ABSTRACT

The rapid advancement of medical imaging technology has created significant challenges in maintaining the privacy, integrity, and security of sensitive MRI data, particularly as healthcare systems face increasingly sophisticated cyber threats. As medical images traverse networks and reside across various storage systems, they become vulnerable to unauthorized access, malicious tampering, and potentially devastating data breaches. To address these critical concerns, this work proposes a comprehensive, multi-layered security framework that synergistically combines steganography with three robust cryptographic encryption methods; AES-128, ASCON, and ECC to create an unprecedented level of protection for medical imaging data. The system first employs Least Significant Bit (LSB) steganography to cleverly conceal MRI scans within ordinary cover images, effectively hiding sensitive medical data in plain sight while preserving diagnostic quality. This stego-image then undergoes a rigorous triple-layer encryption process: AES-128 provides fast yet extremely secure symmetric encryption, ASCON delivers lightweight authenticated encryption to ensure data integrity with minimal computational overhead, and ECC facilitates secure key exchange through its efficient asymmetric cryptography. Access to protected images follows a strict authentication protocol where physicians or patients must first verify their identity using hospital credentials, followed by an additional verification layer for enhanced security. Only after successful authentication does the system initiate the carefully orchestrated decryption process first reversing the ECC key exchange, then verifying integrity through ASCON, and finally applying AES decryption ultimately extracting the original MRI image without any loss of quality or diagnostic value. To further bolster security, the system incorporates advanced integrity checking mechanisms that continuously monitor for any signs of data tampering, immediately alerting authorized personnel if irregularities are detected. By integrating multiple complementary security technologies into a cohesive framework, the solution provides defense-in-depth protection that addresses both current threats and emerging challenges in medical data security, while maintaining the usability and accessibility required in clinical environments.

ABSTRACT(TAMIL)

மருத்துவ படம் எடுத்தல் தொழில்நுட்பம் முன்னேறியதால், அதனுடன் தொடர்புடைய தனிப்பட்ட, மதிப்புள்ள மற்றும் பாதுகாக்க வேண்டிய MRI படங்களின் தனியுரிமை, ஒருமைப்படுத்தல் மற்றும் பாதுகாப்பு அதிக கவனத்திற்குரியதாக மாற்றியுள்ளது. மருத்துவத் துறைகள் தொடர்ந்து சைபர் தாக்குதல்களுக்கு இலக்காகி வரும் நிலையில், இத்தகைய தரவுகளை பாதுகாப்பது அவசியமாகியுள்ளது. இத்தேசியத்தை எதிர்கொள்வதற்காக, எங்கள் திட்டம் ஒரு விரிவான மற்றும் பல அடுக்குகளைக் கொண்ட பாதுகாப்பு கட்டமைப்பை முன்வைக்கிறது. இதில் ஸ்டீகனோகிராபி மற்றும் முக்கட்டான குறியாக்க முறைமைகள் இணைக்கப்பட்டுள்ளன, இதன் மூலம் மருத்துவ தரவுகள் சேமிப்பு மற்றும் பரிமாற்றம் நடைபெறும் போது பாதுகாக்கப்படுகின்றன. முதற்கட்டமாக, உண்மையான MRI படம் பொதுவான கவர் படத்தில் குறைந்த குறிப்பிடத்தக்க பிட் ஸ்டீகனோகிராபி தொழில்நுட்பத்தின் மூலம் மறைத்து வைக்கப்படுகிறது. இது பார்வையில் எந்தவித மாற்றமும் இல்லாமல் முக்கியமான தகவல்களை மறைக்கிறது. அதன் பின், அந்த ஸ்டீகோ படம் மூன்று அடுக்குகளில் குறியாக்கம் செய்யப்படுகிறது: AES-128 – வேகமான மற்றும் வலுவான சமமான குறியாக்கத்தை வழங்குகிறது, ASCON – குறைந்த வளங்களை தேவையாக்கும் இலகுரக மற்றும் உறுதிப்படுத்தப்பட்ட குறியாக்கத்தை வழங்குகிறது, ECC – குறியாக்க சாவிகளை பாதுகாப்பாக பரிமாற்றம் செய்யும் சமச்சீரற்ற குறியாக்க முறை. பாதுகாக்கப்பட்ட தரவுகளை அனுமதிக்கப்பட்ட பயனர்கள் மட்டுமே அணுகக்கூடிய வகையில், இந்த அமைப்பு மருத்துவமனையால் வழங்கப்படும் பயனர் பெயர் மற்றும் கடவுச்சொல் அடிப்படையிலான உள்நுழைவை அவசியமாக்குகிறது. அதன் பிறகு, நோயாளியின் அடையாள எண் மற்றும் ஒரு முறை கடவுச்சொல் மூலம் பயனர் பக்கம் கூடுதல் உறுதிப்படுத்தல் கட்டுப்பாடுகள் அமல்படுத்தப்படுகின்றன. இந்த சான்றிதழ் செயல் வெற்றிகரமாக முடிந்ததும், முக்கட்டான குறியாக்கங்களை முறையே எதிர்மறையாக செயல்படுத்தி, தரம் குறையாத உண்மையான MRI படம் மீட்டெடுக்கப்படுகிறது. மேலும், ஒருமைப்படுத்தல் சேகரிப்பு செயலி பிணையத்திலும் சேமிப்பிலும் உள்ள தரவுகள் எந்தவொரு மாற்றத்திற்கும் உட்பட்டதா என்பதை தொடர்ந்து கண்காணிக்கிறது. ஏதேனும் மாற்றம் ஏற்படும் போது, பயனருக்கு உடனடி மின்னஞ்சல் எச்சரிக்கையாக அனுப்பப்படுகிறது. இவ்வாறு, இந்த திட்டம் மருத்துவத் தரவுகளை பாதுகாப்பதற்கான நம்பகமான மற்றும் பிரயோஜனமிக்க பாதுகாப்பு தீர்வாக அமைகிறது.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

MRI	Magnetic Resonance Imaging
AES	Advanced Encryption Standard
UML	Unified Modelling Language
PID	Patient Identification Number
IoT	Internet of Things
LSB	Least Significant Bit
ECC	Elliptic Curve Cryptography
OTP	One-Time Password
GAN	Generative Adversarial Networks
PNG	Portable Network Graphics

CHAPTER – 1

INTRODUCTION

1. INTRODUCTION

1.1 Introduction

In the digital transformation of the healthcare industry, protecting sensitive patient data has become more important than ever. With advancements in medical imaging technologies such as MRI (Magnetic Resonance Imaging), hospitals and research institutions are now able to store and transmit large volumes of medical images electronically. While this enhances accessibility and efficiency, it also opens the door to potential data breaches, unauthorized access, and cyberattacks. A single compromised MRI image can not only violate a patient's privacy but also jeopardize diagnosis and treatment outcomes. Addressing this issue requires more than simply basic encryption—it calls for a smart, layered, and user-centric approach to data security. This project presents a multi-layered security framework that combines steganography and cryptography to secure medical images, with a specific focus on MRI scans. The process begins by using Least Significant Bit (LSB) steganography, a technique that hides the encrypted MRI image inside an innocent-looking cover image. This makes the medical data visually undetectable to unauthorized users, adding a layer of obscurity right at the start. Unlike traditional systems where data might simply be encrypted and stored, our approach conceals the very existence of sensitive information, making it much harder for attackers to even locate the target.

Once the image is hidden, a three-layer encryption process is applied to further strengthen security. The first layer uses AES-128 (Advanced Encryption Standard), a widely adopted symmetric encryption method known for its speed and reliability. The second layer incorporates ASCON, a modern lightweight cipher specifically designed for secure performance in resource-constrained environments, such as IoT or embedded medical devices. The final encryption layer utilizes Elliptic Curve Cryptography (ECC) to encrypt the encryption keys themselves, ensuring they can only be decrypted by an authorized user. This multi-level cryptographic strategy ensures not only the confidentiality of the MRI image but also the protection of the keys used to encrypt it. In addition to strong encryption and hidden data transmission, the system includes a robust authentication process. Users—whether they are administrators uploading patient images or patients accessing their own records—must log in with secure credentials. For added protection, a one-time password (OTP) is sent to the user's registered email address, which must be entered to proceed further steps.

1.2 Objective

The primary objective of this project is to design and implement a highly secure and efficient system for protecting sensitive medical images, particularly MRI scans, from unauthorized access and cyber threats. In today's digital healthcare environment, the need for data confidentiality and integrity has become increasingly critical. This project aims to address that need by combining the strengths of cryptographic encryption and steganographic techniques into a single, cohesive framework. The system is designed to ensure that medical images remain confidential during storage and transmission by applying multiple layers of encryption. These include AES-128, ASCON, and Elliptic Curve Cryptography (ECC), each contributing a specific level of protection. AES-128 provides strong symmetric encryption for speed and data confidentiality. ASCON adds another layer of security with lightweight authenticated encryption, ideal for real-time healthcare applications. ECC secures the encryption keys, ensuring only verified users can access the original image. In addition to encryption, the project also incorporates steganography, where the encrypted medical image is hidden within a cover image using Least Significant Bit (LSB) embedding. This not only protects the content but also conceals its presence, reducing the likelihood of detection by malicious actors. Another key objective is to implement a secure user authentication process. Only users with valid credentials and one-time password verification can decrypt and view the original medical image. This prevents unauthorized access and adds an extra layer of security. Overall, the project strives to provide a user-friendly, scalable, and secure solution for healthcare institutions managing sensitive medical data.

1.3 Purpose

This The purpose of this project is to create a secure and user-friendly system for protecting medical images, especially MRI scans, from falling into the wrong hands. In today’s fast-moving healthcare world, doctors, hospitals, and even patients rely heavily on digital systems to store and access critical information. While this makes things faster and more convenient, it also makes sensitive data more vulnerable to cyberattacks and privacy breaches. Medical images are deeply personal and can reveal detailed health information about an individual. If such data is accessed or tampered with by unauthorized people, it can lead to profound consequences ranging from identity theft to incorrect medical treatments. That is why this project focuses on building a safety net that ensures only the right people can see and use this information. Achieve this, we have combined two smart techniques: encryption and steganography. Encryption scrambles the data so it cannot be understood without a key, while steganography hides the encrypted data inside another image, making it almost invisible. On top of that, we have added a secure login system with OTP (one-time password) verification, so only authorized users can unlock and access the original image. The goal is not just to make the system secure it is also to make it easy to use for both medical professionals and patients. This way, we are not only protecting information but also making sure it does not get in the way of timely medical care. In short, the purpose is to bring peace of mind to everyone involved in the digital healthcare process.

1.4 Scope

The scope of this project encompasses the development of a comprehensive, enterprise-grade security solution tailored specifically for protecting sensitive medical imaging data across healthcare ecosystems. Designed for deployment in hospitals, specialty clinics, and medical research facilities, the system establishes a robust framework for safeguarding critical diagnostic assets like MRI, CT, and X-ray images through a multi-layered defence strategy that integrates military-grade encryption protocols, advanced steganographic concealment techniques, and rigorous multi-factor authentication. At its core, the solution focuses on implementing granular access controls that ensure only vetted medical professionals, authorized staff members, and verified patients can retrieve protected images, while employing sophisticated obfuscation methods to thwart potential breaches by malicious actors. The technical architecture combines AES-256 encryption for data-at-rest protection, ASCON's lightweight cryptography for efficient real-time processing, and elliptic-curve cryptography for secure key exchange, complemented by adaptive steganography algorithms that embed sensitive metadata within the image pixels themselves without compromising diagnostic quality. Recognizing the diverse technical competencies of end-users in healthcare environments, the system features an intuitive interface with role-based workflows, automated security protocols, and contextual guidance to ensure seamless adoption by clinicians, radiologists, and administrative personnel alike. Beyond immediate security benefits, the project aims to transform medical data governance by establishing new standards for secure image sharing in collaborative care scenarios, clinical research collaborations, and cross-institutional consultations, ultimately enhancing both patient privacy and healthcare outcomes in an increasingly connected digital landscape.

CHAPTER - 2

LITERATURE SURVEY

2. LITERATURE SURVEY

1. ASIC Implementation of ASCON Lightweight Cryptography for IoT Applications.

Author names: K.D. Nguyen, T.-K. Dang, B. Kieu-Do-Nguyen, D.-H. Le, C.-K. Pham, and T.-T. Hoang.

The paper titled, “ASIC Implementation of ASCON Lightweight Cryptography for IoT Applications” by K.-D. Nguyen et al., focuses on designing a hardware-optimized (ASIC) implementation of the ASCON encryption algorithm, suitable for constrained environments like IoT devices. ASCON is a lightweight, authenticated encryption algorithm selected by NIST for its balance of security and performance. This paper emphasizes reducing power consumption, chip area, and latency, making it ideal for applications such as medical devices, where resources are limited. In the context of the mini project, ASCON is used as the second layer in a triple encryption system that secures MRI images. This base paper justifies the inclusion of ASCON by demonstrating its real-time performance capabilities and resilience against common cryptographic attacks. The ASIC implementation ensures that ASCON can be efficiently deployed even in low-power environments such as hospital systems or portable medical equipment. By adopting ASCON, the project benefits from both strong encryption and system scalability. The paper's findings support the feasibility of implementing high-performance, energy-efficient security mechanisms in healthcare, validating ASCON’s role in the project's layered encryption model. Thus, it forms a crucial technical foundation for enhancing confidentiality and integrity in medical image protection.

2. High-Performance Elliptic Curve Scalar Multiplication Architecture Based on Interleaved Mechanism.

Author names: J. Zhang et al.

This paper focuses on improving the speed and efficiency of a key process in Elliptic Curve Cryptography (ECC), called scalar multiplication. ECC is known for its strong security using smaller keys, but scalar multiplication can be slow and computationally demanding. To solve this, the authors propose a new design that uses something called an "interleaved mechanism," which allows the system to perform parts of the calculation at the same time, instead of one after the other. By doing so, they achieve much faster performance while still keeping the system lightweight and secure—perfect for devices or applications that have limited resources. Their design is especially useful in situations where quick and secure encryption is needed, like in mobile or embedded systems. The strength of this paper lies in showing that ECC, often thought of as too heavy for smaller systems, can actually be optimized to work efficiently. It’s a valuable contribution to the field of cryptography, particularly for anyone trying to build secure systems that also need to be fast and efficient.

3. A Multi-Scenario Authenticated Key Exchange Scheme with Forward Secrecy for Fog-Enabled VANETs

Author names: G. Yu, Q. Li, H. Mao, A. A. A. El-Latif, and J. J. P. C. Rodrigues.

This paper presents a secure key exchange scheme designed for environments where data needs to be transmitted safely across multiple devices, such as in fog-enabled vehicular networks (VANETs). These are systems where vehicles and roadside units communicate using cloud-like infrastructure, and security is a major concern due to constant data exchange. The authors introduce a method that ensures two major things: authentication communication and forward secrecy. Authentication makes sure that the devices involved in the communication are legitimate, while forward secrecy guarantees that even if one session key is compromised, previous keys remain safe. Their approach works efficiently in dynamic, real-world conditions where connections might change frequently—like moving cars or mobile users. What makes this work stand out is its ability to maintain strong security without slowing down performance, which is important for real-time systems. Though it's designed for vehicular networks, the concepts in this paper—secure key exchange, user authentication, and protection from data breaches—can be applied to other fields too. It offers valuable insights into building trustworthy systems where data privacy and real-time access are both essential.

4. A High-Performance Transparent Memory Data Encryption and Authentication Scheme Based on Ascon Cipher.

Author names: D. Xu, X. Wang, Q. Hao, J. Wang, S. Cui, and B. Liu.

This paper focuses on securing data stored in memory using a lightweight, yet powerful encryption method based on the Ascon cipher. The authors propose a system that can encrypt and authenticate memory data transparently, meaning it operates behind the scenes without requiring major changes to how memory is used or accessed. This is especially important for systems that handle sensitive information but also need to run smoothly and quickly. The Ascon cipher, which the scheme is built upon, is known for being efficient and secure, making it well-suited for environments like embedded systems or devices with limited resources. The paper shows how their approach can protect memory contents from tampering or unauthorized access without compromising system speed. By using Ascon in a clever way, the authors manage to provide robust encryption and authentication while keeping the system lightweight and fast. Their research is a strong example of how modern encryption can be integrated into real-world applications, especially where data privacy is critical—such as in healthcare or IoT-based systems.

5. Balanced Encoding of Near-Zero Correlation for an AES Implementation.

Author names: S. Lee, Jeong-Nyeo Kim.

The paper "ASIC Implementation of ASCON Lightweight Cryptography for IoT Applications" discusses the implementation of the ASCON lightweight cryptography algorithm in an Application-Specific Integrated Circuit (ASIC) for use in Internet of Things (IoT) devices. ASCON is designed to provide a secure and efficient encryption method while maintaining low resource consumption, making it suitable for constrained environments typical of IoT systems. The authors focus on the advantages of ASCON, such as its small footprint, low power usage, and fast processing speed, which are essential for IoT applications where devices often have limited processing power and memory. The paper presents the results of the ASIC implementation, demonstrating its effectiveness in terms of speed, area, and power consumption. By leveraging the ASIC implementation, the authors show that ASCON can be a viable cryptographic solution for securing IoT devices while meeting the stringent requirements of low-cost, low-energy, and high-performance systems.

6. Constructing Immune-Cover for Improving Holistic Security of Spatial Adaptive Steganography.

Author names: Y. Chen, H. Wang, and Wanjie L.

Traditional steganography aims to hide information within a cover image, but it's vulnerable to steganalysis, techniques that detect hidden messages. This paper argues that Immune-cover improves security against both conventional steganalysis methods and more advanced deep-learning-based steganalysis. The research indicates that using AIS to pre-process cover images strengthens steganography by making it more resistant to distortions introduced during the embedding process. It also makes the hidden information less detectable. A key advantage is that Immune cover maintains the visual quality of the cover image. It doesn't require retraining of Steg analyzers and can be applied to various cover images and steganographic techniques. In essence, Immune cover optimizes cover images using AIS principles to provide more robust and secure steganography.

7. Cover Selection in Encrypted Images.

Author names: J. Yu, J. Zhang, Z. Wang, F. Li, X. Zhang.

The paper "Cover Selection in Encrypted Images", introduces a method for selecting cover images in steganography when dealing with encrypted images. Steganography involves hiding a secret message within a seemingly innocent cover image. However, when the cover image itself is encrypted, the selection process becomes more complex. This paper tackles that challenge by proposing a technique that operates directly on encrypted images, enhancing security and privacy. Their method involves several key components. First, they employ partial encryption using the Most Significant Bit (MSB) encryption. This means that only a portion of the image data, specifically the most important bits, is encrypted. Second, they use block shuffling to further conceal the data. Finally, they incorporate Shifted Local Binary Pattern (SLBP) analysis to assess the complex texture of the encrypted images. SLBP helps in selecting suitable cover images for steganography. By using SLBP to guide cover selection, the method aims to choose images that are better suited for hiding information, making it harder for steganalysis techniques to detect the presence of a hidden message. A significant advantage of this approach is that it avoids the need to decrypt the cover image before performing steganography, preserving privacy.

8. Exploring Adversarial Attacks in Federated Learning for Medical Imaging.

Author names: E. Darzi, F. Dubost, N.M. Sijtsema, P.M.A. van Ooijen.

The paper "Exploring Adversarial Attacks in Federated Learning for Medical Imaging" explores the vulnerabilities of Federated Learning (FL) in the context of medical imaging. Federated Learning is a decentralized approach that allows models to be trained across multiple devices or institutions without sharing raw data, which is particularly beneficial for medical imaging, where data privacy and security are paramount. However, the authors investigate how adversarial attacks—deliberate attempts to manipulate or deceive a machine learning model—can affect the integrity and performance of FL systems. The paper highlights potential weaknesses in the FL framework, where attackers can exploit model updates sent from clients to the central server, leading to incorrect or biased model predictions. This is particularly dangerous in medical applications, where inaccurate predictions can have serious implications for patient outcomes. The authors examine different adversarial strategies and propose methods to detect, mitigate, or defend against such attacks in FL settings. Ultimately, the study emphasizes the need for enhanced security and robust techniques in Federated Learning to ensure safe deployment in sensitive medical environments.

9. Provably Secure Robust Image Steganography

Author names: Z. Yang, K. Chen, K. Zeng, W.Zhang, N. Yu

This paper "Provably Secure Robust Image Steganography", introduces PARIS, a novel approach to image steganography using Generative Adversarial Networks (GANs). Steganography aims to conceal secret messages within ordinary-looking images. PARIS focuses on achieving provable security and robustness, meaning it offers quantifiable security guarantees and maintains its effectiveness even under various image manipulations. The core idea is to map secret messages into a latent space, a lower-dimensional representation, and then use a GAN to generate stego images from these latent vectors. This process makes the hidden message more difficult to detect. A key advantage of PARIS is its resilience to lossy transformations like JPEG compression, which typically degrade image data and disrupt steganographic methods. PARIS allows for message recovery without needing a separate, pre-trained extractor. Instead, it employs gradient descent to retrieve the hidden information. The method relies on GANs for image generation and inverse transform sampling to convert uniform distributions into Gaussian latent vectors, contributing to its security and robustness.

10. Steganography With Generated Images: Leveraging Volatility to Enhance Security.

Author names: J. Zhang, K. Chen, W. Li,W.Zhang, N. Yu.

The paper "Steganography with Generated Images: Leveraging Volatility to Enhance Security" proposes a novel approach to steganography that leverages the generative capacity of deep neural networks, specifically generative adversarial networks (GANs), to create stego-images rather than modify existing ones. Traditional steganographic methods embed secret information into natural images by altering their pixels, which introduce detectable statistical anomalies and can be vulnerable to steganalysis. In contrast, this paper introduces generation-based steganography, where the image is entirely synthesized with the embedded message during the generation process itself. The authors emphasize the concept of volatility, meaning that each stego-image is unique and ephemeral, reducing the chances of detection due to repeated patterns. This strategy significantly enhances the security and undetectability of the steganographic process. Moreover, the paper presents an end-to-end framework integrating both a generator and an extractor, ensuring that the embedded message can be reliably recovered. The proposed method shows superior resistance to modern detection techniques and introduces a shift in how steganography can be approached in the age of AI-generated content. It highlights the potential of generative models to not only create realistic images but also redefine secure information hiding techniques.

11. High-Performance ECC Scalar Multiplication Architecture Based on Comb Method and Low-Latency Window Recoding Algorithm

Author names: J. Zhang, Z. Chen, M. Ma ,R. Jiang, H. Li ,W. Wang

This paper presents a high-efficiency hardware architecture for performing scalar multiplication in Elliptic Curve Cryptography (ECC), which is a critical operation for secure communications. The authors propose an improved scalar multiplication technique that combines the comb method with a novel low-latency window recording algorithm. The comb method is known for its regular computation pattern, making it highly suitable for parallel implementation in hardware. Meanwhile, the window recoding algorithm optimizes the representation of the scalar (secret key), reducing the number of required point additions and doublings. Together, these two innovations significantly enhance computation speed and reduce latency, making ECC more viable for high-performance and resource-constrained environments such as embedded systems and IoT devices. The architecture is designed to minimize critical path delay and improve throughput, all while maintaining security standards. Experimental results show that the proposed design achieves substantial improvements over existing implementations in terms of speed and hardware efficiency. This contribution is particularly valuable for applications where rapid cryptographic operations are essential, such as in secure wireless communication or blockchain systems.

12. Novel Optimized Implementations of Lightweight Cryptographic S-Boxes via SAT Solvers.

Author names: J. Feng, Y. Wei, F. Zhang, E. Pasalic, Yu Zhou

This paper introduces a novel approach for optimizing the design and implementation of lightweight cryptographic S-Boxes using SAT (Boolean satisfiability) solvers. S-Boxes (substitution boxes) are fundamental components in symmetric cryptography, playing a crucial role in ensuring nonlinearity and resistance to cryptanalytic attacks. The authors focus on minimizing the hardware cost of S-Box implementations, which is particularly important for constrained environments such as IoT devices and embedded systems. By encoding the problem of finding optimal S-Box representations into a SAT framework, the paper systematically searches for implementations that use fewer logic gates while maintaining cryptographic strength. The proposed method allows precise control over performance metrics like algebraic degree, nonlinearity, and differential uniformity, ensuring that the S-Boxes meet strict security requirements. Compared to traditional heuristic-based approaches, the SAT-based method offers deterministic guarantees and reproducible results. The authors also explore various S-Box structures and demonstrate how their method can find more compact and efficient logic realizations for known cryptographic S-Boxes. Experimental results show that the new implementations significantly reduce gate count and improve hardware efficiency without compromising security.

13. Design and Construction of a Low-Cryogen, Lightweight, Head-Only 7T MRI Magnet.

Author names: A. Wu, J. Ricci, G. Conte, C. Van Epps, M. Xu, Y. Bai, M. Parizh, W. Stautner, Y. Hua, M. Vermilyea, V. Soni.

This paper presents the design and development of a compact, low-cryogen, and lightweight 7 Tesla (7T) MRI magnet system intended specifically for head-only imaging. Traditional 7T MRI systems require large quantities of liquid helium for cooling and involve heavy, bulky magnet structures. To address these challenges, the authors propose a novel magnet configuration that drastically reduces cryogen consumption while maintaining the high magnetic field strength needed for ultra-high-resolution brain imaging. The design incorporates advanced superconducting wire technology, optimized coil configurations, and a cryogen-efficient cooling system that reduces both weight and operational complexity. By limiting the imaging region to the head, the system benefits from significant size and cost reductions without compromising image quality or performance. The lightweight nature of the magnet also enhances its potential for installation in smaller clinical or research facilities that cannot accommodate full body 7T systems. The paper details the electromagnetic design, cryostat engineering, and safety considerations of the system, along with initial testing results. This work represents a step forward in making high-field MRI more accessible, portable, and sustainable, particularly for neuroscientific and clinical research focused on brain disorders and advanced neuroimaging.

14. Cover Reproducible Steganography via Deep Generative Models.

Author names: K. Chen, H. Zhou, Y. Wang, M. Li, W. Zhang, N. Yu.

This paper introduces a new framework for steganography called cover reproducible steganography, which uses deep generative models to overcome key limitations in traditional and generation-based steganography. In most steganographic methods, a cover image is either modified or fully synthesized for embedding a secret message. However, these methods often lack cover reproducibility, meaning the same image cannot be regenerated again, making verification and synchronization difficult in practical applications. To address this, the authors propose a two-stage method using deep generative models such as GANs or diffusion models. First, a public latent representation of a natural-looking image is generated and reproducibly saved. Then, given the same latent input and a shared secret, the model can generate the same cover image with the hidden message embedded. This approach allows both sender and receiver to independently reproduce the same cover, enhancing reliability while maintaining high secrecy and low detectability. The framework enables practical advantages such as public cover verification, deterministic decoding, and resistance to image tampering. The experimental results show strong performance in both security and steganographic capacity. This work opens new possibilities for integrating AI-driven reproducibility into secure communication systems.

15. EG-FourQ: An Embedded GPU-Based Efficient ECC Cryptography Accelerator for Edge Computing.

Author names: J. Dong, P. Zhang, K. Sun, F. Xiao, F. Zheng, J. Lin.

This paper presents EG-FourQ, a high-performance and energy-efficient accelerator for elliptic curve cryptography (ECC) targeting embedded GPU platforms, particularly for edge computing scenarios. ECC is widely adopted in secure communications due to its strong security with small key sizes, but its intensive computations can burden low-power edge devices. EG-FourQ addresses this by implementing efficient scalar multiplication—the core operation in ECC—on embedded GPUs using the FourQ curve, which is known for its fast and secure arithmetic. The authors designed an optimized parallel computing strategy tailored to the GPU architecture, applying algorithmic improvements, memory access optimizations, and fine-grained parallelism to maximize throughput and minimize energy usage. Implemented on platforms like NVIDIA Jetson, EG-FourQ demonstrates substantial gains in both speed and power efficiency compared to conventional CPU-based or FPGA-based ECC solutions. By combining the mathematical advantages of FourQ with the parallel processing capabilities of embedded GPUs, this work provides a practical and scalable solution for secure cryptographic operations at the network edge. The proposed accelerator is well-suited for use in IoT, mobile, and other real-time edge applications that require secure and efficient data processing under hardware constraints.

16. Light-SAE: A Lightweight Authentication Protocol for Large-Scale IoT Environments Made with Constrained Devices.

Author names: P. Rosa, A. Souto, J. Cecílio.

This paper introduces Light-SAE, a lightweight authentication protocol specifically designed for large-scale Internet of Things (IoT) environments composed of constrained devices with limited computational power, memory, and energy. Traditional authentication methods are often too resource-intensive for such settings, creating a need for solutions that balance security with efficiency. Light-SAE offers a secure and scalable mechanism that enables mutual authentication between devices and servers while minimizing cryptographic overhead. The protocol is based on symmetric cryptography, carefully optimized to reduce the number of communication rounds and computational operations required. It also supports dynamic device registration and key management, making it suitable for rapidly changing IoT networks. The authors validate the protocol through formal security analysis and practical implementation on widely used embedded platforms. The results show that Light-SAE outperforms many existing approaches in terms of energy consumption, processing time, and memory usage, without compromising the level of security required in modern IoT systems.

This work is particularly relevant for environments such as smart cities, industrial automation, and home automation, where numerous low-power devices must securely communicate and authenticate under tight resource constraints.

17. Lightweight Encryption and Authentication for Controller Area Network of Autonomous Vehicles.

Author names: J. Cui, Y. Chen, H. Zhong, D. He, L. Wei, I. Bolodurina, L. Liu.

This paper presents a lightweight encryption and authentication scheme tailored for the Controller Area Network (CAN) used in autonomous vehicles. The CAN protocol, while widely adopted for in-vehicle communication, lacks built-in security mechanisms, making it vulnerable to attacks such as spoofing, replay, and unauthorized access. The proposed solution addresses these vulnerabilities by introducing a low-overhead cryptographic framework that ensures both data confidentiality and message authenticity. The authors design a symmetric key-based scheme that integrates lightweight encryption with message authentication codes (MACs), optimized to fit within the strict timing and computational constraints of CAN-based systems. Their method introduces minimal changes to the existing CAN infrastructure, ensuring backward compatibility and ease of deployment in current automotive environments. Extensive simulations and real-world testing show that the proposed protocol provides robust protection against known attacks with negligible impact on system performance and latency. The work is particularly significant for enhancing the cybersecurity of safety-critical components in autonomous vehicles, where secure and reliable communication is essential. This research contributes to the growing need for embedded, efficient, and scalable security solutions in the automotive domain as vehicles become increasingly connected and autonomous.

18. Low Area and Low Power Threshold Implementation Design Technique for AES S-Box.

Author names: J. Song, K. Lee, J. Park.

This paper proposes a novel design technique for implementing the AES S-Box that minimizes both hardware area and power consumption while maintaining resistance against side-channel attacks. The Advanced Encryption Standard (AES) S-Box is a non-linear component critical to the cipher's security, but its hardware implementation is often a target for power analysis attacks. To address this, the authors adopt and enhance a threshold implementation (TI) approach, which is a widely used countermeasure that offers provable resistance to first-order side-channel attacks. The proposed method focuses on optimizing the number of logic gates and shares required in the TI design, reducing resource usage without compromising security. Key improvements include a more compact logic structure and an efficient share-splitting mechanism that lowers switching activity, thereby decreasing power consumption. The design is particularly suited for lightweight and embedded cryptographic devices where physical resources and battery life are limited. Experimental results and synthesis data demonstrate that the new design achieves significant reductions in both area and power compared to conventional TI-based AES S-Box implementations.

19. Speed/Area-Efficient ECC Processor Implementation Over GF(2m) on FPGA via Novel Algorithm-Architecture Co-Design.

Author names M. Zeghid, H.Y. Ahmed, A. Chehri, A. Sghaier.

This paper presents a speed and area-efficient implementation of an Elliptic Curve Cryptography (ECC) processor over GF(2m) (binary field) on FPGA, achieved through a novel algorithm-architecture co-design approach. ECC is widely used for secure communications, but its implementation can be computationally expensive, especially in constrained environments. To address these challenges, the authors focus on optimizing both the algorithm and the hardware architecture in parallel, ensuring high performance while minimizing area and power consumption. The key contribution of this work is the co-design methodology that optimizes the elliptic curve scalar multiplication process by integrating an efficient multiplication algorithm with a custom hardware architecture. The approach involves using binary field arithmetic to take advantage of the parallelism offered by FPGA, thus improving processing speed. Additionally, the design reduces hardware resource usage by simplifying control logic and minimizing redundant operations. Experimental results on FPGA platforms demonstrate that the proposed processor significantly outperforms traditional ECC implementations in terms of speed, area, and power efficiency, making it suitable for use in resource-constrained environments such as IoT devices and mobile platforms.

20. LIGHT: Lightweight Authentication for Intra Embedded Integrated Electronic Systems.

Author names: X. Li, D. He, Y. Gao, X. Liu, S. Chan, M. Pan, K.K.R. Choo

This paper introduces LIGHT, a lightweight authentication protocol designed for intra-embedded integrated electronic systems, which are often used in environments with constrained resources such as smart devices, IoT, and embedded systems. As these systems become more connected, the need for secure communication grows, but traditional authentication protocols can be too resource-intensive for embedded devices with limited processing power, memory, and energy. The LIGHT protocol addresses this issue by providing an efficient solution for secure device authentication with minimal computational and communication overhead. The protocol leverages symmetric key-based cryptography combined with a simplified authentication mechanism that reduces the number of operations and message exchanges needed for secure communication. This makes it particularly well-suited for systems that operate under stringent resource constraints. The authors demonstrate through formal analysis and implementation that LIGHT achieves strong security guarantees, protecting against common threats such as unauthorized access and message replay attacks, while maintaining low latency and power consumption. This work provides a promising approach to enhancing the security of embedded electronic systems without significantly impacting their performance or resource usage.

CHAPTER - 3

SYSTEM REQUIREMENTS

3. REQUIREMENTS AND SPECIFICATIONS

3.1 SOFTWARE REQUIREMENTS

Operating System	: Windows 11
Platform	: Visual studio code (VS code), Web application
Libraries	: flask, pycryptodome, ecdsa, pillow, Tkinter

3.2 SOFTWARE ENVIRONMENT

The platforms and infrastructures were used in our project are mentioned below and briefly explained.

3.2.1 WINDOWS 11

The Microsoft Windows Operating system is the latest version in the Windows 11. It is the successor of Windows 10 and was announced by Microsoft on June 24, 2021. Windows 11 has several new features, a bunch of visual enhancements and improvements over its predecessor. It has a new user interface and corresponding UI enhancements that could convey a more efficient and simplistic exploration of how to work with digital content and watermarking tools.

3.2.2 VISUAL STUDIO CODE

Visual Studio Code (VS Code) is a free, open-source, and powerful code editor developed by Microsoft. It is widely used by developers for building applications across various programming languages, including Python, JavaScript, C++, and more. In the context of the Securing MRI Images by Stego-Crypto Encryption project, VS Code serves as the primary development environment, offering features like intelligent code completion, real-time debugging, and Git integration, all of which streamline the development process.

3.2.3 WEB APPLICATION

A web application is a software program that runs on a web server and is accessed through a web browser using the internet. Unlike traditional desktop applications that need to be installed on a computer, web applications can be used from any device with an internet connection, making them highly accessible and user-friendly. They typically use a combination of front-end technologies (like HTML, CSS, JavaScript) and back-end technologies (such as Python, PHP, or Node.js) to provide interactive and dynamic user experiences.

3.3 TECHNOLOGIES AND LIBRARIES

Tkinter: Python's standard GUI library for making interactive graphical user interfaces is Tkinter. It offers a set of widgets such as buttons, labels, text boxes, and menus which are used to gain visual feedback from the users. File lists, popups and input dialogs are displayed in this system using Tkinter as the basis. Its windowing system integration is lightweight, fast, cross platform and supports both Windows and Linux without the need for more installations.

Cryptography / Pycryptodome: These are the Python libraries used to implement secure encryption algorithms. They support symmetric encryption standards like AES-128, ensuring confidentiality of sensitive data. In this project, they are used to encrypt and decrypt MRI images before hiding or retrieving them via steganography.

Pillow: The Pillow libraries are used for handling and processing image files throughout the encryption and steganography workflow. Pillow supports image format conversions and manipulations; it enables advanced image analysis and pixel-level operations. Together, they ensure efficient image encoding, decoding, and display.

Hashlib: A built-in Python library called hashlib stores various secure hash functions such as SHA-256 that can be used to produce unique and tamper proof digital fingerprints on data. In this system, the SHA-256 hashes of file contents are computed during Merkle tree construction by hashlib in order to generate Merkle roots. File integrity validating roots are essential for these roots. This is especially important because hashlib guarantees strong data validation and a key ingredient in detecting the 'unauthorized modifications' even a small change would make the file's hash completely different.

Pyotp: The pyotp library is used to generate and verify time-based one-time passwords (TOTP) for secure user authentication. It ensures that only users with valid OTPs can access or decrypt sensitive medical images. This adds a dynamic layer of verification that strengthens access control.

ECDSA: The ECDSA library in this project is used as part of the final encryption layer based on Elliptic Curve Cryptography. It encrypts the AES and ASCON keys, enabling secure key exchange with compact key sizes. This ensures only authenticated users can decrypt and access the protected medical image data.

Os: The os module manages operating system calls. It permits the script to perform certain types of file operations like accessing directory paths, checking file existence, and actually handling file names. In this project, it is used to monitor files inside a directory, reacting to file changes including creation and modification, in turn helping to integrate with system-level resources.

Stegano: The stegano library is used to perform Least Significant Bit (LSB) steganography for hiding encrypted medical images within cover images. It embeds data in a way that is visually undetectable, preserving image quality. This technique ensures an additional layer of security by concealing the existence of the sensitive data.

Smtplib: The smtplib is a built-in Python library that enables sending emails via the Simple Mail Transfer Protocol (SMTP). In secure systems, it is commonly used to notify users through automated alerts. This makes it essential for delivering OTPs or alerts when unauthorized access or data tampering is detected.

Hmac: The hmac is a Python library used to ensure data integrity and authenticity by creating cryptographic hash-based message authentication codes. It combines a secret key with a message using secure hash functions. In this project, it validates encrypted data integrity, preventing tampering and unauthorized alterations during transmission or storage.

Numpy: The NumPy is a powerful Python library for numerical and matrix operations. It provides high-performance array structures and tools for numerical computations. In our project, NumPy is used to manipulate pixel data efficiently during the LSB steganography process, enabling precise embedding and extraction of hidden data from image matrices.

OpenCV: The OpenCV libraries are used for handling and processing image files throughout the encryption and steganography workflow. It supports image format conversions and manipulations, while OpenCV enables advanced image analysis and pixel-level operations. Together, they ensure efficient image encoding, decoding, and display.

CHAPTER - 4

SYSTEM STUDY

4. SYSTEM STUDY

4.1 FEASIBILITY STUDY

The proposed system presents a highly feasible and robust solution for implementation in medical environments, addressing critical needs for data security, operational efficiency, and regulatory compliance. From a technical standpoint, the system leverages a sophisticated architecture that combines LSB (Least Significant Bit) steganography with a triple-layer encryption framework comprising AES-128, ASCON, and ECC (Elliptic Curve Cryptography). This multi-layered approach ensures unparalleled data security, making it exceptionally resistant to unauthorized access and cyber threats. LSB steganography allows for the seamless embedding of sensitive patient data within MRI images, while the triple encryption mechanism provides an additional safeguard, ensuring that even if data is intercepted, it remains indecipherable without the proper decryption keys. This technical robustness is further enhanced by the system's adaptability to existing hospital IT infrastructure, requiring minimal modifications for integration. Operationally, the system is designed with a user-friendly interface that simplifies its adoption by medical staff, reducing the learning curve and minimizing disruptions to hospital workflows.

The inclusion of role-based access control ensures that only authorized personnel can access specific data, while OTP (One-Time Password) authentication adds an extra layer of security, preventing unauthorized logins. These features make the system particularly suitable for fast-paced medical environments where efficiency and security are paramount. Economically, the project is highly cost-effective, as it relies primarily on open-source tools and requires minimal hardware investments. This affordability makes it accessible to hospitals of varying sizes, from small clinics to large medical centers, without compromising on functionality or security. The system's scalability further enhances its appeal, as it can be easily expanded or modified to accommodate growing data volumes or evolving regulatory requirements. From a legal and ethical perspective, the system is designed to comply with stringent patient data protection standards such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation), ensuring that patient privacy and confidentiality are always maintained. This compliance not only mitigates legal risks for healthcare institutions but also fosters trust among patients, who can be assured that their sensitive information is being handled with the utmost care. Additionally, the system's ability to securely manage and transmit MRI images in real-time significantly improves operational efficiency, reducing delays in diagnosis and treatment. By streamlining data sharing between departments or even across different healthcare facilities, the system facilitates quicker decision-making and enhances patient outcomes.

The emphasis on safeguarding patient confidentiality while improving workflow efficiency underscores the system's potential to revolutionize how medical data is managed in hospitals. Overall, the project demonstrates strong potential for real-world deployment, offering a comprehensive solution that addresses the technical, operational, economic, and ethical challenges associated with managing sensitive medical data. Its combination of advanced security features, user-friendly design, cost-effectiveness, and regulatory compliance makes it an ideal choice for healthcare institutions looking to enhance their data management capabilities while ensuring the highest standards of patient privacy and security. The system's versatility and scalability further ensure its relevance in a rapidly evolving healthcare landscape, making it a future-proof investment for hospitals aiming to stay ahead in the digital age.

4.2 ECONOMICAL FEASIBILITY

The proposed system stands out as an economically viable solution for healthcare institutions seeking to enhance data security without incurring prohibitive costs. By leveraging open-source cryptographic libraries and steganography tools, the system significantly reduces software licensing expenses, which are often a major financial burden in proprietary security solutions. Libraries such as OpenSSL for AES-128 encryption, ASCON for lightweight cryptography, and widely available ECC implementations eliminate the need for costly third-party software, making advanced security accessible even to budget-constrained medical facilities. Additionally, the use of established steganography techniques ensures that sensitive patient data can be embedded within medical images without requiring expensive proprietary algorithms. The system's reliance on existing computing infrastructure further minimizes upfront investments, as hospitals can deploy it on their current servers and workstations without the need for specialized hardware. This approach not only lowers capital expenditures but also simplifies integration, as IT teams can implement the solution without overhauling their existing network architecture. Since the system focuses on digital image encryption and secure electronic transmission, it eliminates the logistical and financial costs associated with physical data handling, such as printing, storing, and transporting sensitive documents—a common expense in traditional medical record management.

Beyond initial cost savings, the system offers substantial long-term financial benefits by mitigating the risks of data breaches, which can be devastatingly expensive for healthcare providers. The average cost of a healthcare data breach far exceeds the expenses required to implement robust security measures like this system, making it a cost-effective preventive investment. Compliance with regulations such as HIPAA and GDPR also reduces the risk of costly legal penalties and reputational damage, which can arise from inadequate data protection. The system's scalability ensures that future upgrades or expansions—whether to accommodate larger datasets, additional users, or new security protocols—can be implemented with minimal financial strain. Unlike rigid proprietary systems that require expensive vendor support for scaling, this solution allows hospitals to adapt incrementally, using open-source updates and modular enhancements.

Moreover, the system's operational efficiency contributes to indirect cost savings by streamlining workflows. Secure, real-time transmission of MRI and other medical images reduces delays in diagnosis and treatment, optimizing hospital resource utilization and improving patient outcomes. The role-based access control and OTP authentication mechanisms further enhance efficiency by reducing administrative overhead in managing user permissions. By avoiding the need for multiple standalone security tools—such as separate encryption, access control, and authentication systems—the solution consolidates functionalities into a single, cost-efficient platform.

Ultimately, the system presents a sustainable and affordable approach to medical data security, aligning with the financial realities of modern healthcare institutions. Small clinics and large hospitals alike can adopt it without straining their budgets, ensuring that even resource-limited facilities can achieve high standards of patient data protection. In an era where cyber threats are escalating and regulatory demands are tightening, this solution provides a financially prudent way to safeguard sensitive information while maintaining operational flexibility. By balancing advanced security with economic feasibility, the system empowers healthcare providers to embrace digital transformation confidently, knowing that robust data protection does not have to come at an exorbitant cost.

4.3 TECHNICAL FEASIBILITY

The proposed system is technically feasible due to its strategic integration of proven, industry-standard cryptographic and steganographic techniques, each carefully selected to balance security, performance, and practical implementation requirements. At its core, the system employs a multi-layered encryption approach combining AES-128 (Advanced Encryption Standard with 128-bit keys), ASCON (a lightweight authenticated encryption algorithm), and ECC (Elliptic Curve Cryptography) - three well-established cryptographic methods that have undergone rigorous academic and industrial scrutiny. AES-128 serves as the workhorse for symmetric encryption, providing a robust and efficient method for securing bulk data with its 128-bit key strength, which has become the gold standard for data protection across numerous industries, from financial services to government applications. Complementing this, ASCON brings its unique advantages as a lightweight cryptographic solution, specifically designed to offer both confidentiality and data integrity while maintaining minimal computational overhead, making it particularly suitable for environments where system resources may be constrained or where energy efficiency is a priority. The inclusion of ECC adds another dimension of security through public-key cryptography, offering equivalent protection to traditional RSA systems but with significantly smaller key sizes, resulting in faster computations, reduced storage requirements, and lower bandwidth consumption - all critical factors in medical imaging environments where large files are routinely transmitted.

Beyond these encryption layers, the system incorporates LSB (Least Significant Bit) steganography as an additional security measure, embedding sensitive patient data directly within medical images in a manner that is both secure and visually imperceptible. This technique, while conceptually straightforward, provides an effective means of data concealment that has been thoroughly tested in various security contexts. The implementation leverages open-source steganography libraries, ensuring reliability and reducing development time while maintaining the visual fidelity of medical images - a crucial consideration in healthcare where diagnostic quality must never be compromised. The steganographic approach adds an extra barrier against unauthorized access, as potential attackers would need to first identify the presence of hidden data before even attempting decryption. Access control is managed through a comprehensive authentication framework combining traditional credential-based login with OTP (One-Time Password) verification, creating a multi-factor authentication system that significantly reduces the risk of unauthorized access. This dual-layer authentication mechanism is particularly valuable in hospital environments where multiple personnel may require access to sensitive data but where strict access controls must be maintained. The OTP component adds a dynamic security element that mitigates risks associated with stolen or compromised credentials, while the role-based access control ensures that users only have permissions appropriate to their clinical or administrative responsibilities.

From an implementation perspective, all system components are designed to work within standard programming environments and can be deployed on conventional computing hardware, eliminating the need for specialized infrastructure. The cryptographic libraries selected for the system are widely available, well-documented, and supported across multiple platforms, ensuring that healthcare institutions can find developers with the necessary expertise to implement and maintain the solution. Compatibility with existing hospital IT systems is a key consideration, with the architecture designed to integrate smoothly with common medical imaging formats and hospital information systems. The use of open standards and protocols further enhances interoperability, allowing the system to function within diverse healthcare IT ecosystems without requiring extensive customization. Performance optimization has been carefully considered throughout the design process, with particular attention paid to maintaining acceptable processing times for encryption and decryption operations, even when handling large medical image files. The combination of efficient algorithms (particularly ASCON and ECC) with careful system architecture ensures that security enhancements do not come at the cost of unacceptable delays in clinical workflows. This balance between security and performance is crucial in medical environments where timely access to patient data can have direct implications for care quality and outcomes.

The technical implementation also considers futureproofing, with modular design principles that allow for algorithm upgrades or replacements as cryptographic standards evolve. This adaptability ensures that the system can maintain its security posture over time without requiring complete redesigns, protecting the hospital's investment in the technology. The use of widely adopted cryptographic primitives also means that the system benefits from ongoing security research and community scrutiny, with any vulnerabilities in the underlying algorithms likely to be identified and addressed promptly by the broader security community. Collectively, these technical attributes demonstrate that the system is not only theoretically sound but also practically implementable within real-world healthcare environments. The careful selection of established technologies, attention to performance requirements, and consideration of implementation realities all contribute to a solution that hospitals can deploy with confidence, knowing that it meets both their security needs and operational constraints. The system's architecture successfully bridges the gap between cutting-edge security theory and practical healthcare IT requirements, delivering a solution that is as feasible to implement as it is robust in its protection of sensitive medical data.

4.4 SOCIAL FEASIBILITY

The system demonstrates strong social feasibility by directly responding to one of the most pressing concerns in modern healthcare - the protection of sensitive patient data in an increasingly digitalized medical landscape. As hospitals and clinics rapidly transition from paper-based to electronic health records, and as telemedicine and cloud-based medical imaging become more prevalent, patients and healthcare providers alike face growing anxieties about data privacy and security. The system addresses these concerns through its innovative stego-crypto approach, which combines steganography and cryptography to create a dual-layered security mechanism specifically designed for protecting sensitive MRI images and associated patient data. This solution comes at a critical time when healthcare data breaches are occurring with alarming frequency, often resulting in significant financial penalties for institutions and profound violations of patient trust. By implementing robust encryption that maintains both confidentiality and data integrity, the system helps restore confidence in digital healthcare systems, reassuring patients that their most sensitive medical information - including detailed diagnostic imaging - is protected against unauthorized access or tampering. The social value of this protection cannot be overstated, as medical imaging often contains not just clinical data but deeply personal information about a patient's body and health conditions.

The system's social acceptance is further enhanced by its alignment with evolving public expectations around data privacy. In the wake of high-profile data breaches across various industries and the implementation of stringent data protection regulations like GDPR and HIPAA, patients are becoming more aware and concerned about how their health information is handled. They increasingly expect healthcare providers to implement state-of-the-art security measures, and this system meets those expectations by employing advanced cryptographic techniques that represent current best practices in data security. The use of steganography to hide sensitive data within medical images adds an extra layer of protection that is particularly meaningful in healthcare contexts, where the visual integrity of medical images must be preserved for diagnostic purposes while still ensuring data security. This balanced approach demonstrates an understanding of both the technical requirements and the human factors involved in medical data security, making it more likely to be embraced by both healthcare professionals and patients. Moreover, the system promotes important social values in healthcare by supporting equitable access to secure medical services. Its design considerations for lightweight cryptography ensure that it can be implemented even in resource-constrained healthcare settings, preventing a scenario where only well-funded hospitals can afford proper data protection. This is particularly important in underserved communities where healthcare providers may lack extensive IT budgets but still handle equally sensitive patient data. The system's user-friendly design also reduces potential resistance from medical staff who might otherwise view stringent security measures as obstacles to efficient patient care. By integrating seamlessly with existing workflows while providing robust protection, the system avoids the common pitfall of security systems that are so cumbersome they encourage workarounds that compromise security.

The social impact of the system extends to strengthening the crucial trust relationship between patients and healthcare providers. When patients know their sensitive MRI data is protected by advanced security measures, they are more likely to share complete medical information and consent to valuable data sharing for research purposes, ultimately benefiting public health outcomes. This trust is especially important for vulnerable populations or patients dealing with stigmatized health conditions, who may have heightened concerns about privacy. The system's transparency in data handling - showing what protections are in place while still maintaining security - helps address the growing patient demand for both privacy and transparency in healthcare data management. As society becomes increasingly aware of digital privacy issues, with frequent media coverage of data breaches and identity theft, the public is developing higher standards for data protection across all sectors, particularly in sensitive areas like healthcare. The system positions healthcare providers to meet these rising expectations, giving them a competitive advantage in patient trust while fulfilling their ethical obligations to protect patient confidentiality. Its timing is particularly apt as healthcare systems worldwide accelerate their digital transformation due to the increased reliance on telemedicine and remote diagnostics brought about by recent global health challenges. By addressing both the technical requirements of data security and the human factors of trust and usability, the system demonstrates a comprehensive understanding of what makes a healthcare security solution socially viable. This makes the system not just technologically sound, but socially necessary and likely to be welcomed by all stakeholders in the healthcare ecosystem.

CHAPTER - 5

SYSTEM DESIGN

5. SYSTEM DESIGN

5.1 SYSTEM ARCHIECTURE

The architecture diagram presents a comprehensive and secure workflow for handling sensitive medical images through three well-defined components that ensure end-to-end protection of patient data. In the initial Image Handling phase, authorized administrators upload medical images such as MRIs or CT scans into the system through a secure interface designed to maintain data integrity from the point of entry. The system then processes these images through its robust Encryption Process, where multiple security layers are applied for maximum protection. This includes triple-layer encryption combining AES-128 for bulk encryption, ASCON for lightweight authenticated encryption, and ECC for secure key exchange, followed by LSB steganography that embeds patient data within the image pixels themselves. The encrypted images are then stored in highly secure cloud storage with additional safeguards like access logs and redundancy checks. The final Authenticator component forms the critical access control layer, implementing a strict two-factor authentication protocol. When medical professionals need to access patient records, they must first provide valid Patient ID verification matched against hospital records, followed by a dynamically generated one-time password (OTP) sent to their registered device.

Only after both authentication factors are successfully verified does the system initiate the decryption process, retrieving the protected images from cloud storage while maintaining a complete audit trail of all access attempts. This architecture ensures that sensitive medical data remains protected at every stage - during upload, storage, and retrieval - while still providing authorized healthcare providers with efficient access when needed for patient care, striking an optimal balance between security and usability in clinical environments. Role-based access controls ensure only authorized personnel can initiate uploads or access requests, while end-to-end encryption maintains security during data transmission. The system's modular design allows for seamless integration with existing hospital information systems, and real-time monitoring tools track all data transactions for compliance reporting. The layered security approach creates defence-in-depth protection, making the system resilient against both external cyber threats and internal breaches while maintaining the fast response times critical for medical workflows. The Figure 5.1 demonstrates the overall architecture of the system.

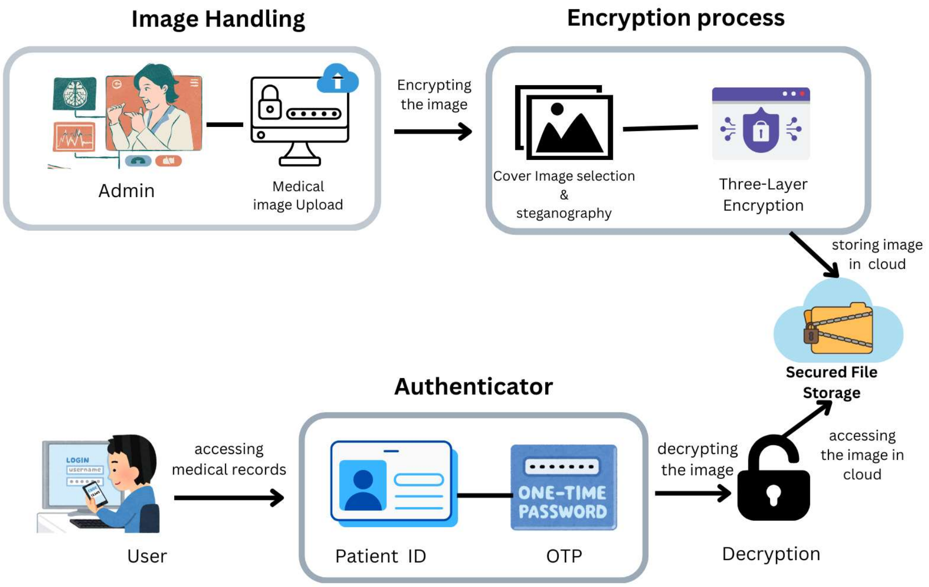


Figure 5.1: Overall Architecture Diagram

5.2 UML DIAGRAM

UML, or Unified Modelling Language, is a standardized general-purpose modelling language used in software engineering for visualizing, specifying, constructing, and documenting the artifacts of software systems. It provides a set of graphical notation techniques to create models of systems at various levels of abstraction, from conceptual to concrete. UML diagrams are graphical representations of different aspects of a system, such as its structure, behaviour, interactions, and architecture. They are used to depict different perspectives of a system, aiding in understanding, designing, communicating, and documenting software systems and processes. In a soundless credential system based on lip synchronization, UML diagrams can be utilized in various stages of the system development lifecycle to model various aspects of the system. The primary goals of UML diagrams are to:

Visualize and Design Systems: UML diagrams provide a graphical representation of software systems, allowing developers and stakeholders to visualize the system's structure, behaviour, and interactions. This visualization aids in designing the system's architecture and components.

Improve Understanding: By representing complex systems in a visual format, UML diagrams enhance understanding and comprehension of system functionalities, relationships between components, and overall system behaviour. This clarity reduces misunderstandings and facilitates effective collaboration among team members.

Facilitate Analysis and Planning: UML diagrams support various analysis activities such as requirements analysis, system modelling, and design validation. They enable stakeholders to analyse system requirements, identify potential design flaws or improvements, and plan system development and implementation strategies.

5.3 DATA FLOW DIAGRAM

The process begins with secure user authentication, where either medical professionals or patients log in through a multi-factor verified portal to initiate the upload procedure. Once authenticated, the user selects both the raw MRI scan and an appropriate cover image typically another medical image that maintains diagnostic quality while serving as a security vessel. The system then employs LSB (Least Significant Bit) steganography to meticulously embed the MRI data within the cover image's pixel structure, creating a stego object that appears identical to the original cover to human observation but contains the concealed medical information. This stego image then undergoes a rigorous triple-layer encryption process: first with AES-128 for robust symmetric encryption, followed by ASCON for lightweight authenticated encryption ensuring data integrity, and finally ECC for secure key exchange and additional protection.

The fully encrypted output is stored in a secure, access-controlled repository with multiple safeguards including activity logging and backup protocols. When retrieval is required, the system implements a stringent OTP-based authentication challenge, sending a time-sensitive one-time password to the user's registered device. Only after successful verification does the system initiate the reversal process – first decrypting the data using the appropriate cryptographic keys, then extracting the hidden MRI through de-steganography algorithms. The restored original MRI image is temporarily cached in a secure viewing environment where the authenticated user can access it for medical review or diagnostic purposes, with all access attempts recorded in an immutable audit trail for compliance monitoring and security analysis. The Figure 5.2 illustrates a comprehensive, security-focused workflow for handling sensitive MRI images within a medical system.

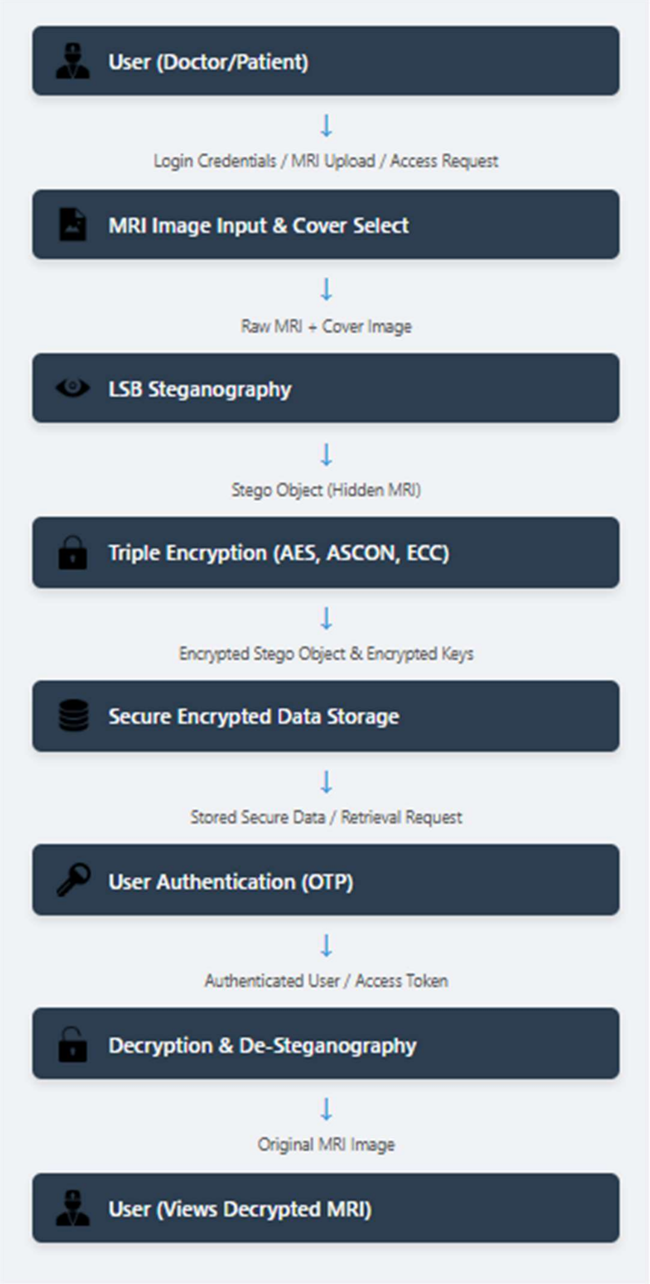

User (Doctor/Patient)
Login Credentials / MRI Upload / Access Request
MRI Image Input & Cover Select
Raw MRI + Cover Image
LSB Steganography
Stego Object (Hidden MRI)
Triple Encryption (AES, ASCON, ECC)
Encrypted Stego Object & Encrypted Keys
Secure Encrypted Data Storage
Stored Secure Data / Retrieval Request
User Authentication (OTP)
Authenticated User / Access Token
Decryption & De-Steganography
Original MRI Image
User (Views Decrypted MRI)

Figure 5.2: Data Flow Diagram

5.4 USE CASE DIAGRAM

For medical professionals, the diagram outlines a detailed workflow beginning with the Doctor's ability to upload sensitive MRI images to the system, which automatically initiates the "Secure Data" protocol as an included use case. This upload process is seamlessly integrated with the steganography function, where the Doctor selects an appropriate cover image from the system's repository or uploads a new one, ensuring the MRI data is concealed within what appears to be a standard medical image. The authentication functionality available to doctors serves a dual purpose: verifying their own credentials when accessing the system and, when necessary, authenticating other users such as specialists requiring temporary access to specific patient scans. The "Secure Data" use case, which is fundamental to all Doctor-initiated actions, can be extended to the "Decrypt Data" functionality when authorized access to the original MRI is required, demonstrating the system's flexible security model that adapts to legitimate clinical needs while maintaining stringent protection.

For system administrators, the diagram captures their critical role in maintaining the security infrastructure through several key responsibilities. The admin’s "Manage System" use case encompasses user account management, permission configuration, and system parameter adjustments, all of which inherently include security validations through the "Secure Data" protocol. Their "Monitor Integrity" function represents continuous surveillance of system activities, with the capability to trigger immediate security responses when anomalies are detected. This includes activating the "Security Breach Alert" extension, which not only notifies relevant stakeholders but also initiates automated countermeasures through the Security System actor. The Admin's OTP generation responsibility is particularly crucial, as it serves as the backbone for the system's two-factor authentication mechanism, ensuring that even if login credentials are compromised, unauthorized access remains blocked without the secondary verification.

The Security System actor in the diagram operates as both a proactive guardian and reactive defender within the ecosystem. It automatically enforces encryption protocols whenever data is processed or transferred and stands ready to respond to potential threats through its "Respond to Breach" use case, which may involve locking compromised accounts, initiating data protection sequences, or alerting administrators to suspicious activities. During normal operations, the Security System facilitates the "Assist Decryption" function, working in tandem with authorized users to safely retrieve original MRI images while maintaining a complete audit trail of all access attempts. Its role in authentication processes is particularly sophisticated, verifying OTP validity, checking device fingerprints, and evaluating access patterns to detect potential security risks before they materialize. The diagram effectively demonstrates how these three primary actors Doctor, Admin, and Security System – interact through carefully designed use cases to create a secure yet functional environment for handling sensitive medical images, balancing robust data protection with the practical needs of healthcare delivery. The inclusion relationships (like "Secure Data" being part of upload processes) and extension points (such as security breach responses) clearly illustrate how security is not an afterthought but rather an integral, pervasive element throughout all system functionalities, ensuring that patient confidentiality and data integrity are maintained at every interaction point while still allowing medical professionals to perform their critical work efficiently. The use case diagram in Figure 5.3 provides a comprehensive visualization of the Medical Image Security System's functional architecture, highlighting the distinct roles and interactions between key actors the Doctor, Admin, and Security System while emphasizing the system's robust security protocols.

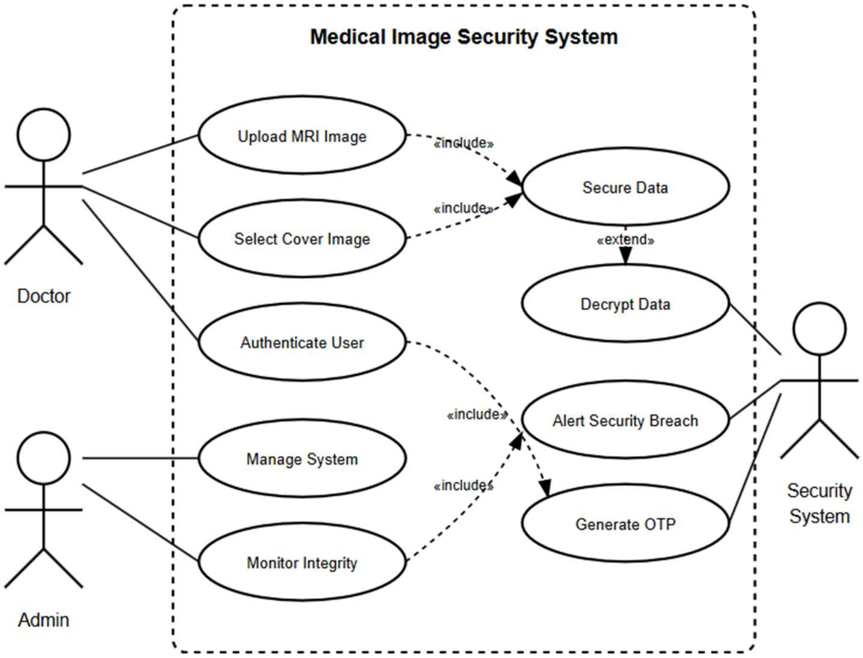


Figure 5.3: Use Case Diagram

5.5 ACTIVITY DIAGRAM

The process initiates with a secure login sequence where users – whether medical professionals or patients – must first submit their credentials, which undergo rigorous verification against encrypted database records. Upon successful authentication, the system dynamically generates a time-sensitive One-Time Password (OTP) and transmits it through a secure channel to the user's registered device, establishing a critical second factor of authentication that significantly reduces the risk of unauthorized access. With OTP validation completed, authorized users gain entry to the image upload interface where they can select MRI scans for processing.

The system then intelligently auto-selects an appropriate cover image from its medical image repository, choosing one that optimally balances concealment capacity with preservation of diagnostic quality. The core security transformation begins as the system applies Least Significant Bit (LSB) steganography to meticulously embed the MRI data within the pixel matrix of the cover image, creating a stego-image that appears visually identical to the original but contains the concealed medical information. This stego-image then undergoes a rigorous triple-layer encryption process: first with AES-128 encryption for robust data protection using symmetric cryptography, followed by ASCON's lightweight authenticated encryption to ensure data integrity with minimal computational overhead, and finally secured with Elliptic Curve Cryptography (ECC) for efficient yet powerful public-key encryption of the sensitive payload. The fully protected data package is then stored in secure, access-controlled cloud storage with redundant backups and continuous integrity checks. When legitimate access is requested, the system reverses this protection scheme – first verifying the requester's authentication status, then systematically applying the triple decryption sequence (ECC, ASCON, and AES in reverse order), before carefully extracting the hidden MRI data from the stego-image through inverse steganography algorithms. The restored original MRI is temporarily cached in a secure viewing environment with watermarking and access logging, where authorized medical personnel can review the diagnostic images while the system maintains a complete, tamper-evident audit trail of all access events.

This comprehensive activity flow demonstrates how the system seamlessly integrates multiple security technologies into a cohesive workflow that protects sensitive medical data throughout its entire lifecycle from initial upload through storage to eventual authorized access without compromising the practical usability required in fast-paced healthcare environments. The diagram effectively visualizes how each security measure builds upon the previous one to create defence-in-depth protection, ensuring that even if one layer were compromised, subsequent barriers would maintain the confidentiality and integrity of the patient's sensitive MRI data. This activity diagram Figure 5.4 outlines the secure process of MRI image handling within a medical data protection system.

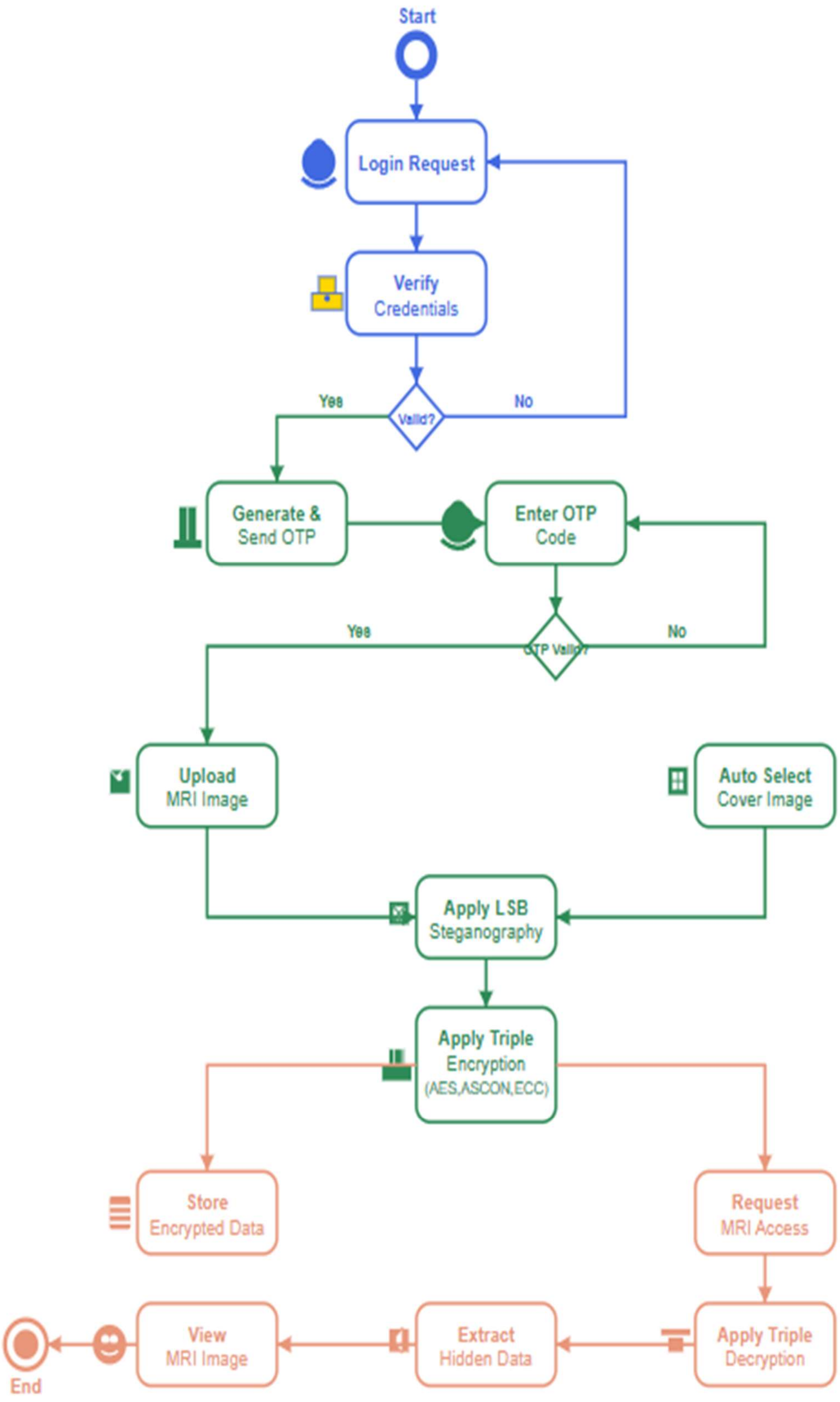


Figure 5.4: Activity Diagram

5.6 CLASS DIAGRAM

At the core, the Image Handler class serves as the system's gateway, managing the upload and retrieval of sensitive MRI images while enforcing strict access controls. These images are then processed by the Steganography class, which implements LSB (Least Significant Bit) algorithms to seamlessly embed MRI data within ordinary-looking cover images, maintaining diagnostic quality while adding a crucial layer of data concealment.

The Encryption Manager orchestrates a multi-layered security approach, coordinating three robust cryptographic protocols: AES-128 for symmetric encryption, ASCON for lightweight authenticated encryption, and ECC (Elliptic Curve Cryptography) for secure key exchange. Security verification is handled by the Authentication Module, which incorporates OTP generation and validation capabilities to ensure strong user authentication through two-factor security. The IntegrityChecker class plays a vital protective role by continuously monitoring data through cryptographic hash verification (like SHA-256), immediately triggering the Email Service to dispatch security alerts if any tampering or corruption is detected. When authorized access is required, the Decryption Pipeline systematically reverses the protection measures, first validating user credentials, then applying the appropriate decryption algorithms in sequence (ECC for key exchange, ASCON for integrity verification, and AES for data decryption), and finally extracting the original MRI from its steganographic cover.

This well-structured class architecture demonstrates how the system combines steganography with multiple encryption layers and rigorous verification processes to create a comprehensive security framework, ensuring end-to-end protection of sensitive medical imaging data while maintaining clear separation of concerns and modular extensibility for future security enhancements. Each class collaborates through precisely defined interfaces, creating a cohesive yet flexible system capable of adapting to evolving security requirements in healthcare environments. The diagram effectively visualizes how each security measure builds upon the previous one to create defence-in-depth protection, ensuring that even if one layer were compromised, subsequent barriers would maintain the confidentiality and integrity of the patient's sensitive MRI data. In Figure 5.5, a class diagram depicts a secure medical imaging system focused on protecting MRI data through steganography and encryption.

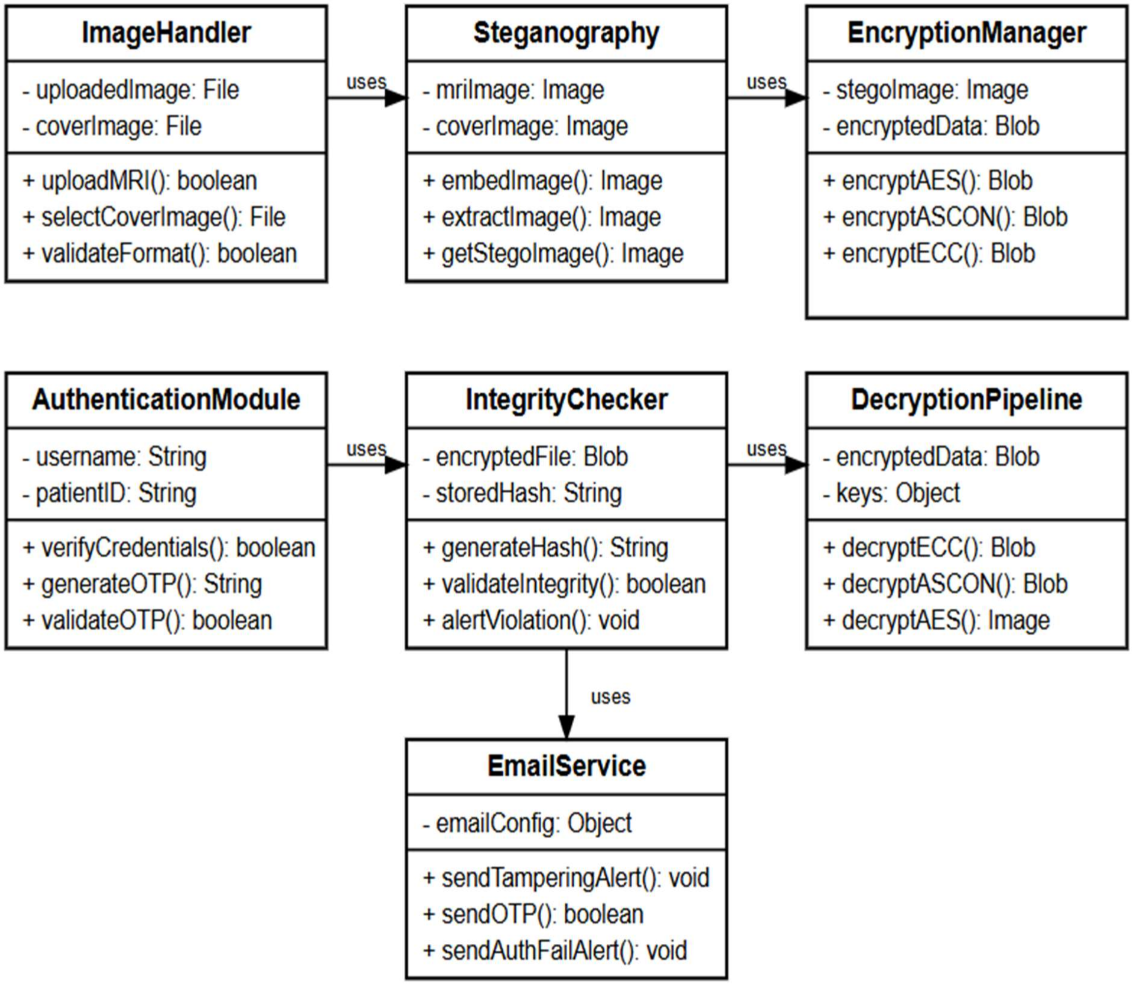


Figure 5.5: Class Diagram

CHAPTER - 6

IMPLEMENTATION

IMPLEMENTATION

6.1 CLASSIFICATION OF MODULES

- Image handler for admin & user
- Auto cover image selector & Steganography
- Triple layer of encryption
- Authenticator and Decryption
- Integrity checker & Alert system

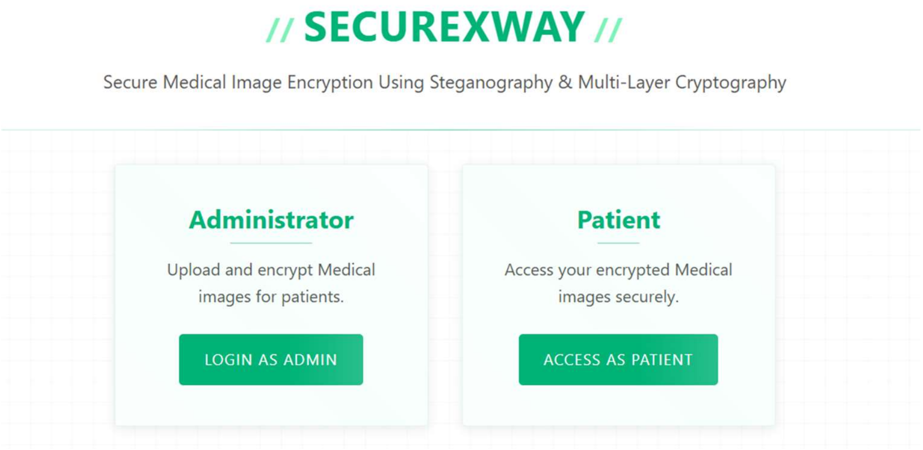
6.2 MODULE DESCRIPTION

The different modules of the system are explained in this section. Each module has its own job, such as image handling, selecting cover image, encryption with triple cryptographic layer and decryption, checking the integrity. Together, all the modules are secure and integrity protection to the files.

6.2.1 IMAGE HANDLER FOR ADMIN & USER

The first module acts as the main link between the system and the users. It separates the features for two types of users, the administrator (normally a medical professional), and the end user (normally the patient). This module ensures that, only authorized personnel have access to encryption and decryption processes for sensitive medical images. A secure and user-friendly interface provides an entry point to upload and retrieve medical data (especially MRI images). The authentication mechanism in the admin panel requires a working username and password. After logging in, the administrator can upload MRI images via a simple file selection process. The uploaded image's format is checked and, with the image handler, is ready for the encryption and steganography pipeline. Home page for the Administrator and user is shown. Interface for Admin & User Also, to track and securely retrieve the encrypted data, the administrator must also create a unique Patient Identification Number (PID). The interface can provide a more secure but limited use access point from the user's perspective, because patients will be required to enter a PID and a One-Time Password (OTP) generated by the system to verify their identity. In doing so, it ensures that the sensitive decrypted medical data can only be accessed by those authorized to do so. Adding OTP provides another layer of security and protects the system from brute force or unauthorized access attempts. Also, the module has to deal with image and metadata storage. Once an image is uploaded, it is temporarily saved in store before it is sent to encryption or the steganography modules. Likewise, the PID and related data is associated in a backend database as a secure record for possible future recovery and to track complete identity in the event of a system failure, or for future audits. In addition, the image handler will ensure that there is not an unencrypted image permanently stored, which will lessen the chances of data alteration or unintentional data leakages.

The Admin Login page, that requires the admin to enter valid credentials (username and password) as a descriptor to continue. Admin Login Page In addition, this module's user interface design is uniquely suited to medical environments, especially in terms of readability, usability, and availability for training. The interface guarantees speed of responses and minimal clicks for every function since medical staff usually have no time to waste. All actions are accompanied by feedback messages and status messages that guide users throughout the entire process of uploading or retrieving images. The module establishes the basis for image management and security enforcement in the context of this system; it is the main focal point for secure operation. On the user side, this point limits access to decrypted data to only authorized and verified users. The system also guarantees that the users find and identify the right image, and to tag and submit this record for potential further secure processing. The Image Handler module is paramount to ensuring the protection and confidentiality of medical imaging data because this module ensures that procedures for upload, identifying information, and retrieval are secure and efficient. Figure 6.1 shows the flow where the admin uploads the MRI image, which is temporarily stored before being handed off to the encryption module for processing.


// SECUREXWAY //

Secure Medical Image Encryption Using Steganography & Multi-Layer Cryptography

Administrator

Upload and encrypt Medical images for patients.

Patient

Access your encrypted Medical images securely.

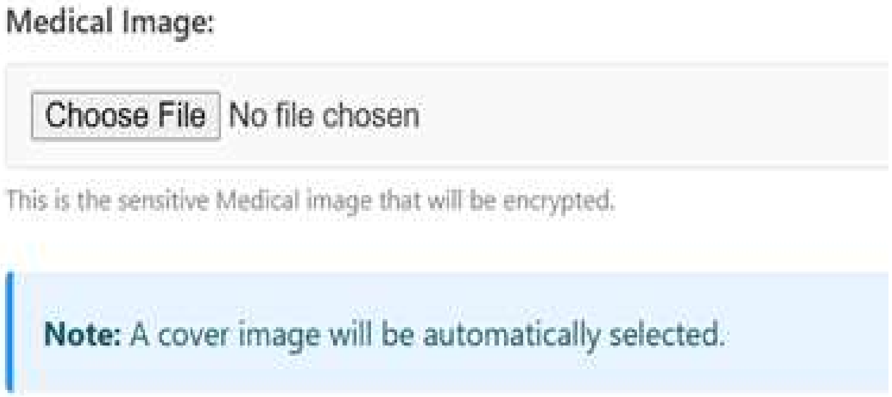
Figure 6.1: Image Handling for admin & user

In addition to upload and retrieval, this module handles directory management by organizing files in structured folders ensuring that no overlap or corruption occurs. The Flask framework handles routing logic such as redirections and file response handling, which allows authenticated users to receive secure downloads. Admin privileges are reinforced through conditional access rendered on the frontend, and user sessions are tracked for auditing. This ensures that every interaction with the sensitive MRI image is logged and secured, preventing unauthorized tampering or file leaks. This setup ultimately ensures high availability and integrity for all image interactions in the framework.

6.2.2 AUTO COVER IMAGE SELECTOR & STEGANOGRAPHY

The second module of the system deals with selecting the Image Cover and then using Least Significant Bit (LSB) steganography to insert the encrypted MRI image into the Image Cover. This step is very important because it adds another layer of obscurity and makes it more difficult for hackers to realize that they are transmitting or storing any private information. The method of LSB steganography hides the presence of the encrypted medical images and protects the images while they are being stored or transmitted by hiding the data within the pixels of an image. The order of actions during this step begins with the admin selecting a folder of standard images, sometimes referred to as cover images. The standard images are ordinary images that are shared or stored without raising suspicion. A picture in the folder will be randomly selected and used as the carrier for the encrypted data. The Upload Medical Image interface that the administrator interface uses. The random element to the selection process allows for unknowns and enhances the overall system security.

Once the cover image has been selected, the triple layer encryption process provides an encrypted MRI image ready for the embedding process. The idea behind LSB steganography is to replace the bits from the encrypted image for the least significant value of the pixel values in the cover image. By changing the least significant bits, there is negligible effect to the image as the least effective in defining the pixel colour. The result is a stego image that will have the same properties as the original cover image while hiding private medical information. The end terminal output following the steganography operation. In summary, it is possible to securely and covertly store encrypted medical images using a simple, yet powerful LSB steganography process included in this module. By using realistic looking cover photos to hide encrypted medical images, attackers have a hard time being able to identify the intention of the owner of the data. This module is optimal for privacy-related applications due to its bit-level embedding, random photo selection, and optional hashing validation features, particularly in healthcare use cases, where privacy of data is important. The Figure 6.2 shows how a chosen cover image is, and the LSB of each byte is modified to embed bits of the encrypted data, forming the final stego-image stored in a secure folder.



Medical Image:

Choose File No file chosen

This is the sensitive Medical image that will be encrypted.

Note: A cover image will be automatically selected.

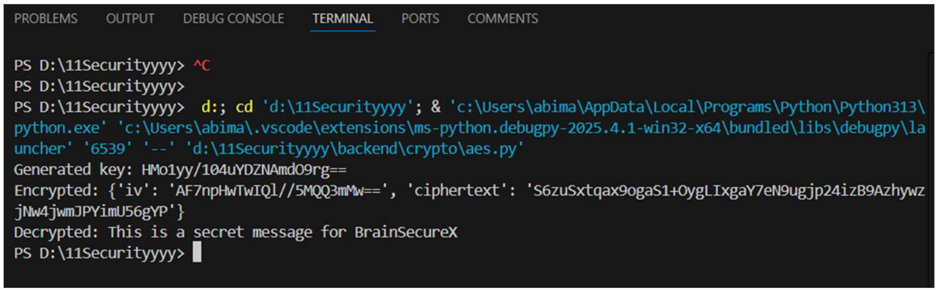
Figure 6.2: Auto Cover image selection

This module uses image processing libraries like PIL (Python Imaging Library) to manipulate pixels directly. The cover image and encrypted MRI data are both converted into binary representations, where the embedding process systematically replaces the least significant bit of each cover pixel with one bit of the encrypted image data. Once completed, the resulting stego image is saved, retaining visual integrity. This ensures plausible deniability while transmitting or storing sensitive patient data. This covert technique provides a significant advantage in highly surveyed or constrained environments where encryption alone might raise suspicion. The process remains fully reversible only by authorized personnel with the correct decryption and extraction mechanisms.

6.2.3 TRIPLE LAYER OF ENCRYPTION

The encryption module comprises three cryptographic layers that provide confidentiality, integrity, and robust key protection for the MRI images. First, the AES-128 algorithm encrypts the raw image data, offering rapid and secure block-based encryption. Second, the output of AES is passed through the lightweight ASCON cipher, enhancing security with minimal performance cost especially relevant for low-resource medical devices or networks. Finally, the AES and ASCON encryption keys themselves are encrypted using a custom Elliptic Curve Cryptography (ECC) implementation built on the curve.

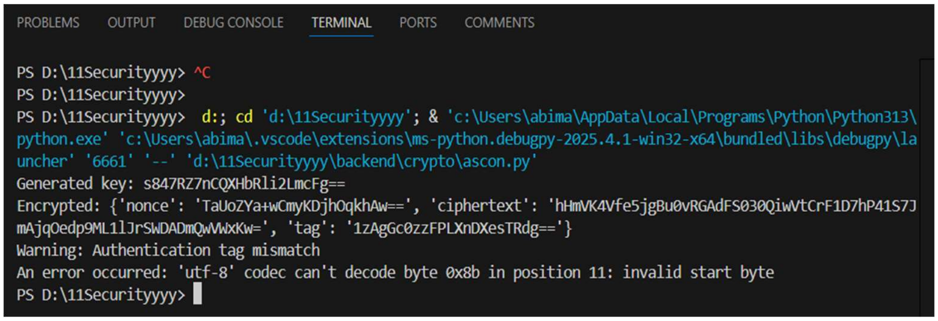
The Advanced Encryption Standard (AES-128) algorithm is a kind of symmetric block cipher that's fast and secure enough. AES then starts the encryption using a special key to encrypt the raw MRI image data. Finally, the raw image data is transformed to ciphertext and is unreadable at this stage, ensuring that no one except an authorized person will read the original image. AES-128 is appropriate in this case because it gives a reasonable balance between strong encryption and computer processing time. The Figure 6.3 uses the AES-128 to perform encryption.



```
PS D:\11Securityyyy> ^C
PS D:\11Securityyyy>
PS D:\11Securityyyy>  d:; cd 'd:\11Securityyyy'; & 'c:\Users\abima\AppData\Local\Programs\Python\Python313\
python.exe' 'c:\Users\abima\.vscode\extensions\ms-python.debugpy-2025.4.1-win32-x64\bundled\libs\debugpy\la
uncher' '6539' '--' 'd:\11Securityyyy\backend\crypto\aes.py'
Generated key: HMo1yy/104uYDZNAmdO9rg==
Encrypted: {'iv': 'AF7npHwTwIQl//5MQQ3mMw==', 'ciphertext': 'S6zuSxtqax9ogaS1+OygLIxgaY7eN9ugjp24izB9Azhywz
jNw4jwmJPYimU56gYP'}
Decrypted: This is a secret message for BrainSecureX
PS D:\11Securityyyy> █
```

Figure 6.3: AES protocol execution

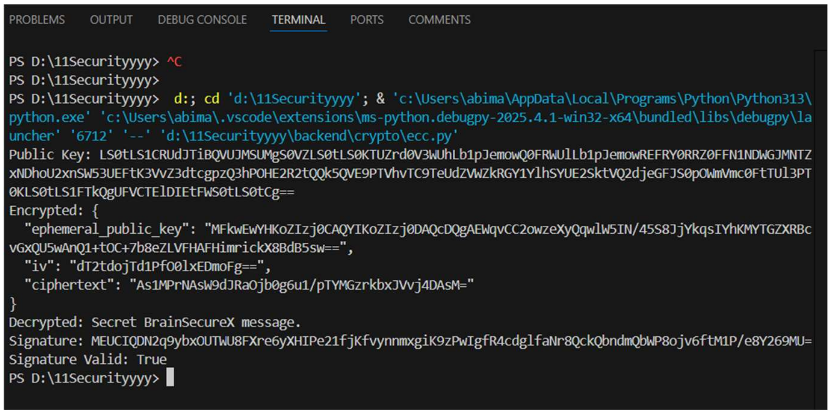
In short, the AES output was then fed into ASCON, an authenticated encryption algorithm that is also very efficient with resources and more resistant to side-channel attacks than other lightweight, authenticated encryption schemes. In using an authenticated encryption scheme like ASCON, there is an added advantage in guaranteeing the authenticity of the data in addition to ensuring the confidentiality of the original ciphered data. When decrypting data with ASCON, any unauthorized alterations to the ciphertext will be flagged right away and not let you have the data. Figure 6.4 shows the ASCON encryption.



```
PS D:\11Securityyyy> ^C
PS D:\11Securityyyy>
PS D:\11Securityyyy>  d:; cd 'd:\11Securityyyy'; & 'c:\Users\abima\AppData\Local\Programs\Python\Python313\
python.exe' 'c:\Users\abima\.vscode\extensions\ms-python.debugpy-2025.4.1-win32-x64\bundled\libs\debugpy\la
uncher' '6661' '--' 'd:\11Securityyyy\backend\crypto\ascon.py'
Generated key: s847RZ7nCQXHbRli2LmcFg==
Encrypted: {'nonce': 'TaUoZYa+wCmyKDjhOqkhAw==', 'ciphertext': 'hHmVK4Vfe5jgBu0vRGAdFS030QiwVtCrF1D7hP41S7J
mAjqOedp9ML1lJrSWDADmQwVWxKw=', 'tag': '1zAgGc0zzFPLXnDXesTRdg=='}
Warning: Authentication tag mismatch
An error occurred: 'utf-8' codec can't decode byte 0x8b in position 11: invalid start byte
PS D:\11Securityyyy> █
```

Figure 6.4: ASCON encryption

This module last layer, ECC, will not be encrypting the image; it will be using the encryption keys of the AES and ASCON procedures. ECC is a public-key cryptography method that provides secure key management and distribution. Only the intended receiver of the AES and ASCON encrypted keys can decrypt them using their private key against a public key which has been created based on the mathematics of an elliptic curve. ECC provides strong security through smaller key sizes while requiring less memory footprint and processing overhead. The Figure 6.5 performs the ECC encryption.



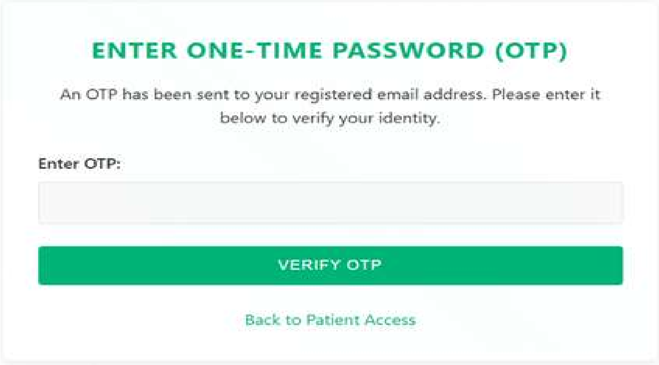
```
PS D:\11Securityyyy> ^C
PS D:\11Securityyyy>
PS D:\11Securityyyy>  d:; cd 'd:\11Securityyyy'; & 'c:\Users\abima\AppData\Local\Programs\Python\Python313\
python.exe' 'c:\Users\abima\.vscode\extensions\ms-python.debugpy-2025.4.1-win32-x64\bundled\libs\debugpy\la
uncher' '6712' '--' 'd:\11Securityyyy\backend\crypto\ecc.py'
Public Key: LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUZrd0V3WUhLb1pJemowQ0FRWUlLb1pJemowREFRY0RRZ0FFN1NDWGJMNTZ
xNDhoU2xnSW53UEFtK3VvZ3dtcgpzQ3hPOHE2R2tQQk5QVE9PTVhvTC9TeUdZVWZkRGY1YlhSYUE2SktVQ2djeGFJS0pOWmVmc0FtTUl3PT
0KLS0tLS1FTkQgUFVCTElDIEtFWS0tLS0tCg==
Encrypted: {
  "ephemeral_public_key": "MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEWqvCC2owzeXyQqwlW5IN/45S8JjYkqsIYhKMYTGZXRBc
vGxQU5wAnQ1+tOC+7b8eZLVFHAFHimrickX8BdB5sw==",
  "iv": "dT2tdojTd1PfO0lxEDmoFg==",
  "ciphertext": "As1MPrNAsW9dJRaOjb0g6u1/pTYMGzrkbxJVvj4DAsM="
}
Decrypted: Secret BrainSecureX message.
Signature: MEUCIQDN2q9ybxOUTWU8FXre6yXHIPe21fjKfvynnmxgiK9zPwIgfR4cdglfaNr8QckQbndmQbWP8ojv6ftM1P/e8Y269MU=
Signature Valid: True
PS D:\11Securityyyy> █
```

Figure 6.5: ECC encryption

The three layers of encryption create a solid wall of protection from unwanted access. The architecture of the triple-layered security in such a way that even if one layer is compromised in some form, the data is still protected. The sequence of encryption allows for modular encryption where each component can be updated or swapped based on security needs in the future. A triple-layered encryption model ensures security, privacy, confidentiality and non-repudiation that all medical data management requires. That means that the system can safely send and store a private MRI without the risk of interception or being altered. The three layers of encryption create a solid wall of protection from unwanted access. The architecture of the triple-layered security in such a way that even if one layer is compromised in some form, the data is still protected. The sequence of encryption allows for modular encryption where each component can be updated or swapped based on security needs in the future. A triple layered encryption model ensures security, privacy, confidentiality and non-repudiation that all medical data management requires. That means that the system can safely send and store a private MRI without the risk of interception or being altered.

6.2.4 AUTHENTICATOR AND DECRYPTION

Only valid users can pull or access sensitive health data because of the system's Authenticator and Decryption module, which is the last and the most important module. Medical images like MRI scans are private and critical for diagnosing patient's problems. For this reason, it is important to ensure that valid users have access to that verified data, while the integrity and confidentiality of that data is kept intact. To go back to the original medical image, this module includes secure decryption mechanisms and user authentication mechanisms that are versatile. Figure 6.6 demonstrates the interface for OTP authentication.



ENTER ONE-TIME PASSWORD (OTP)

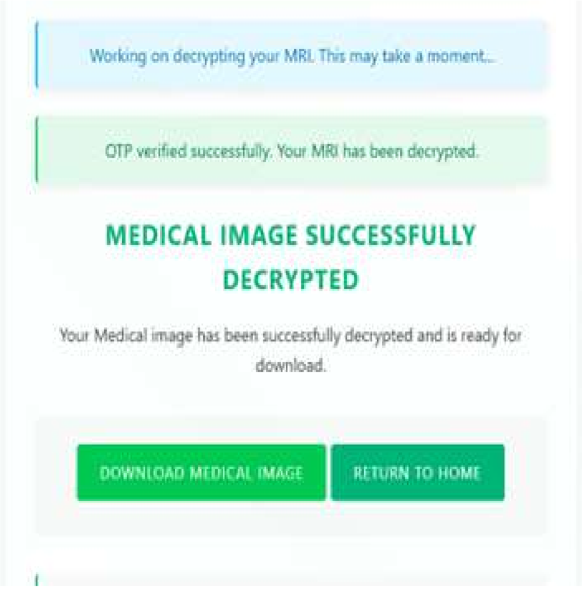
An OTP has been sent to your registered email address. Please enter it below to verify your identity.

Enter OTP:

Figure 6.6: OTP authentication

Whenever a user a doctor, patient, or hospital staff member wants to get a view of the encrypted medical image, this module would be triggered. The user authentication is the first step of this module, requiring the user to input a username and password that are provided by the hospitals secure record management system. This helps ensure that only registered users and authorized users can move past this step. After verifying their credentials, the system goes to a secondary identification process, where the user enters a unique patient identification number and a one-time password, or OTP, to be sent to the registered email or mobile device. Using this type of dual-layered verification process helps the potential of impersonation and unauthorized access.

After authentication, the system then obtains the encrypted stego-image during the decryption phase of its operations. The decryption process proceeds in precisely reverse order to the encryption layers. The system first decrypts the keys used to execute AES and ASCON encryption with elliptic curve cryptography or ECC. ECC is a more secure form of key management, and offers less computational overhead, which is particularly important given the nature of a medical IoT system. The Figure 6.7 shows the decryption process of the medical image.


Working on decrypting your MRI. This may take a moment...

OTP verified successfully. Your MRI has been decrypted.

MEDICAL IMAGE SUCCESSFULLY DECRYPTED

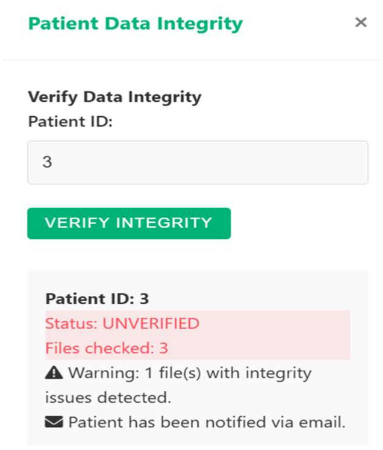
Your Medical image has been successfully decrypted and is ready for download.

Figure 6.7: Image decryption

Next, we move on to ASCON decryption, a lightweight cipher that provides encryption and authentication, after deleting the elliptic curve cryptography (ECC) keys. The data that was encrypted originally in the second layer using ASCON, is decrypted during the process of encryption. After we disabled the ASCON cipher, the output was given to the last decryption layer, which implemented AES-128. The low-level encryption algorithm AES, or Advanced Encryption Standard, is a trustworthy and reliable symmetric encryption algorithm that removes any remaining encryption and retrieves the original pixel values for the medical image.

6.2.5 INTEGRITY CHECKER & ALERT SYSTEM

The Integrity Checker and Alert System, the project's fifth module, is fundamental for maintaining the integrity of the entire security system. In any system handling extremely sensitive information, especially medical records like MRI images, it must be ensured that not only is data encrypted and concealed, but that it can also be regularly verified that it has remained unaltered. To maintain awareness in real-time, and to ensure that data is not misused, this module has been created to monitor file integrity and subsequently notify the end-user of any unauthorized changes or file corruption. The data integrity activity, which is performed in the module using cryptographic hash functions, is the main programmatic basis of this module. The Figure 6.8 shows the interface to check data integrity.



Patient Data Integrity ×

Verify Data Integrity

Patient ID:

3

VERIFY INTEGRITY

Patient ID: 3

Status: UNVERIFIED

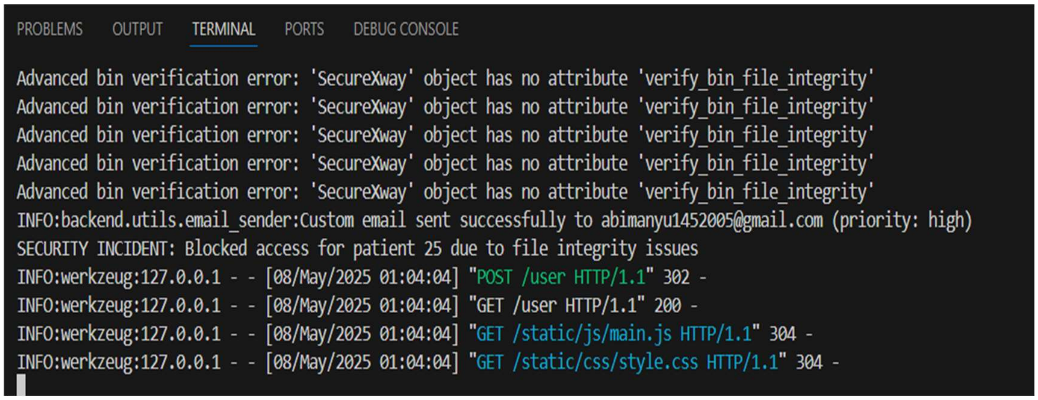
Files checked: 3

⚠ Warning: 1 file(s) with integrity issues detected.

✉ Patient has been notified via email.

Figure 6.8: Integrity Checker

Initially, when the MRI image is encrypted so that it is then 'hidden' into a cover image (stego image), a unique hash value (for example SHA-256 or some other digital signature) is generated for the encrypted file. This hash will serve as the digital fingerprint of the file; any change in the digital file, even a change of a single bit, will create a different hash value. This original (cached) hash is protected, either in a secure database somewhere, or in another log file. The file is confirmed as original and has not been tampered with when both values are the same. If there is a difference between the values, it indicates the file has been changed in some way either it has been illegally accessed or is corrupt, or was possibly subject to a cyberattack. To simple avoid further risk in this case, the system immediately stops decryption or access process. This gives the affected or concerned stakeholder an early notice to react as necessary, such as to investigate the incident, take mitigation action like restore secure stored backups, look at the audit logs, or turn off the affected systems, potentially saving time and money. In addition to an alert, the module can also be configured to execute automated responses; including, creating audit trails for the system administrator to review, temporarily restricting access to any affected user account and creating system logs. The Figure 6.9 shows the alert generation mechanism where it sends to the corresponding patient id email id.



```
Advanced bin verification error: 'SecureXway' object has no attribute 'verify_bin_file_integrity'
Advanced bin verification error: 'SecureXway' object has no attribute 'verify_bin_file_integrity'
Advanced bin verification error: 'SecureXway' object has no attribute 'verify_bin_file_integrity'
Advanced bin verification error: 'SecureXway' object has no attribute 'verify_bin_file_integrity'
Advanced bin verification error: 'SecureXway' object has no attribute 'verify_bin_file_integrity'
INFO:backend.utils.email_sender:Custom email sent successfully to abimanyu1452005@gmail.com (priority: high)
SECURITY INCIDENT: Blocked access for patient 25 due to file integrity issues
INFO:werkzeug:127.0.0.1 - - [08/May/2025 01:04:04] "POST /user HTTP/1.1" 302 -
INFO:werkzeug:127.0.0.1 - - [08/May/2025 01:04:04] "GET /user HTTP/1.1" 200 -
INFO:werkzeug:127.0.0.1 - - [08/May/2025 01:04:04] "GET /static/js/main.js HTTP/1.1" 304 -
INFO:werkzeug:127.0.0.1 - - [08/May/2025 01:04:04] "GET /static/css/style.css HTTP/1.1" 304 -
```

Figure 6.9: Alert mail generation to patient

This module is don’t just give you alerts when certain events happen. The system is connected into the integrity verification subsystem, and it sends alerts automatically. When any file tampering event (file access) is detected, an alert email is automatically created and sent to the authorized user who is impacted, this could be the patients(s), system administrator or doctor. It contains the file name, file access time, the suspected modification, and warning message in the email notification. This gives the affected or concerned stakeholder an early notice to react as necessary, such as to investigate the incident, take mitigation action like restore secure stored backups, look at the audit logs, or turn off the affected systems, potentially saving time and money. In addition to an alert, the module can also be configured to execute automated responses; including, creating audit trails for the system administrator to review, temporarily restricting access to any affected user account, and/or creating system logs. The alerts system can facilitate tracking the amount and content of various attacks and can assist with improving security protocols and policy over time. The module will provide accountability of the system and provide transparency to enable compliance in addition to improving data security.

Users can know their medical information is being monitored and will receive real-time alerts if anything is out of place. What is more, integrity verification is done securely and with low overhead through the application of a cryptographic hash. In short, the Integrity Checker and Alert System is an important first and last line of defence for the project. The medical data protection framework is made significantly more robust and is thus quite reliable for real-world healthcare use cases by being able to verify the legitimacy of encrypted files stored and notifying authorized users quickly when tampering is detected.

CHAPTER - 7

RESULT AND DISCUSSION

7. RESULT AND DISCUSSION

7.1 RESULT

A dataset of high-resolution MRI images protected by triple-layer encryption (AES-128, ASCON, and ECC) and embedded within cover images using LSB-based steganography was used to thoroughly test the system. Execution time, authentication robustness, image quality preservation, data recovery accuracy, and encryption dependability were the main areas of evaluation. All embedded images were safely encrypted in every test case thanks to the encryption process 100% success rate. The original MRI images were recovered with no data loss upon decryption, preserving their integrity for use in medicine. The concealed data was invisible to the human eye thanks to the LSB-based steganography, which made sure the cover image didn't change noticeably. For high-resolution images, the system's encryption and decryption times varied from 1.5 to 3 seconds, which is crucial for real-time performance in clinical settings. By successfully preventing unwanted access, the OTP-based authentication method protected the data from possible breaches. With only a minor increase in file size brought on by encryption and stego-embedding, the system showed very little storage overhead, guaranteeing that storage resources are optimized. Furthermore, data security during network sharing was guaranteed by secure file transmission using SSL/TLS protocols. Because it supported batch processing, which is essential for managing the massive datasets that are frequently encountered in healthcare settings, and integrated seamlessly with the hospital's current management systems, the system's scalability was tested and validated. Because it could handle multiple images at once without experiencing performance degradation, the solution turned out to be both practical and effective. The system offers a robust defense against unauthorized access, guarantees compliance with data protection regulations, and protects sensitive medical data without sacrificing usability. For hospitals and other healthcare organizations looking to protect patient data while preserving operational effectiveness, this makes it the perfect choice. Additionally, the system supports multi-platform compatibility, enabling integration with both cloud and on-premises infrastructures, providing hospitals with flexibility in deployment options. The use of cloud-based storage also facilitates easier access and management of large volumes of medical data, ensuring that healthcare providers can retrieve necessary information quickly and efficiently in emergencies. Finally, regular system updates and vulnerability assessments are incorporated into the platform to ensure continuous improvement in security measures, keeping pace with evolving cyber threats.

7.2 DISCUSSION

The system's performance shows how well it can protect private medical images using a hybrid strategy that blends innovative cryptography and steganography. Strong data confidentiality and multi-level protection are ensured using a triple-layer encryption model, which combines AES-128, ASCON, and ECC. The remaining encryption layers serve as strong defences against unwanted access, even in situations where one layer may be compromised. Moreover, the system's capacity to preserve secrecy and stealth at the same time was improved by the remarkable success of LSB (Least Significant Bit) steganography in embedding encrypted medical image data into cover images without resulting in any discernible visual degradation. The encryption and decryption procedures' dependability were confirmed by extensive testing, which produced results that showed 100% successful image recovery and no data loss. The system can handle high-resolution images without causing noticeable delays, as evidenced by the average processing time staying within acceptable bounds. In every test case, the OTP-based authentication method effectively prevented unwanted access by adding an extra layer of access control. In terms of user experience, medical staff who may not be technically inclined can interact with the system with ease thanks to its web-based interface. Even though the current implementation works well in controlled environments, there are still some issues that present chances for future development. Despite being straightforward and effective, the LSB-based steganographic method may be susceptible to advanced steganalysis techniques, which are intended to uncover hidden information in images. To increase resistance to detection, future versions of the system might investigate transform-domain or adaptive steganography (like DCT or DWT-based techniques). ECC encryption tends to be computationally demanding, especially on devices with limited resources, even though it offers high security with smaller key sizes. Performance optimization or the use of hardware accelerators like GPUs or cryptographic modules could be used to address this. Currently, the OTP system relies on email delivery, which may experience deliverability or latency problems in real-time situations. In real-world implementations, integrating two-factor authentication (2FA) techniques via SMS or apps could greatly improve the system's responsiveness and dependability. Incorporating user role-based access control, thorough logging for audit trails, and real-time monitoring can also improve the platform's adherence to data protection laws like GDPR and HIPAA. To sum up, the suggested system proves to be a very safe, scalable, and technically sound platform made especially to protect encrypted medical images in contemporary digital healthcare settings.

CHAPTER - 8

CONCLUSION AND FUTUREWORK

8. CONCLUSION AND FUTURE WORK

8.1 CONCLUSION

By combining LSB steganography with triple-layer encryption (AES-128, ASCON, ECC), the solution effectively illustrates a safe and multi-layered method of safeguarding private medical images. Using successive encryption techniques and the embedding of MRI images within cover images, the system guarantees data confidentiality, integrity, and resistance to unauthorized access. While the use of robust encryption algorithms at multiple layers makes it extremely resistant to cyber threats, the technique of concealing medical content within everyday images prevents visual detection. User authentication and OTP-based verification are features of the system that further secure access by establishing an efficient access control mechanism that guarantees that only verified users can access or interact with the protected data. In the healthcare industry, where patient privacy and data protection are crucial, this degree of security is necessary.

8.2 FUTURE WORK

The system can be significantly enhanced by incorporating more advanced steganographic techniques. These methods offer greater robustness against detection compared to the current Least Significant Bit (LSB) method, which may be vulnerable to certain attacks. Adaptive steganography adjusts the embedding process based on the image content, making it more difficult for unauthorized parties to detect alterations. Another critical area for improvement is real-time image processing. As the system grows in scale, especially in medical environments dealing with large volumes of medical images, real-time encryption and decryption would become crucial. Implementing real-time capabilities would allow the system to process medical images dynamically without causing significant delays, ensuring that healthcare providers can access and share encrypted images swiftly. This would be especially beneficial in high-demand scenarios like telemedicine, emergency services, and large-scale imaging platforms where timely access to accurate data is essential. Integrating machine learning models into the system could further enhance its security by enabling the automatic detection of tampering attempts or abnormal patterns in image processing. Machine learning algorithms could be trained to identify potential vulnerabilities in encrypted images and optimize encryption paths based on predictive threat analysis.

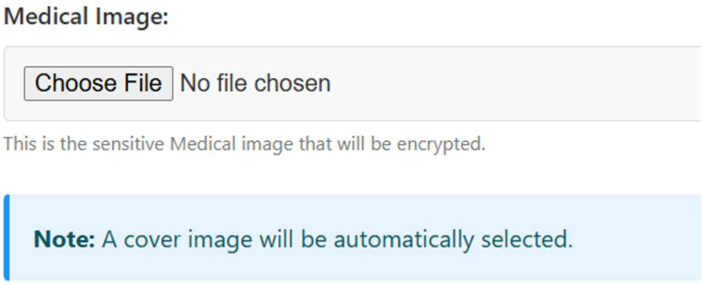
CHAPTER 9

APPENDIX - I

9. APPENDIX – I

9.1 OUTPUT

The graphical user interface of the Secure File System as it is observed during file upload. The Figure 9.1 shows a file selection dialog is shown to choose file to be monitored and secured. After selecting the file once, and then safely stored.



Medical Image:

Choose File No file chosen

This is the sensitive Medical image that will be encrypted.

Note: A cover image will be automatically selected.

Figure 9.1: Uploading file

The architecture of the triple-layered security in such a way that even if one layer is compromised in some form, the data is still protected. The sequence of encryption allows for modular encryption where each component can be updated or swapped based on security needs in the future. The Figure 9.2 performs the three layers of encryption create a solid wall of protection from unwanted access.

encrypted > 10_20250325035726.bin

```
{"nonce": "x++osi7aigsdauBhUQPtKg==", "ciphertext": "IQ05nkhK1tZ/uYANQHfpz6H9E6S/f/
A4EAw1Um8VWwkATVat2yGc6dbS+ztJ++IHIpBLCdB0VvjH4pB1lz3DEMTeZvxx3AAq/+dfAWZ4kSGds6W774/
664TXyl5ytx8hhC2tnKTdNV5pRFCSGZhB/HEV4WkMNUl14VZ13us9Ex4JV33gVYDobU+GdRcnwjg
+HoifdmsZfncauv8fMbXVNbXIDLJKyY+QiJBkdEGFG4AOr5mt1tq3JR6M4CAj+tFMdveRr1ba4MX2RRvxc42mc
+hftG6OWdCaFfTjcE1shWT8ORAm4tYmJQC4cGIwhjXnjuBHmh003NpJ+J/fgLaPmXCCVU6n+/tt7lxmYfS5dFfG/
IUAT2qgOYQyXtgXIZz53uUBXH5YWqzsbhcbOhPkARnBdbMrK/
3WGqPjZOsrCeMk51N2GciRYqH9FQxxQIBRqgyvLOh74DnNEGPr9QmYQTyAcdL2Tdr4wY4dO0/
a5tFNW8Qq1zUkEimeSTq787JXb2P6OsE0Be07hCPBqM4eUoh77Jxor+vovf/vir
+gd7mYjzY4oEt7v6RClq5KNNgsobjbnudFmXAIgkC/RW4V1SdT91Wy5pl1WZIUIATEL+B10xj0zH64U/
r7RBqNK6upmom665hg6CqgTnQlRYBtKW9Nrsj49OvcCm4qpV2IyadU93UmYPxMlqXHlhnst8YIuDdWj6GutmXcq0a8uWISie0I
vpzh+1WTrh2HF1Dl5lI9KQmSMNSgUAmAC47cThY265ACODR4SaIYdRle4hc2axA2XIQREQxxS9VQ3KkYNaKf3X8zmTeODg/
eGjpxmt7tuXuO14kUx3K7N6IdnkvhZFf2EYNtJ0qST3/S5QYtjDP2x8Pg5fAJYshL
+vsmdVcCIWXEaZ6WFzhMZX161L2hYHDMouunvZD7eOa0jPg3XBwzrG2eT1a2wiwIts40aMaksnDbbzSm69VJN2H6JQ3kLszaad
P/zSs9XqxJq8m3jQ9j7XSoSliMIxiSrdIYVj1VZfxsPJh9gssvtUU5y6NA/
aC7sxDvbeD6CiBG2fLef3xxCSjXWSSsnuxKSMrByeJ4DNOo54akRcS7kxkivii7vChECyLDwWcdAEJFv4ND
+qR2BpLfO4w0ltyXno53hT8aNqYWpjdq79lq4e8uGj2Th5lqg/KeP2rS7EaaD6QGWZEAZXfQ32XzrpUNViSnl/AggtgJudXI/
OTTWaDzYKyRAmNRD86fpWGEYrvWd5XCbR7vExCc/ByXIRwaNRndr0+kodSfjfsBx59HAT
+OQ1LOzGGsd3Hr0dQKUzNqvWoyRqrEzJNMakMtRJSlCOoGiPSEzNfDNoZ0hnFsAFhGA0hbjaR7jBDAuIee7b4VRFM5bL6omZNl
J3wtCSTDwzkMOQ9pwAb4QImoO2en7nh2lNMIJ/eeaJ5Dipb91N2GDH7w4l0G2wcFiP+zd+E1/ioMwP8HH
+fUvrW9SAQSp0QEV1oWnjj35IRzWFsE3vqPWTvLixyy9TPNvwzQgwThf1EW+qzC0t+KeGjTSXkeTt2NjMd4AJQRg
+ACeVU7Svv9qPq+oLUc6ggdBzw1gXg6Mzd3mfZuWv5wYzLM2S3X7GH0uRFSEVbYXG3mhQHHK/9y2f4vAA
+L6Ry9YEwl23H18EunoDUL2eiDBoAgoDE2Oz1mS5m0rERbav/
mjcJ7WrLP4pvSruEpyvgiewbUkan4jCeCL0TUvw1DfNBSX9dHi+Yg5jpgxv4bRinN08VkWgIolx7JkR28F/f/
sjWpYnlyv5BFC0/l2ypEN89xtJGbvqRapYmuFG9wUPLSYLc/
mYEq9GCQt6PKdbihV5Jj2Vz55jZoDenmTZFsUfA66kvSDXSsICLEDqhiSk/HqheIrJtF3cZzTKPIzvJYHOzRlY93pf8k+eax/
3N+yMxogK+JKFfBKWGeyA5sbkTAJzqy0Z8qHQAKqsGdOFw4fXBNAd1mvCzoFS8GTmgnaC2Ceav5Yaqvwws9Jg
+dJyqtxZFXdqedlVmRMLUU4AG5pSdDWFcicWTldUqPbBL5EmalyCbPrI419gB4B0kONjkL52GO
+JARk3GGMqxgXAVeL3x6h5HxiBUwqI62wyf9cNynNhu2Bk49xuD1xwl/
ZSDGhRyHfzVGJ4NQkmcnUOyQ9ZtGMBNH5r56Y9iobr90bNb5S1G/
```

Figure 9.2: Output in ciphertext

The steganography and triple layer encryption is successfully retrieved by the user by passing the authentication mechanisms and the decrypted image as downloaded when we click the download button in the interface. The Figure 9.3 provides the output that the file that we are encrypted using such techniques.

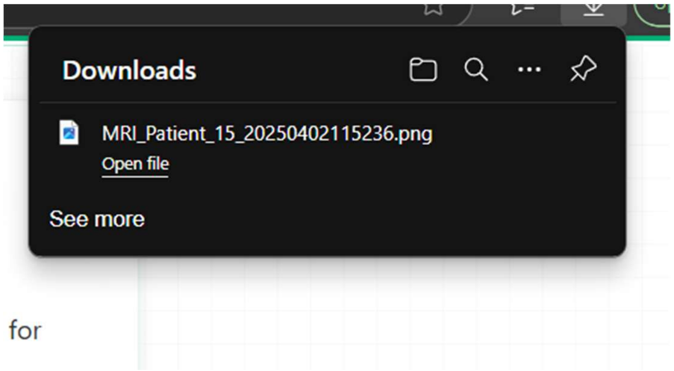
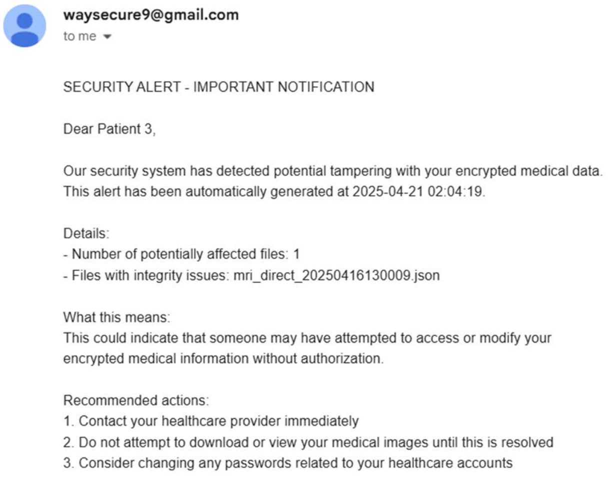


Figure 9.3: Decrypted Image download

If any malicious functions happen in our system or any attacker attempt to tamper our encrypted file in the cloud database this enables the user to prevent from the unauthorized access and malicious modification of our encrypted file, The Figure 9.4 gives the alert system output that will be sent to the user.



waysecure9@gmail.com
to me

SECURITY ALERT - IMPORTANT NOTIFICATION

Dear Patient 3,

Our security system has detected potential tampering with your encrypted medical data.
This alert has been automatically generated at 2025-04-21 02:04:19.

Details:
- Number of potentially affected files: 1
- Files with integrity issues: mri_direct_20250416130009.json

What this means:
This could indicate that someone may have attempted to access or modify your encrypted medical information without authorization.

Recommended actions:
1. Contact your healthcare provider immediately
2. Do not attempt to download or view your medical images until this is resolved
3. Consider changing any passwords related to your healthcare accounts

Figure 9.4: Generation of Alert mail

APPENDIX - II

9. APPENDIX – II

9.2 SAMPLE CODE

9.2.1 INTEGRITY VERIFICATION

```
import os
import sys
import hashlib
import argparse
import difflib
from datetime import datetime

def compare_files(original_file, decrypted_file, report_file=None):
    if not os.path.exists(original_file):
        print(f"Error: Original file not found: {original_file}")
        return False

    if not os.path.exists(decrypted_file):
        print(f"Error: Decrypted file not found: {decrypted_file}")
        return False

    orig_size = os.path.getsize(original_file)
    decr_size = os.path.getsize(decrypted_file)

    if orig_size != decr_size:
        print(f" Size mismatch: Original={orig_size} bytes, Decrypted={decr_size} bytes")
        size_match = False
    else:
        print(f" Size match: Both files are {orig_size} bytes")
        size_match = True

    with open(original_file, 'rb') as f:
        orig_hash = hashlib.md5(f.read()).hexdigest()

    with open(decrypted_file, 'rb') as f:
        decr_hash = hashlib.md5(f.read()).hexdigest()
    if orig_hash != decr_hash:
        print(f" Hash mismatch: Original={orig_hash}, Decrypted={decr_hash}")
        hash_match = False
    else:
        print(f" Hash match: Both files have MD5={orig_hash}")
        hash_match = True

    results = []
    if not (size_match and hash_match):
        print("Performing detailed binary comparison...")
        results.append(f"Detailed binary comparison - {datetime.now().strftime('%Y-%m-%d %H:%M:%S')}")
        results.append(f"Original file: {original_file} ({orig_size} bytes, MD5: {orig_hash})")
        results.append(f"Decrypted file: {decrypted_file} ({decr_size} bytes, MD5: {decr_hash})")
        results.append("-" * 80)

        with open(original_file, 'rb') as f1, open(decrypted_file, 'rb') as f2:
            orig_data = f1.read()
            decr_data = f2.read()

        min_len = min(len(orig_data), len(decr_data))
        diff_positions = []

        for i in range(min_len):
            if orig_data[i] != decr_data[i]:
                diff_positions.append(i)
                if len(diff_positions) <= 20:
                    results.append(f"Difference at position {i}: Original=0x{orig_data[i]:02x}, Decrypted=0x{decr_data[i]:02x}")

        if len(diff_positions) > 20:
            results.append(f"... and {len(diff_positions) - 20} more differences")

        results.append(f"\nTotal differences: {len(diff_positions)} bytes")
        for line in results:
            print(line)

        if report_file:
            with open(report_file, 'w') as f:
                f.write("\n".join(results))
            print(f"Detailed report saved to {report_file}")

    return size_match and hash_match

def main():
    parser = argparse.ArgumentParser(description='Verify binary equivalence between original and decrypted files')
    parser.add_argument('original', help='Path to original file')
    parser.add_argument('decrypted', help='Path to decrypted file')
    parser.add_argument('-r', '--report', help='Path to save detailed report')

    args = parser.parse_args()

    result = compare_files(args.original, args.decrypted, args.report)
    if result:
        print("\n SUCCESS: Files are binary-identical!")
        sys.exit(0)
    else:
        print("\n FAILURE: Files are different!")
        sys.exit(1)

if __name__ == "__main__":
    main()
```

9.2.2 COVER SELECTION & STEGANOGRAPHY

```
from steganography import Steganography

steg = Steganography()

original_image = "cover_images/sample.png"
secret_message = "This is a secret message hidden using BrainSecureX!"
output_image = "encrypted_files/stego_image.png"
password = "securepass123"

try:
    result_path = steg.hide_data_lsb(
        image_path=original_image,
        data=secret_message,
        output_path=output_image,
        password=password
    )
    print(f"Data successfully hidden. Stego image saved at: {result_path}")
except Exception as e:
    print(f"Error hiding data: {e}")

try:
    extracted_data = steg.extract_data_lsb(
        image_path=result_path,
        password=password
    )
    print("Extracted data:", extracted_data.decode('utf-8'))
except Exception as e:
    print(f"Error extracting data: {e}")
```

9.2.3 TRIPLE LAYER ENCRYPTION

```
from encryption.aes_encryption import AESEncryption
from encryption.ascon_encryption import AsconEncryption
from encryption.ecc_encryption import ECCEncryption
```

```
aes = AESEncryption()
ascon = AsconEncryption()
ecc = ECCEncryption()

data1 = b"Patient A - MRI Scan Encrypted"
data2 = b"Patient B - Brain Tumor Image"
data3 = b"Patient C - Encrypted EEG Record"

aes_key1 = aes.generate_key()
aes_key2 = aes.generate_key()
aes_key3 = aes.generate_key()

cipher1 = aes.encrypt(data1, aes_key1)
cipher2 = aes.encrypt(data2, aes_key2)
cipher3 = aes.encrypt(data3, aes_key3)

cipher1_ascon = ascon.encrypt(cipher1)
cipher2_ascon = ascon.encrypt(cipher2)
cipher3_ascon = ascon.encrypt(cipher3)

ecc_keys = ecc.generate_key_pair()

keys1 = ecc.encrypt_keys(aes_key1, ascon.key, ecc_keys['public_key'])
keys2 = ecc.encrypt_keys(aes_key2, ascon.key, ecc_keys['public_key'])
keys3 = ecc.encrypt_keys(aes_key3, ascon.key, ecc_keys['public_key'])

dec_keys1 = ecc.decrypt_keys(keys1, ecc_keys['private_key'])
dec_keys2 = ecc.decrypt_keys(keys2, ecc_keys['private_key'])
dec_keys3 = ecc.decrypt_keys(keys3, ecc_keys['private_key'])

ascon.key = dec_keys1[1]
dec_ascon1 = ascon.decrypt(cipher1_ascon)
plain1 = aes.decrypt(dec_ascon1, dec_keys1[0])

ascon.key = dec_keys2[1]
```

```
dec_ascon2 = ascon.decrypt(cipher2_ascon)
plain2 = aes.decrypt(dec_ascon2, dec_keys2[0])

ascon.key = dec_keys3[1]
dec_ascon3 = ascon.decrypt(cipher3_ascon)
plain3 = aes.decrypt(dec_ascon3, dec_keys3[0])

print(plain1.decode())
print(plain2.decode())
print(plain3.decode())
```

9.2.4 ALERT GENERATION

```
def on_modified(self, event):
    if event.is_directory:
        return
    file_path = event.src_path
    print(f"File modified: {file_path}")

    new_merkle_root = calculate_merkle_root(file_path)
    stored_merkle_root = get_stored_hash(file_path)

    if new_merkle_root != stored_merkle_root:
        print("Unauthorized modification detected! Restoring file...")
        self.restore_backup(file_path)
    else:
        print("Modification verified as authorized.")
def restore_backup(self, file_path):
    backup_path = os.path.join(BACKUP_FOLDER, os.path.basename(file_path))
    if os.path.exists(backup_path):
        shutil.copy2(backup_path, file_path)
        print(f"Restored {file_path} from backup.")
    else:
        print("Backup not found. Unable to restore.")
```

REFERENCES

REFERENCES

[1] K. -D. Nguyen, T. -K. Dang, B. Kieu-Do-Nguyen, D. -H. Le, C. -K. Pham and T. -T. Hoang, 'ASIC Implementation of ASCON Lightweight Cryptography for IoT Applications,' in *IEEE Transactions on Circuits and Systems II: Express Briefs,* Vol. 72, No. 1, pp. 278-282, Jan. 2025.

[2] J. Zhang et al., ‘High-Performance Elliptic Curve Scalar Multiplication Architecture Based on Interleaved Mechanism,’ in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 33, No. 3, pp. 757-770, March 2025.

[3] G. Yu, Q. Li, H. Mao, A. A. A. El-Latif and J. J. P. C. Rodrigues, ‘A Multi-Scenario Authenticated Key Exchange Scheme With Forward Secrecy for Fog-Enabled VANETs,’ in *IEEE Transactions on Vehicular Technology,* Vol. 74, No. 1, pp. 831-846, Jan. 2025.

[4] D. Xu, X. Wang, Q. Hao, J. Wang, S. Cui and B. Liu, ‘A High-Performance Transparent Memory Data Encryption and Authentication Scheme Based on Ascon Cipher,’ in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 32, No. 5, pp. 925-937, May 2024.

[5] S. Lee and J. -N. Kim, ‘Balanced Encoding of Near-Zero Correlation for an AES Implementation,’ in *IEEE Transactions on Information Forensics and Security*, Vol. 19, pp. 6589-6603, Aug. 2024.

[6] Y. Chen, H. Wang and W. Li, ‘Constructing Immune-Cover for Improving Holistic Security of Spatial Adaptive Steganography,’ in *IEEE Transactions on Dependable and Secure Computing,* Vol. 21, No. 6, pp. 5403-5419, Dec. 2024.

[7] J. Yu, J. Zhang, Z. Wang, F. Li and X. Zhang, ‘Cover Selection in Encrypted Images,’ *in IEEE Transactions on Circuits and Systems for Video Technology,* Vol. 34, No. 12, pp. 13626-13641, Dec. 2024.

[8] E. Darzi, F. Dubost, N. M. Sijtsema and P. M. A. van Ooijen, ‘Exploring Adversarial Attacks in Federated Learning for Medical Imaging,’ *in IEEE Transactions on Industrial Informatics*, Vol. 20, No. 12, pp. 13591-13599, Dec. 2024.

[9] Z. Yang, K. Chen, K. Zeng, W. Zhang and N. Yu, ‘Provably Secure Robust Image Steganography,’ in *IEEE Transactions on Multimedia*, Vol. 26, pp. 5040-5053, Jan. 2024.

[10] J. Zhang, K. Chen, W. Li, W. Zhang and N. Yu, ‘Steganography With Generated Images: Leveraging Volatility to Enhance Security,’ *in IEEE Transactions on Dependable and Secure Computing,* Vol. 21, No. 4, pp. 3994-4005, Aug. 2024.

[11] J. Zhang, Z. Chen, M. Ma, R. Jiang, H. Li and W. Wang, ‘High-Performance ECC Scalar Multiplication Architecture Based on Comb Method and Low-Latency Window Recoding Algorithm,’ in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 32, No. 2, pp. 382-395, Feb. 2024.

[12] J. Feng, Y. Wei, F. Zhang, E. Pasalic and Y. Zhou, ‘Novel Optimized Implementations of Lightweight Cryptographic S-Boxes via SAT Solvers,’ in *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 71, No. 1, pp. 334-347, Jan. 2024.

[13] A. Wu et al., ‘Design and Construction of a Low-Cryogen, Lightweight, Head-Only 7T MRI Magnet,’ in *IEEE Transactions on Applied Superconductivity,* Vol. 34, No. 5, pp. 1-5, Aug. 2024.

[14] K. Chen, H. Zhou, Y. Wang, M. Li, W. Zhang and N. Yu, ‘Cover Reproducible Steganography via Deep Generative Models,’ *in IEEE Transactions on Dependable and Secure Computing*, Vol. 20, No. 5, pp. 3787-3798, Oct. 2023.

[15] J. Dong, P. Zhang, K. Sun, F. Xiao, F. Zheng and J. Lin, ‘EG-FourQ: An Embedded GPU-Based Efficient ECC Cryptography Accelerator for Edge Computing,’ in *IEEE Transactions on Industrial Informatics,* Vol. 19, No. 6, pp. 7291-7300, June 2023.

[16] P. Rosa, A. Souto and J. Cecílio, ‘Light-SAE: A Lightweight Authentication Protocol for Large-Scale IoT Environments Made with Constrained Devices,’ in *IEEE Transactions on Network and Service Management,* Vol. 20, No. 3, pp. 2428-2441, Sept. 2023.

[17] J. Cui et al., ‘Lightweight Encryption and Authentication for Controller Area Network of Autonomous Vehicles,’ in *IEEE Transactions on Vehicular Technology,* Vol. 72, No. 11, pp. 14756-14770, Nov. 2023.

[18] J. Song, K. Lee and J. Park, ‘Low Area and Low Power Threshold Implementation Design Technique for AES S-Box,’ in *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol. 70, No. 3, pp. 1169-1173, March 2023.

[19] M. Zeghid, H. Y. Ahmed, A. Chehri and A. Sghaier, ‘Speed/Area-Efficient ECC Processor Implementation Over GF(2m) on FPGA via Novel Algorithm-Architecture Co-Design,’ in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* Vol. 31, No. 8, pp. 1192-1203, Aug. 2023.

[20] X. Li et al., ‘LIGHT: Lightweight Authentication for Intra Embedded Integrated Electronic Systems,’ in *IEEE Transactions on Dependable and Secure Computing,* Vol. 20, No. 2, pp. 1088-1103, April 2023.