking attacks, maintaining normalized correlation values above 0.75. Furthermore, its encryption and decryption processes are computationally efficient, making it highly suitable for telemedicine applications. The integration of advanced watermarking techniques like this has become essential in addressing challenges related to data integrity and confidentiality in telemedicine, as evidenced by various algorithms such as SVD-DCT and hybrid methods. These approaches facilitate secure sharing of sensitive medical data and protect against tampering and unauthorized access, reinforcing their critical role in modern clinical environments.

CHAPTER 3
SYSTEM ANALYSIS

3.1 EXISTING SYSTEM:

Multimedia security, particularly in safeguarding medical images, was the focus of numerous studies that proposed diverse techniques such as watermarking, steganography, and a limited number of encryption algorithms. Common approaches included DES, Arnold scrambling, pixel permutation, Self-Adaptive Grey Wolf Optimization, LSB steganography, and transformations like SVD, DWT, DCT, chaotic maps, series, and the Lorenz map. Steganographic algorithms often enhanced security by using a cover image to conceal sensitive medical data, while encryption algorithms, though less frequently researched, typically employed fixed or restricted key sizes for securing information. Watermarking techniques were applied in spatial, frequency, or hybrid domains, with some studies addressing image distortion by segmenting the image into regions of interest (ROI) and non-interest, embedding watermarks in non-interest regions to preserve image quality. These methodologies collectively aimed to protect medical images against various threats, including cryptanalysis, JPEG compression, cropping, filtering, brute-force attacks, chosen-plaintext attacks, differential attacks, and tampering.

Limitations:

1. Watermarked images are vulnerable to attacks such as cropping, rotation, compression.
2. Limited image datasets used in many studies can lead to overfitting.
3. Images encoded using techniques like watermarking or steganography or other similar methods often exhibit visible changes that affect image quality, potentially causing misdiagnosis, especially for critical diseases such as brain tumors and cancer.

4. Such techniques may result in low to moderate PSNR values, impacting the imperceptibility of the encoding.
5. Poorly implemented watermarking can significantly distort images, especially in 3D images, where maintaining spatial consistency is crucial.
6. Encryption algorithms like DES, with their low-key sizes, are prone to attacks such as brute force or differential cryptanalysis.

3.2 PROPOSED SYSTEM:

Existing encryption methods, while effective in certain contexts, often face limitations in terms of security, speed, accuracy, computational efficiency, resilience to modern, complex attacks or a combination of these factors. To address these issues, hybrid encryption algorithms combine the strengths of multiple encryption techniques, offering a balanced solution that enhances both security and efficiency. These hybrid approaches integrate symmetric and asymmetric encryption methods, leveraging the strengths of both to ensure high levels of security while maintaining computational efficiency. They not only increase the resilience of the encryption system against a wider range of attacks but also optimize performance in environments with limited computational resources. Hybrid encryption systems are particularly useful in real-time applications, such as medical image transmission, where both security and speed are critical. By combining the strengths of various algorithms, hybrid encryption offers greater flexibility and adaptability, making it an ideal solution for modern security challenges in diverse applications.

The hybrid encryption algorithms are proposed and implemented in the algorithms section of the modules chapter. The general architecture of the proposed hybrid encryption algorithm is shown in Fig. 1.

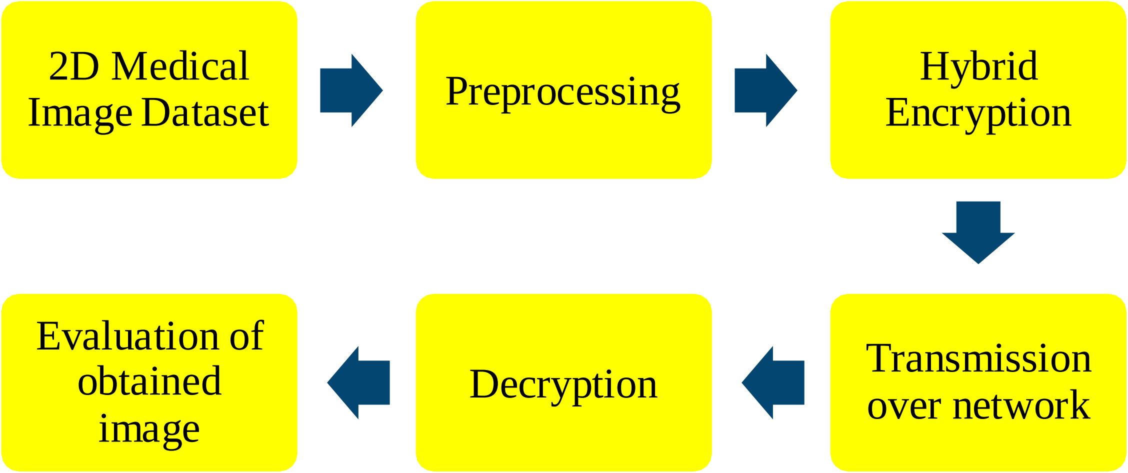


Fig. 3.1 Generalized flow diagram of proposed hybrid algorithm

Each algorithm’s strengths and weaknesses are discussed below in detail, highlighting how they complement each other to create a more robust system. Additionally, the subsequent sections outline how the weaknesses of individual algorithms are mitigated through their integration, and how the combination of their strengths leads to superior performance in real-time encryption tasks.

Algorithm	**Type**	**Key Feature**	**Key Size**	**Advantages**	**Weaknesses**
RSA	Asymmetric (Public-key)	Uses two keys: public and private	1024-4096 bits	Relies on factoring large composite numbers, has strong security, and are widely used for key exchange	Slow encryption/decryption, large key sizes
ECC	Asymmetric (Public-key)	Based on elliptic curves for encryption	Typically, 256 bits	Smaller keys for equivalent security to RSA	Requires careful implementation to avoid vulnerabilitie

					s
AES	Symmetric (Private-key)	Block cipher with 128-bit block size	128, 192, or 256 bits	Industry standard for fast, highly secure data encryption.	Key management can be difficult in large systems
Blowfish	Symmetric (Private-key)	Variable key size, 64-bit block size	32-448 bits	Fast and efficient, good for smaller systems as it uses a small block size (64-bit)	Vulnerable to brute force with short keys and birthday attacks.
DES	Symmetric (Private-key)	56-bit key, 64-bit block size	56 bits	Fast and simple, historically important	Obsolete, prone to brute-force and complex modern attacks
MD5	Hash function	Produces a 128-bit hash	128 bits (hash length)	Fast and simple	Broken due to collision vulnerabilities
SHA-256	Hash function	Produces a 256-bit hash	256 bits (hash length)	Secure, widely used and trusted for digital signatures and integrity checks	Computationally expensive compared to simpler hashes

DNA Cryptography	Experimental (Biological cryptography)	Uses DNA sequences for encryption and storage	N/A	Ultra-high-density data storage via biological molecules. Has high security due to biological complexity, difficult to reverse	Computationally expensive, not widely implemented
Chaotic Maps	Pseudorandom generation	Uses chaotic systems to generate random keys	N/A	Lightweight, highly sensitive to initial conditions, hard to predict, suitable for secure random number generation.	Can be unstable or difficult to implement securely in practice

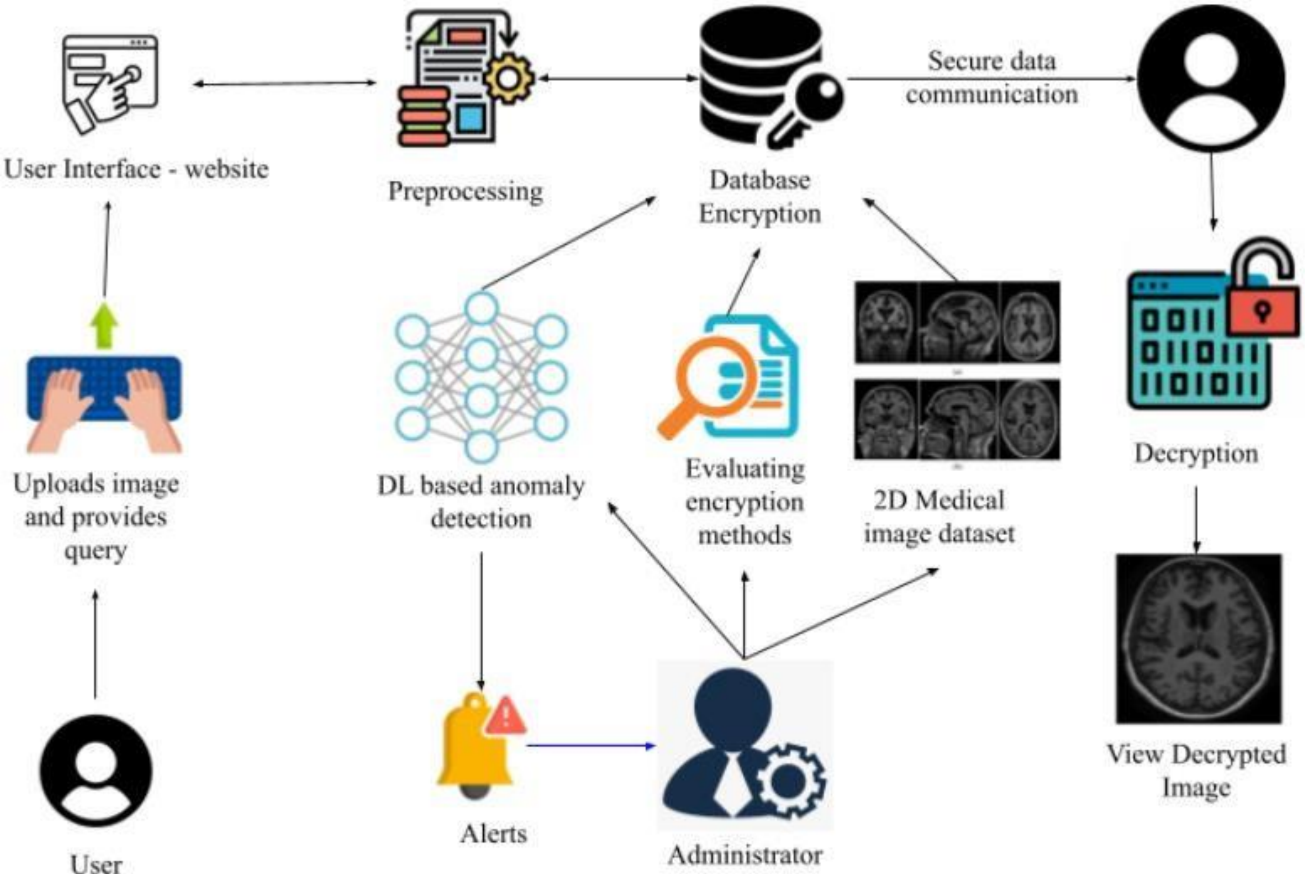
APPLICATIONS:

1. Telemedicine
2. IOT healthcare systems
3. Remote health monitoring systems
4. Healthcare websites, apps
5. Remote Diagnosis
6. Electronic Health Records (EHR) Systems
7. Digital Pathology
8. Tele-radiology
9. Medical Research
10. Medical Image Sharing Platforms, etc.

CHAPTER 4

SYSTEM DESIGN

4.1 ARCHITECTURE DIAGRAM:



4.2 MODULE DESCRIPTION:

1. ADMIN MODULE
   1. User Management
   2. Data Management
   3. Encryption Settings
2. USER MODULE
   1. User authentication
   2. Image upload and encryption
   3. View encrypted images.

3. DATASET COLLECTION
4. DATASET PREPROCESSING
5. IMAGE ENCRYPTION/DECRYPTION USING ALGORITHMS

4.2.1 ADMIN MODULE

4.2.1.1 USER MANAGEMENT

Administrators oversees and manages user accounts, roles, and permissions in user management. It ensures that each user is granted appropriate access based on their role, allowing for secure and efficient management of system resources. By defining specific roles (e.g., admin, healthcare provider, patient) and assigning corresponding permissions, user management helps maintain data security and ensures that sensitive information, such as medical images, is accessible only to authorized individuals. This approach enhances both user experience and system integrity.

4.2.1.2 DATA MANAGEMENT

Overseeing the management of medical image datasets involves tasks such as uploading, organizing, and maintaining data integrity. This includes securely storing images, properly categorizing by patient, procedure, or date, maintaining and regularly verifying their accuracy and consistency. Effective management ensures that medical images remain easily accessible to healthcare professionals while protecting against data corruption or unauthorized access, thereby supporting efficient clinical workflows and improving patient care.

4.2.1.3 ENCRYPTION SETTINGS

Configuring proposed seven hybrid encryption algorithms and settings for secure storage and transmission medical images.

4.2.2 USER MODULE

4.2.2.1 USER AUTHENTICATION

Implementing secure login and access control mechanisms for users involves ensuring that only authorized individuals can access the system. This is achieved through user authentication protocols, such as username/password combinations, multi-factor authentication, or biometric verification. By enforcing strict access control policies, the system ensures that users are granted appropriate permissions based on their roles, protecting sensitive medical data and maintaining system security.

4.2.2.2 IMAGE UPLOAD AND ENCRYPTION

Allowing users to upload medical images for encryption involves providing a user-friendly interface where authorized users can securely upload 2D medical images. Once uploaded, the system applies the selected hybrid encryption algorithms to protect the images from unauthorized access during storage or transmission. The encryption process ensures that patient data remains confidential and secure while allowing for efficient processing and retrieval when needed.

4.2.2.3 VIEW ENCRYPTED IMAGES

Enabling users to access and view encrypted medical images ensures that authorized individuals can verify image integrity and authenticity. The system provides the ability to display encrypted images along with their corresponding cryptographic hashes, which are used to verify the integrity of the images. By comparing the generated hash with the stored hash, users can ensure that the images have not been tampered with, thereby maintaining the reliability and trustworthiness of the medical data.

4.3 DATASET COLLECTION

Collecting medical images involves acquiring a diverse set of high-quality images from various medical imaging devices, such as X-rays, CT scans, and MRIs, ensuring they cover a wide range of conditions and imaging techniques. The dataset used in this project is a part of the dataset present in Cancer Imaging archive and taken from Kaggle. Once collected, the images are stored in standardized formats, primarily Digital Imaging and Communications in Medicine (DICOM), which preserves essential metadata such as patient information, imaging parameters, and timestamps. Additionally, images are stored in Joint Photographic Experts Group (JPEG) format, which offers efficient compression for easier storage and transmission while maintaining acceptable image quality. This structured approach to collection and storage ensures the images are easily accessible, compatible with healthcare systems, and ready for further processing or analysis.

4.4 DATASET PREPROCESSING

Pre-processing refers to the transformations applied to our data before feeding it to the algorithm. Data preprocessing is a technique that is used to convert the raw data into a clean data set. In other words, whenever the data is gathered from different sources it is collected in raw format which is not feasible for the analysis.

4.5 IMAGE ENCRYPTION/DECRYPTION USING ALGORITHMS

The pre-processed medical images are encrypted using seven hybrid encryption algorithms proposed in this project, each combining different cryptographic techniques. These algorithms are evaluated based on their effectiveness in security, speed, and other performance factors with the results for all six-evaluation metrics discussed in later sections. The seven proposed algorithms are:

4.5.1 RSA+AES+SHA-256:

The first encryption method leverages a combination of asymmetric encryption (i.e., Rivest-Shamir-Adleman (RSA) algorithm) for key exchange and symmetric encryption (i.e., Advanced Encryption Standard (AES)) for fast data encryption. The asymmetric encryption system is responsible for securely transferring the symmetric encryption key between the communicating parties. Once the key is securely exchanged, the symmetric encryption algorithm is used to encrypt the medical image, ensuring both speed and security. To ensure that the data has not been altered in transit, a cryptographic hash function (Secure Hash Algorithm 256-bit, also referred to as SHA-256) is used to generate a digest of the original image. The encrypted image along with the hash is transmitted at the sender's side and is received at the receiver's side. Then the image is decrypted, and a hash of decrypted image is generated and is compared with the received hash to verify that the image has remained intact during transmission.

4.5.2 ECC+AES+SHA-256:

In this approach to securing medical image data, a multi-layered cryptographic system is utilized to address both the confidentiality and integrity of the data. To start, the technique uses a highly efficient method (i.e., Elliptic Curve Cryptography (ECC)) to create a shared key between two parties, ensuring that sensitive information can be exchanged securely. This method is especially advantageous in settings with limited computing power, such as mobile devices, as it achieves a high level of security using smaller key sizes, which reduces the computational load. After this secure key exchange, the system employs a fast and strong encryption mechanism (i.e., AES) to safeguard the image data. This encryption process ensures that the image is transformed into a format that cannot be understood without the proper decryption key. Beyond just encrypting the data, an additional step is taken to ensure the image has not been altered during transmission. A unique identifier, generated by a specialized algorithm (i.e., SHA-256), acts as a fingerprint of the image, allowing the receiver to verify that the data remains intact and unchanged. By combining these techniques, the system provides a balanced solution that prioritizes both security and performance, making it ideal for real-time applications in healthcare environments where quick access to protected data is essential.

4.5.3 AES+SHA-256:

The AES + SHA-256 hybrid algorithm offers a streamlined approach to securing medical images by combining efficient encryption with integrity verification. In this method, the data is encrypted using a symmetric encryption algorithm, which ensures both high speed and strong security. A shared key is used for the encryption process, meaning both the sender and receiver must possess the same key. Alongside the encryption, a cryptographic hash function is applied to the original image to generate a unique hash value. This hash serves as a digital fingerprint of the image, enabling the recipient to verify that the data has not been altered during transmission. After decryption, the receiver recalculates the hash of the decrypted image and compares it with the transmitted hash to confirm that the image is intact. This method is particularly suited for scenarios where asymmetric encryption is not required, offering a balance of speed and simplicity while ensuring the security and integrity of the image data.

4.5.4 Chaotic Maps + AES:

The Chaotic Maps + AES hybrid encryption method introduces an innovative layer of unpredictability to traditional AES encryption by leveraging the inherent randomness of chaotic systems. In this approach, a chaotic map is used to generate the encryption key. Chaotic systems are highly sensitive to initial conditions, meaning small changes in input can lead to drastically different outputs. This property creates a key that is highly unpredictable and difficult to replicate, even with knowledge of the system's parameters. Once the key is generated through the chaotic map, the AES algorithm is used to encrypt the medical image using the key, ensuring fast and strong protection of the data. On the receiver's side, the same chaotic map parameters are applied to regenerate the key, which is then used to decrypt the image. This combination of chaotic map-based key generation with AES encryption significantly increases security, making it more resistant to common cryptographic attacks. The approach is particularly valuable in contexts where data protection is critical, such as healthcare, finance, and secure communications.

4.5.5 DNA Cryptography + AES:

The DNA Cryptography + AES encryption method integrates biological encoding with traditional cryptographic techniques to enhance data security. Initially, the medical image is transformed into a DNA-like sequence, effectively leveraging the complex structure and high information density of DNA to represent the image. This encoding process adds an extra layer of obfuscation, ensuring that the image is no longer in a recognizable format. Once encoded into this DNA sequence, the image is then encrypted using AES, a fast and secure symmetric encryption algorithm. By using both DNA encoding and AES, the approach significantly strengthens the protection of the image, as an attacker would have to overcome both the challenges of decrypting the AES layer and understanding the DNA encoding. After the encrypted data is transmitted, the process is reversed:

AES is first applied to decrypt the data, and then the DNA sequence is decoded back into its original image form. While this dual encryption method offers a unique approach to securing medical images, it is computationally intensive, making it more suitable for niche applications where high security is a priority.

4.5.6 Blowfish + SHA-256:

This hybrid encryption approach utilizes Blowfish, a lightweight symmetric encryption technique, to ensure the confidentiality of medical images. Its design allows for rapid encryption and decryption processes, making it a strong candidate for resource-constrained environments, such as those with limited hardware capabilities. To protect the data further and ensure its integrity during transfer, the encrypted image is paired with SHA-256, a cryptographic hash function that generates a unique hash value. The hash acts as a checksum, enabling the recipient to verify the image's integrity by comparing the recalculated hash of the decrypted data with the original image. This combination offers an efficient solution where speed is crucial, especially in resource-constrained environments. However, it’s important to note that while Blowfish is effective for fast encryption, it is vulnerable certain types of cryptographic attacks, such as brute-force or birthday attacks.

4.5.7 DES + AES + MD5:

In this encryption scheme, the medical image is first secured using DES, a traditional symmetric encryption method known for its speed but considered vulnerable by modern standards. To reinforce the security, a second layer of encryption is applied using AES, a more robust and widely trusted encryption algorithm. This two-step process helps enhance the overall security of the image, though it’s worth noting that DES alone is not recommended for high-security environments due to its susceptibility to various cryptographic attacks.

Additionally, the integrity of the encrypted image is ensured using MD5, a hash function that generates a fixed-length digest of the encrypted data. This hash acts as a signature for the image, allowing the recipient to verify whether the data has been altered during transmission. However, MD5 has known weaknesses, including its vulnerability to collision attacks, which can lead to hash collisions and compromise data integrity.

While this layered approach provides additional security through multiple encryption techniques, it is not ideal for high-risk applications due to the weaknesses inherent in both DES and MD5. It is better suited for scenarios where a balance of performance and moderate security is required.

CHAPTER 5

SYSTEM SPECIFICATION

5.1 HARDWARE REQUIREMENTS

CPU: Intel Core i7/i9 (10th generation to 13th generation) or Intel Core Ultra 7/9 or AMD Ryzen 7 (5000 series or later)

RAM: 8/16 GB (DDR4/DDR5)

STORAGE: 512 GB SSD + 1 TB HDD

EXTERNAL CONNECTIONS: Keyboard, Mouse (wired or wireless)

MONITOR RESOLUTION: 1920 x 1080 (Full HD) or 4K (preferred)

GPU: NVIDIA GeForce GTX 1660 or AMD Radeon RX 6600 or higher

COOLING SYSTEM: Air or Liquid cooler

USB PORTS: 3.0

WIFI CONNECTION: Wi-Fi (802.11ac or later)

PRINTER: High-resolution printer (if required)

MINIMUM CPU CLOCK SPEED: 2.5 GHz or higher

5.2 SOFTWARE REQUIREMENTS

OS: Windows 11 or Linux (Ubuntu 20.04 LTS or later)

LANGUAGE: Python 3.12 or higher

PLATFORM/IDE: Jupyter Notebook or Google Colab or Colab Pro or Anaconda or Visual Studio Code

PYTHON LIBRARIES: Numpy, matplotlib, pycryptodome, seaborn, skimage (scikit-image), pillow, cryptography, os, scipy, sklearn, hashlib, time, random

DATASET SOURCE: Kaggle, Cancer Imaging Archive

BROWSER: Google Chrome or any modern browser

ADDITIONAL TOOLS: Python package manager (pip/conda)

CHAPTER 6
SOFTWARE SPECIFICATIONS

System specifications are critical to the successful execution of any project, ensuring the hardware and software capabilities align with the project requirements. For this project, the specifications are carefully chosen to support efficient processing, secure data handling, and advanced computational tasks. Below is a detailed overview of software requirements tailored to meet the demands of this project.

6.1 PYTHON

Python is a high-level, interpreted programming language created by Guido van Rossum and first released in 1991. It emphasizes readability and simplicity, making it ideal for beginners and professionals alike. Python supports multiple programming paradigms, including procedural, object-oriented, and functional programming.

Features: Python is known for its dynamic typing, extensive standard library, cross-platform compatibility, and strong support for integration with other languages and tools. It is particularly popular in fields like web development, data analysis, artificial intelligence, and scientific computing.

Evolution: Python has undergone significant evolution over the years, with major releases like Python 2.x and Python 3.x introducing several enhancements. The transition to Python 3 resolved compatibility issues and modernized the language, making it more efficient and feature-rich.

Version: The project uses Python 3.12 or higher, ensuring compatibility with the latest tools and libraries while benefiting from performance improvements and new features introduced in recent versions.

6.2 PYTHON LIBRARIES

6.2.1 NumPy

NumPy (Numerical Python) is a core library for numerical computations in Python. It provides powerful tools for creating and manipulating multi-dimensional arrays, which form the basis of numerical and scientific computations. With its extensive collection of mathematical functions, Numpy enables efficient operations on large datasets, such as matrix operations, linear algebra, Fourier transforms, and random number generation. Its performance is optimized through integration with low-level languages like C and Fortran, making it faster than traditional Python lists for array-based computations.

Numpy is fundamental for data analysis and machine learning workflows, serving as the backbone for many other libraries such as Pandas, Scikit-Learn, and TensorFlow. Its simplicity, versatility, and robust functionality make it an indispensable tool for data scientists, engineers, and researchers.

6.2.2 Matplotlib

Matplotlib is a plotting library used to create static, animated, and interactive visualizations. It is widely used for generating graphs, charts, and plots, making data visualization accessible and highly customizable. The library supports various plot types, such as line graphs, bar charts, scatter plots, and histograms, providing flexibility for diverse visualization needs. It integrates seamlessly with Numpy for numerical data and supports customization options like labels, colors, and styles to enhance clarity and aesthetics. Matplotlib's ease of use and extensive documentation make it a go-to choice for both beginners and advanced users in data analysis and scientific research.

6.2.3 Pycryptodome

Pycryptodome is a Python library for cryptographic operations, offering a wide range of tools for implementing robust security measures. It supports encryption and decryption using symmetric and asymmetric algorithms, such as AES, RSA, and ECC, ensuring the confidentiality of data. Additionally, it provides functionalities for hashing, digital signatures, secure key generation, and random number generation, which are crucial for maintaining data integrity and authenticity. Pycryptodome is designed to be a drop-in replacement for the PyCrypto library, offering enhanced performance and support for modern cryptographic standards. Its versatility and reliability make it a critical component for secure applications.

6.2.4 Seaborn

Seaborn is a data visualization library built on top of Matplotlib, designed to make the creation of attractive and informative statistical graphics simpler and more intuitive. It provides high-level interfaces for drawing visually appealing plots, such as heatmaps, pair plots, box plots, and violin plots, allowing for better exploration and understanding of datasets. Seaborn seamlessly integrates with Pandas DataFrames, enabling efficient handling of complex data structures. Its built-in themes and color palettes enhance the aesthetics of visualizations, making it an ideal choice for creating publication-quality graphics while maintaining ease of use.

6.2.5 Skimage (Scikit-Image)

Scikit-Image is a library for image processing in Python, built on top of Numpy and Scipy. It provides a comprehensive set of tools for tasks such as image segmentation, filtering, feature extraction, and transformation. These functionalities are crucial for analyzing and processing medical images, enabling tasks like identifying regions of interest, enhancing image quality, and detecting anomalies. Scikit-Image supports a variety of image formats and includes algorithms for both basic and advanced image processing techniques, such as edge detection, morphological operations, and multi-dimensional image analysis. Its ease of use and efficiency make it a preferred choice for researchers and developers in medical imaging and computer vision.

6.2.6 Pillow

Pillow is a modernized and actively maintained fork of the Python Imaging Library (PIL). It facilitates a wide range of image manipulation tasks, including resizing, cropping, rotating, and filtering, making it indispensable for handling image data in Python projects. Pillow supports numerous image file formats, such as JPEG, PNG, BMP, and GIF, and provides tools for format conversion, color management, and drawing text or shapes on images. Its simplicity and versatility make it a foundational library for preprocessing and transforming images in applications like medical imaging, computer vision, and graphic design.

6.2.7 Cryptography

Cryptography is a robust library that provides cryptographic recipes and primitives essential for implementing secure communication in Python. It supports a variety of operations, including encryption and decryption using modern algorithms like AES, RSA, and ChaCha20, as well as generating and verifying digital signatures to ensure data authenticity. The library also facilitates secure key management, including key generation, storage, and exchange, which are vital for maintaining the confidentiality and integrity of sensitive data. With a focus on simplicity and reliability, Cryptography ensures compliance with modern security standards, making it an indispensable tool for developing secure applications.

6.2.8 os

The os module is a standard library in Python that facilitates interaction with the operating system, making it a crucial tool for performing system-level tasks. It provides functions for file handling, such as creating, reading, writing, and deleting files, as well as directory manipulation like creating, renaming, and navigating directories. Additionally, the os module allows access to environment variables, system paths, and process management, enabling seamless integration of Python scripts with the underlying operating system. Its versatility and ease of use make it an essential component for automating and managing system-related operations in Python projects.

6.2.9 Scipy

Scipy builds on Numpy and extends its functionality by providing advanced scientific and engineering tools for complex computations. It includes modules for tasks such as optimization, signal processing, interpolation, integration, and statistical analysis, enabling efficient solutions to mathematical and scientific problems. Scipy also offers specialized submodules for areas like linear algebra, Fourier transforms, and image processing, making it versatile for diverse applications. Its performance is optimized for handling large datasets, and its extensive documentation makes it accessible to both researchers and developers. Scipy's capabilities significantly enhance the computational power of Python for scientific computing and data analysis.

6.2.10 Sklearn(Scikit-Learn)

Scikit-Learn is a powerful and widely-used machine learning library in Python, built on top of Numpy, Scipy, and Matplotlib. It offers an extensive suite of tools for tasks such as classification, regression, clustering, and dimensionality reduction. Additionally, it provides utilities for data preprocessing, model selection, and evaluation, enabling seamless integration into machine learning pipelines. Scikit-Learn includes efficient implementations of algorithms like Support Vector Machines, Random Forests, and K-Means, making it versatile for predictive modeling and anomaly detection. Its simplicity, comprehensive documentation, and consistent API make it an indispensable tool for both beginners and experts in data science and machine learning.

6.2.11 Hashlib

Hashlib is a standard Python library that provides secure hash and message digest algorithms for a variety of cryptographic applications. It supports popular hashing methods like SHA-256, SHA-512, and MD5, which are commonly used for data integrity checks, password storage, and digital signatures. Hashlib ensures that even small changes in input data result in significantly different hash values, making it effective for detecting data tampering. Its ease of use and support for both basic and advanced cryptographic standards make it a reliable choice for implementing secure hashing in Python projects.

6.2.12 Time

The time module is a standard Python library that offers functions for time-related operations, making it essential for tasks like performance monitoring, scheduling delays, and logging. It provides utilities for measuring execution time using functions like `time()` and `perf_counter()`, which are valuable for benchmarking code. The module also supports functions for introducing delays with `sleep()` and for retrieving the current time in various formats, including timestamps. Additionally, it includes tools for working with time-related data, such as converting between different representations of time. The time module is versatile and widely used in applications ranging from debugging to time-sensitive operations.

6.2.13 Random

The random module is a standard Python library used for generating pseudo-random numbers, essential for simulations, probabilistic computations, and testing. It provides functions like `randint()` and `uniform()` for generating random integers and floating-point numbers, respectively, and `choice()` for random sampling from sequences. The module also includes `shuffle()` for randomizing the order of elements in a list and `sample()` for selecting multiple random items without replacement. These capabilities make it valuable for tasks such as data augmentation, cryptographic salt generation, and modeling random events. Together with other Python libraries, the random module strengthens the project by enabling robust data handling, enhancing security, and delivering reliable, consistent results.

6.3 DEVELOPMENT ENVIRONMENT

The development environment for this project leverages versatile platforms and integrated development environments (IDEs) to ensure efficient coding, testing, and debugging. Jupyter Notebook and Google Colab provide interactive environments where code can be executed in cells, making it easy to visualize results and experiment with different solutions. Google Colab Pro enhances this experience by offering access to cloud-based computational resources such as GPUs and TPUs, which is ideal for resource-intensive tasks like image processing. Anaconda simplifies package management and deployment, providing an all-in-one solution for setting up a Python environment with the necessary libraries. Visual Studio Code, known for its lightweight yet powerful features, serves as another alternative for a streamlined coding experience with extensions that support Python development. These platforms collectively support the project's requirements, ensuring smooth development and execution.

CHAPTER 7
RESULTS AND DISCUSSION

The effectiveness of the encryption and decryption algorithms was assessed using various performance metrics, including Structural Similarity Index Measure (SSIM), Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Edge Preservation, and Encryption Time. These metrics collectively provide a detailed evaluation of the algorithms' ability to maintain image quality, structural integrity, pixel accuracy, and processing efficiency while ensuring the security of sensitive medical data. The results for each metric are summarized below:

Structural Similarity Index Measure (SSIM):

All the evaluated algorithms achieved an SSIM score of 1.0, confirming that the decrypted images perfectly preserved the structural integrity of the original images. This indicates no perceptual loss or distortion in the decrypted images, ensuring that the decrypted and original images are identical.

Mean Squared Error (MSE):

Each algorithm yielded an MSE value of 0.0, demonstrating that there was no deviation between the pixel values of the original and decrypted images. This perfect matching underscores the reliability of the encryption and decryption processes and validates their precision in handling medical image data, where even minor errors can affect diagnostic outcomes.

Peak Signal-to-Noise Ratio (PSNR):

The PSNR value for all algorithms was observed as infinity, signifying a complete absence of noise in the decrypted images. This highlights the exceptional performance of the decryption methods in preserving image quality and ensuring that no artifacts or distortions were introduced during the process.

Entropy:

Entropy values were computed to evaluate the randomness and unpredictability of pixel values in the encrypted images. The observed entropy values, as shown in the bar chart, were consistently high for all algorithms, indicating robust randomness and secure encryption. Higher entropy values signify that the encryption effectively obscured the original data, making it resistant to attacks. Entropy score observed for decrypted images for all algorithms is shown in the graph below:

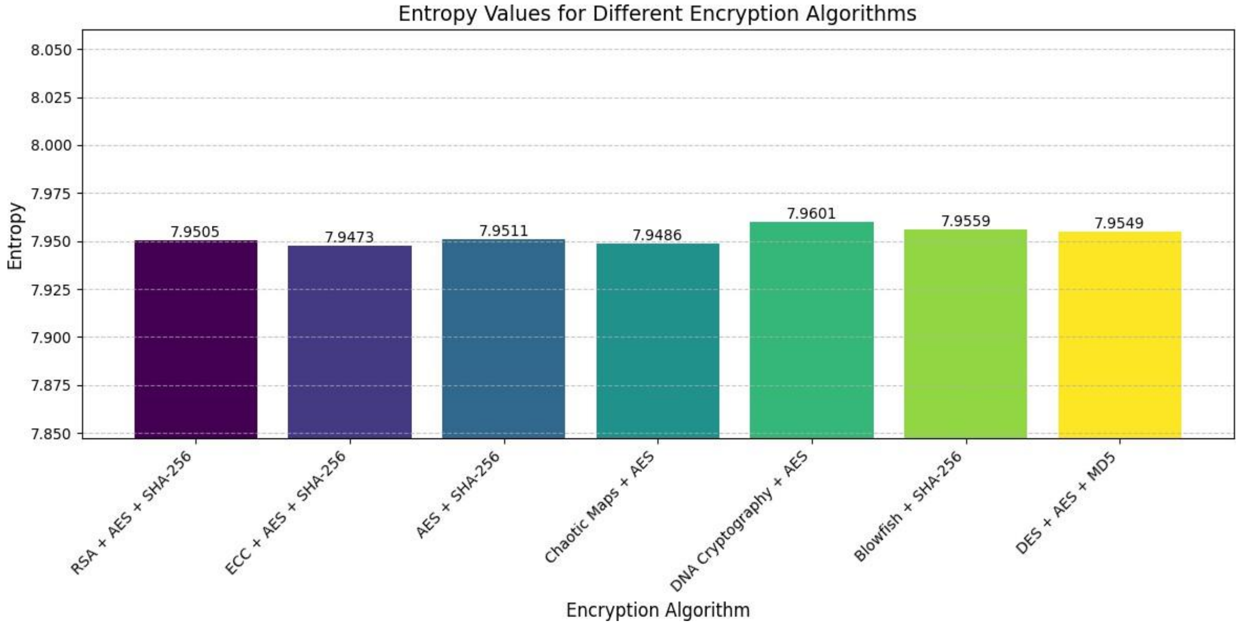


Fig 7.1 Entropy values for different encryption algorithms

Edge Preservation:

Edge preservation was analyzed using Canny edge detection, which confirmed that all algorithms produced an edge preservation score of 1.0. This result indicates that every edge detail was retained during the decryption process, an essential aspect for maintaining diagnostic accuracy in medical imaging.

Encryption Time:

The encryption time for each algorithm was recorded to assess their computational efficiency. The results showed significant variation across the algorithms, reflecting differences in their computational complexity. While some algorithms provided faster encryption times suitable for real-time applications, others, despite being slightly slower, offered higher security strength. A trade-off between encryption time and security level was observed, emphasizing the importance of algorithm selection based on application requirements. Encryption time observed for each decrypted image for all algorithms is shown in the table below:

Hybrid Encryption Algorithms	Encryption time for each medical image
1. RSA + AES + SHA-256	0.05696s
2. ECC + AES + SHA-256	0.00012s
3. AES + SHA-256	0.00004s
4. Chaotic Maps + AES	0.00003s
5. DNA Cryptography + AES	0.00004s
6. Blowfish + SHA-256	0.00008s
7. DES + AES + MD5	0.00010s

Table 1: Encryption time of all hybrid encryption algorithms

CHAPTER 8
CONCLUSION AND FUTURE WORK

This study evaluated various hybrid encryption algorithms to address the critical need for securing medical images in the digital healthcare domain. High entropy scores, observed for all the proposed algorithms, highlight their robustness against unauthorized access. Among these, DNA Cryptography + AES demonstrated the highest entropy, making it the most secure option, though its complexity may pose challenges for implementation. For organizations prioritizing speed, the Chaotic Maps + AES and Blowfish + SHA-256 combinations are ideal, offering rapid encryption times without compromising basic security. Additionally, the ECC + AES + SHA-256 algorithm is highly compatible with mobile devices, balancing security and efficiency for resource-constrained environments.

Future research can delve into encrypting 3D medical images, a domain that introduces unique challenges in terms of data handling and security due to the higher dimensionality and complexity of such datasets. Addressing these challenges will require innovative encryption techniques that can manage the increased computational load while ensuring data integrity and confidentiality. Additionally, there is significant potential to develop lightweight yet robust hybrid encryption algorithms that strike an optimal balance between security and performance. These advancements will be crucial in catering to the growing demands of modern healthcare applications, enabling secure data transmission while meeting the operational efficiency required in an interconnected digital healthcare landscape.

APPENDICES

A.1 SOURCE CODE:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

A.2 SCREENSHOTS

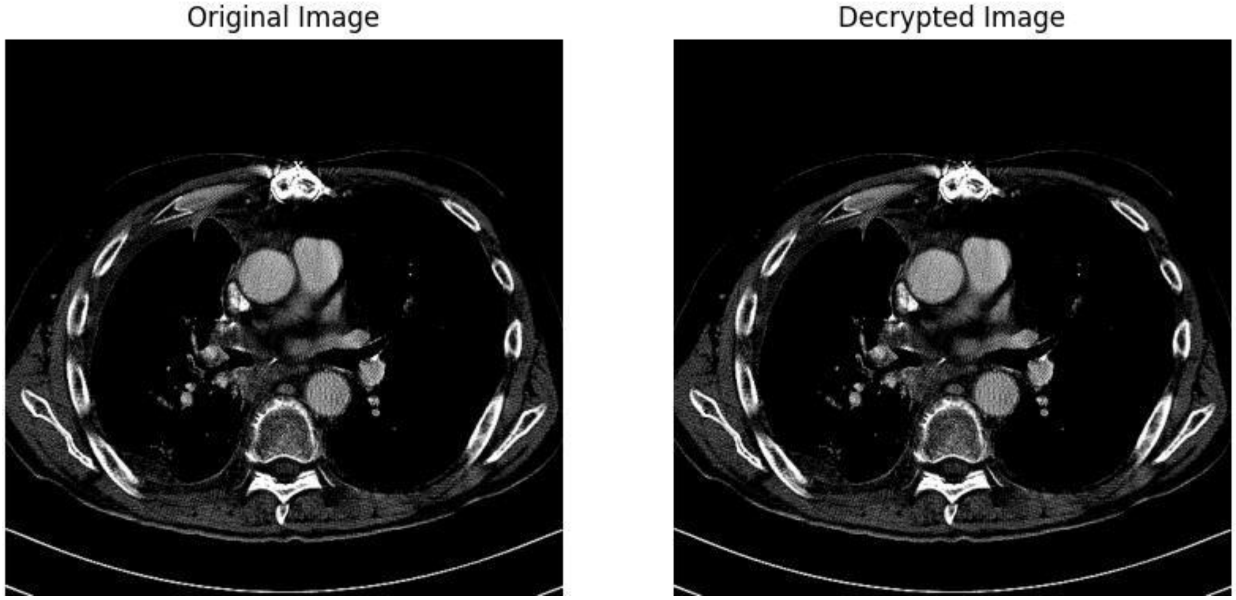
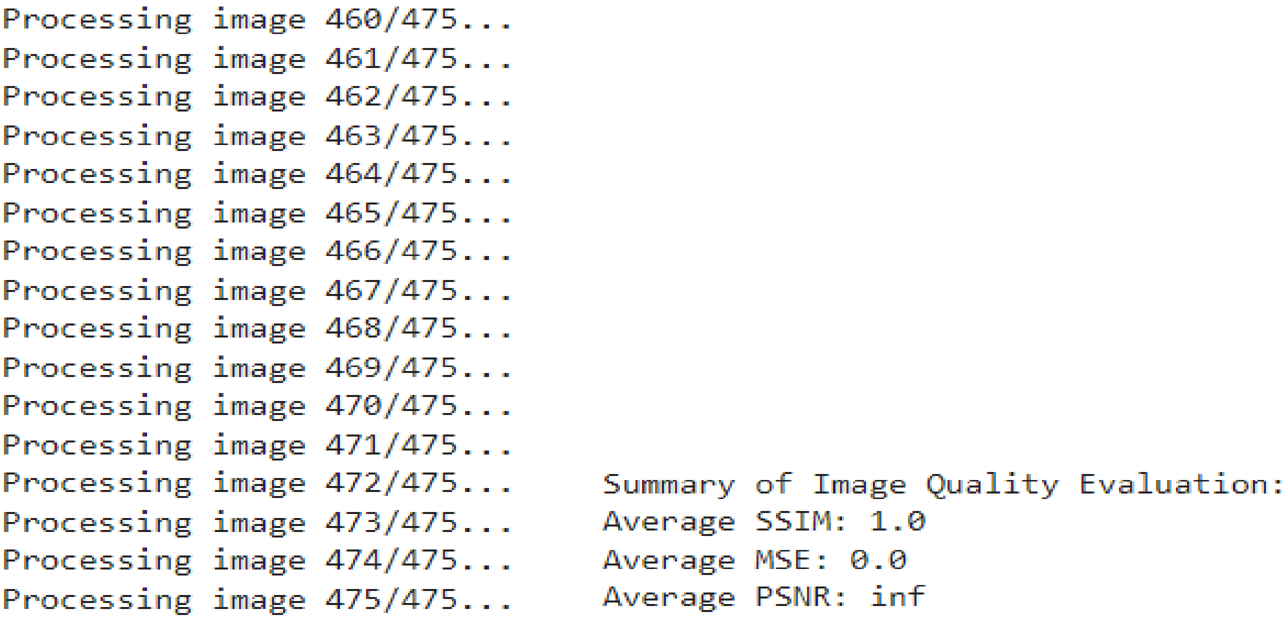


Fig. A.1 Original Vs Decrypted Image

No minor or visible changes were observed in the decrypted image when compared to the original image, as shown above. This indicates that the decryption process has successfully preserved the image's integrity without introducing any noticeable distortion. The comparison confirms that the encryption and decryption methods are robust, maintaining the original quality of the image throughout the process.



```
Processing image 460/475...
Processing image 461/475...
Processing image 462/475...
Processing image 463/475...
Processing image 464/475...
Processing image 465/475...
Processing image 466/475...
Processing image 467/475...
Processing image 468/475...
Processing image 469/475...
Processing image 470/475...
Processing image 471/475...
Processing image 472/475...     Summary of Image Quality Evaluation:
Processing image 473/475...     Average SSIM: 1.0
Processing image 474/475...     Average MSE: 0.0
Processing image 475/475...     Average PSNR: inf
```

Fig. A.2 Processing 2D image dataset and obtaining results

The image displays a sequence of messages indicating the progress of image processing. The image dataset has 475 images as shown above which are processed one by one. The results are summarized by averaging the scores of all the images and displayed to the end user.

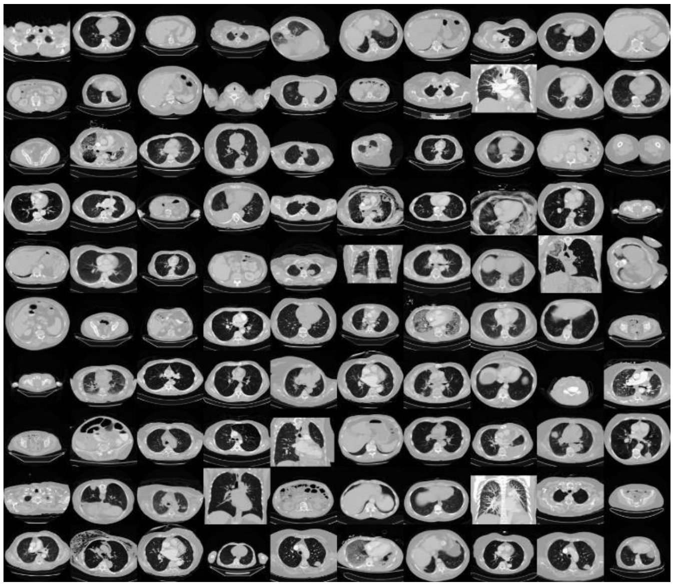


Fig. A.3 2D Medical image dataset

The image displays a grid of 100 grayscale images, representing cross-sectional scans of human lungs and heart. The images vary in appearance, showing different lung structures and potentially abnormalities. Some images appear clear and healthy, while others exhibit varying degrees of opacity or lesions, possibly indicating respiratory conditions. The arrangement of the images suggests a systematic organization, perhaps for comparison or analysis purposes.

REFERENCES

[1] Lili Nemec Zlatolas, Tatjana Welzer, & Lenka Lhotska. (2024). Data breaches in healthcare: security mechanisms for attack mitigation. Cluster Computing. https://doi.org/10.1007/s10586-024-04507-2

[2] Alzahrani, A., & Memon, N. A. (2021). Blind and Robust Watermarking Scheme in Hybrid Domain for Copyright Protection of Medical Images. *IEEE Access*, 9, 113714–113734. https://doi.org/10.1109/access.2021.3104985

[3] Rajendran, S., & Doraipandian, M. (2021). Chaos Based Secure Medical Image Transmission Model for IoT- Powered Healthcare Systems. *IOP Conference Series: Materials Science and Engineering, 1022,* 012106. https://doi.org/10.1088/1757-899x/1022/1/012106

[4] *DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption | IEEE Journals & Magazine | IEEE Xplore*. (n.d.). Ieeexplore.ieee.org. https://ieeexplore.ieee.org/abstract/document/9380566

[5] Alshehri, S. A. (2016). Neural network technique for image compression. *IET Image Processing*, *10*(3), 222–226. https://doi.org/10.1049/iet-ipr.2014.1039

[6] Alan Anwer Abdulla, Harin Sellahewa, & Sabah Jassim. (2014). *Stego Quality Enhancement by Message Size Reduction and Fibonacci Bit-Plane Mapping*. 151–166. https://doi.org/10.1007/978-3-319-14054-4_10

[7] Yuvaraja, T., & Sabeenian, R. S. (2018). Performance analysis of medical image security using steganography based on fuzzy logic. *Cluster Computing*, *22*(S2), 3285–3291. https://doi.org/10.1007/s10586-018-2096-0

[8] A Cryptographic Technique for Security of Medical Images in Health Information Systems. (2015). *Procedia Computer Science*, *58*, 538–543. https://doi.org/10.1016/j.procs.2015.08.070

[9] Yang, F., Mou, J., Sun, K., & Chu, R. (2020). Lossless image compression-encryption algorithm based on BP neural network and chaotic system. *Multimedia Tools and Applications*, *79*(27-28), 19963–19992. https://doi.org/10.1007/s11042-020-08821-w

[10] Niu, Y., & Zhang, X. (2020). A Novel Plaintext-Related Image Encryption Scheme Based on Chaotic System and Pixel Permutation. *IEEE Access*, *8*, 22082–22093. https://doi.org/10.1109/access.2020.2970103

[11] A, P., R, U., N, J., & S, P. (2021, February 1). *Securing Medical Images using Encryption and LSB Steganography*. IEEE Xplore. https://doi.org/10.1109/ICAECT49130.2021.9392396

[12] Shankar, K., Elhoseny, M., Chelvi, E. D., Lakshmanaprabu, S. K., & Wu, W. (2018). An Efficient Optimal Key Based Chaos Function for Medical Image Security. *IEEE Access*, *6*, 77145–77154. https://doi.org/10.1109/access.2018.2874026

[13] Jolfaei, A., Wu, X.-W., & Muthukkumarasamy, V. (2016). On the Security of Permutation-Only Image Encryption Schemes. *IEEE Transactions on Information Forensics and Security*, *11*(2), 235–246. https://doi.org/10.1109/tifs.2015.2489178

[14] Koppu, S., & Viswanatham, V. M. (2018). Medical image security enhancement using two-dimensional chaotic mapping optimized by self-adaptive grey wolf algorithm. *Evolutionary Intelligence*, *11*(1-2), 53–71. https://doi.org/10.1007/s12065-018-0159-z

[15] Sun, T., Wang, X., Lin, D., Bao, R., Jiang, D., Ding, B., & Li, D. (2021). Medical image security authentication method based on wavelet reconstruction and fractal dimension. *International Journal of Distributed Sensor Networks*, *17*(4), 155014772110141-155014772110141. https://doi.org/10.1177/15501477211014132

[16] Thanki, R., & Kothari, A. (2020). Multi-level security of medical images based on encryption and watermarking for telemedicine applications. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-020-09941-z

[17] Liu, V., Musen, M. A., & Chou, T. (2015). Data Breaches of Protected Health Information in the United States. *JAMA*, *313*(14), 1471. https://doi.org/10.1001/jama.2015.2252

[18]*Cybersecurity for Medical Imaging*. (n.d.). NEMA. https://www.nema.org/Standards/view/Cybersecurity-for-Medical-Imaging

[19] A Cryptographic Technique for Security of Medical Images in Health Information Systems. (2015). *Procedia Computer Science*, *58*, 538–543. https://doi.org/10.1016/j.procs.2015.08.070

[20] Avudaiappan, T., Balasubramanian, R., Pandiyan, S. S., Saravanan, M., Lakshmanaprabu, S. K., & Shankar, K. (2018). Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm. *Journal of Medical Systems*, *42*(11). https://doi.org/10.1007/s10916-018-1053-z

[21] Abbasi, F., & Memon, N. A. (2018). *Reversible Watermarking for the Security of Medical Image Databases*. https://doi.org/10.1109/ncg.2018.8593009

[22]Abdulla, A. A. (2015, October 1). *Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography*. Bear.buckingham.ac.uk. https://bear.buckingham.ac.uk/149/

[23]Alan Anwer Abdulla, Sabah Jassim, & Harin Sellahewa. (2013). Secure Steganography Technique Based on Bitplane Indexes. *ArXiv (Cornell University)*. https://doi.org/10.1109/ism.2013.55

[24]Al-Dmour, H., & Al-Ani, A. (2016). Quality optimized medical image information hiding algorithm that employs edge detection and data coding. Computer Methods and Programs in Biomedicine, 127, 24–43. https://doi.org/10.1016/j.cmpb.2016.01.011

[25] Al-Qershi, O. M., & Khoo, B. E. (2014). Controlling hiding capacity using image characteristics with a 2D-DE data hiding scheme. *AEU - International Journal of Electronics and Communications*, *68*(4), 346–350. https://doi.org/10.1016/j.aeue.2013.09.008

[26] S.Arunkumar, V. Subramaniyaswamy, & N. Sivaramakrishnan. (2018). Reversible Data Hiding scheme using modified Histogram Shifting in Encrypted Images for Bio-medical images. *International Journal of Pure and Applied Mathematics*, *119*(12e), 13233–13240. https://hal.science/hal-01826667

[27] Arunkumar, S., Subramaniyaswamy, V., Vijayakumar, V., Chilamkurti, N., & Logesh, R. (2019). SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. *Measurement*, *139*, 426–437. https://doi.org/10.1016/j.measurement.2019.02.069

[28]Ashour, A. S., & Dey, N. (2016). Security of Multimedia Contents: A Brief. Studies in Computational Intelligence, 3–14. https://doi.org/10.1007/978-3-319-44790-2_1

[29]Atawneh, S., Almomani, A., Al Bazar, H., Sumari, P., & Gupta, B. (2016). Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. *Multimedia Tools and Applications*, *76*(18), 18451–18472. https://doi.org/10.1007/s11042-016-3930-0

[30] Hayfaa Abdulzahra Atee, Ahmad, R., Norliza Mohd Noor, Monem, A., & Yazan Aljeroudi. (2017). *Extreme learning machine based optimal embedding location finder for image steganography*. *12*(2), e0170329–e0170329. https://doi.org/10.1371/journal.pone.0170329

[31] Balasubramanian, C., S. Selvakumar, & S. Geetha. (2014). *High payload image steganography with reduced distortion using octonary pixel pairing scheme*. *73*(3), 2223–2245. https://doi.org/10.1007/s11042-013-1640-4

[32]Bamal, R., & Kasana, S. S. (2019). Dual hybrid medical watermarking using walsh-slantlet transform. *Multimedia Tools and Applications*, *78*(13), 17899–17927. https://doi.org/10.1007/s11042-018-6820-9

[33] Alif Siddiqua Begum, A., & Nirmala, S. (2018). Secure visual cryptography for medical image using modified cuckoo search. *Multimedia Tools and Applications*, *77*(20), 27041–27060. https://doi.org/10.1007/s11042-018-5903-y

[34]Banu S, A., & Amirtharajan, R. (2020). A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach. *Medical & Biological Engineering & Computing*, *58*(7), 1445–1458. https://doi.org/10.1007/s11517-020-02178-w

[35] Benssalah, M., Rhaskali, Y., & Drouiche, K. (2020). An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. *Multimedia Tools and Applications*, *80*(2), 2081–2107. https://doi.org/10.1007/s11042-020-09775-9

[36] Cao, W., Zhou, Y., Chen, P., & Xia, L. (2017). Medical image encryption using edge maps. *Signal Processing*, *132*, 96–109. https://doi.org/10.1016/j.sigpro.2016.10.003

[37] Chauhan, D. S., Singh, A. K., Adarsh, A., Kumar, B., & Saini, J. P. (2017). Combining Mexican hat wavelet and spread spectrum for adaptive watermarking and its statistical detection using medical images. *Multimedia Tools and Applications*, *78*(10), 12647–12661. https://doi.org/10.1007/s11042-017-5348-8

[38] Chen, W.-J., Chang, C.-C., & Le, T. (2010). High payload steganography mechanism using hybrid edge detector. *Expert Systems with Applications*, *37*(4), 3292–3301. https://doi.org/10.1016/j.eswa.2009.09.050

[39] Chirakkarottu, S., & Mathew, S. (2019). A novel encryption method for medical images using 2D Zaslavski map and DNA cryptography. *SN Applied Sciences*, *2*(1). https://doi.org/10.1007/s42452-019-1685-8

[40] Conde, J. G., De, S., Hall, R. W., Johansen, E., Meglan, D., & Peng, G. C. Y. (2010). Telehealth Innovations in Health Education and Training. *Telemedicine Journal and E-Health*, *16*(1), 103–106. https://doi.org/10.1089/tmj.2009.0152