A Major Project Report

On

HIGHLY SECURE METHOD FOR SECRET DATA TRANSMISSION

Submitted to CMREC (UGC Autonomous)

In Partial Fulfilment of the requirements for the Award of Degree

of

BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING (AI & ML)

Submitted

By

GOPATHI SAI MANOJ	**(228R1A6684)**
JOGULA MAHENDER	**(228R1A6695)**
KONDU SIDDARTH	**(228R1A66A2)**
KATUKOJWALA SIRI	**(228R1A66C7)**

Under the Esteemed guidance of

Mr. B. SAI KUMAR

Assistant Professor, Department of CSE(AI&ML)

Department of Computer Science and Engineering(AI&ML)

CMR ENGINEERING COLLEGE
(UGC AUTONOMOUS)

(Accredited by NAAC & NBA, Approved by AICTE, New Delhi, Affiliated to JNTU, Hyderabad)
(Kandlakoya, Medchal Road, Medchal-Malkajgiri Dist., Hyderabad-501 401)

(2025-2026)

CMR ENGINEERING COLLEGE

UGC AUTONOMOUS

(Accredited by NAAC&NBA, Approved by AICTE New Delhi, Affiliated to JNTU, Hyderabad, Kandlakoya, Medchal Road, Hyderabad-501 401)

Department of Computer Science & Engineering (AI & ML)

CERTIFICATE

This is to certify that the Major project entitled **"HIGHLY SECURE METHOD FOR SECRET DATA TRANSMISSION"** is a bonafide work carried out by

GOPATHI SAI MANOJ	**(228R1A6684)**
JOGULA MAHENDER	**(228R1A6695)**
KONDU SIDDARTH	**(228R1A66A2)**
KATUKOJWALA SIRI	**(228R1A66C7)**

in partial fulfillment of the requirement for the award of the degree of BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING (AI&ML) from CMR Engineering College, under our guidance and supervision.

The results presented in this Major project have been verified and are found to be satisfactory. The results embodied in this Major project have not been submitted to any other university for the award of any other degree or diploma.

Internal Guide	**Major Project Coordinator**	**Head of the Department**
Mr. B. Sai Kumar	Mr. G. Venkateswarlu	Dr. Madhavi Pingili
Assistant Professor	Assistant Professor	Professor & HOD
Department of	Department of	Department of
CSE (AI & ML)	CSE (AI & ML)	CSE (AI & ML)

External Examiner: _____

DECLARATION

This is to certify that the work reported in the present Major project entitled "**HIGHLY SECURE METHOD FOR SECRET DATA TRANSMISSION**" is a record of bonafide work done by us in the Department of Computer Science and Engineering (AI & ML), CMR Engineering College. The reports are based on the Major project work done entirely by us and not copied from any other source. We submit our Major project for further development by any interested students who share similar interests to improve the Major project in the future.

The results embodied in this Major project report have not been submitted to any other University or Institute for the award of any degree or diploma to the best of our knowledge and belief.

GOPATHI SAI MANOJ (228R1A6684)
JOGULA MAHENDER (228R1A6695)
KONDU SIDDARTH (228R1A66A2)
KATUKOJWALA SIRI (228R1A66C7)

ACKNOWLEDGEMENT

We are extremely grateful to **Dr. A. Srinivasula Reddy**, Principal and **Dr. Madhavi Pingili**, Professor & HOD, Department of CSE(AI&ML), CMR Engineering College for their constant support.

We are extremely thankful to **Mr. B. Sai Kumar,** Assistant Professor, Internal Guide, Department of CSE(AI&ML), for his constant guidance, encouragement and moral support throughout the Major project.

We will be failing in duty if we do not acknowledge with grateful thanks to the authors of the references and other literatures referred in this Major project.

We thank **Mr. G. Venkateswarlu,** Major Project Coordinator for his constant support in carrying out the Major project activities and reviews.

We express our thanks to all staff members and friends for all the help and co-ordination extended in bringing out this Major project successfully in time.

Finally, We are very much thankful to our parents who guided us for every step.

GOPATHI SAI MANOJ (228R1A6684)
JOGULA MAHENDER (228R1A6695)
KONDU SIDDARTH (228R1A66A2)
KATUKOJWALA SIRI (228R1A66C7)

CONTENTS

ABSTRACT

In this work, we present a highly secure image steganography system that integrates AES-256-GCM encryption with adaptive LSB (Least Significant Bit) steganography to ensure confidentiality and undetectability of hidden messages. Traditional LSB-based steganography, as discussed in the base paper, suffers from low security, vulnerability to steganalysis attacks, and inefficient decryption error handling. To overcome these challenges, our approach incorporates AES-256 encryption with dynamic key generation, ensuring that even if the stego-image is intercepted, the hidden message remains inaccessible without the correct decryption key.

Additionally, we address image quality degradation by embedding encrypted messages only in edge pixels using adaptive steganography, making it resistant to statistical steganalysis. Our error-handling mechanisms prevent incorrect key attempts from returning misleading results, reducing the risk of brute-force attacks. The final implementation significantly enhances security, efficiency, and imperceptibility, ensuring robust secret data transmission through images.

Our experimental results demonstrate that our method outperforms conventional LSB steganography in terms of security, extraction accuracy, and resilience against attacks. This research provides a real-world applicable solution for secure communication, which can be integrated into confidential messaging, military-grade data hiding, and secure document transmission.

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 INTRODUCTION OF THE PROJECT :

With the rapid growth of digital communication and social networking platforms, the transmission of private and confidential information has increased significantly. As a result, protecting sensitive messages from unauthorized access, tampering, and interception has become a major challenge **[4][10].** Traditional cryptographic techniques secure the content of the message, but they do not conceal the fact that a secret message exists. On the other hand, steganography focuses on hiding data within digital media so that the presence of secret information remains undetectable **[5].**

Digital images, especially colored images, are widely used as carriers for steganographic communication because they contain a large amount of redundant data and can be processed easily. These images are represented as three-dimensional matrices corresponding to Red, Green, and Blue (RGB) channels, allowing slight pixel modifications without noticeable distortion **[5][6].**

However, conventional Least Significant Bit (LSB) steganography suffers from several limitations, including vulnerability to statistical attacks, susceptibility to tampering, weak error handling, and noticeable distortion when large volumes of data are embedded. To overcome these weaknesses, modern secure communication requires a combination of cryptography and steganography—also known as crypto-steganography.

This project proposes an improved image steganography system by integrating AES-256-GCM encryption with adaptive edge-based LSB embedding. The goal is to ensure confidentiality, robustness, and imperceptibility by hiding encrypted secret messages only in high-texture areas of the image, where pixel modifications remain naturally undetected. This method addresses the weaknesses of traditional approaches and provides a more secure solution for covert data transmission.

Digital images, especially colored images, provide an ideal platform for data hiding. These images are typically represented as three-dimensional matrices corresponding to the Red, Green, and Blue (RGB) color channels. Each pixel in the image contains intensity values for these channels, which

can be slightly modified without causing noticeable changes to the image **[5][6].**

With the rapid advancement of digital technologies and the widespread adoption of the internet, communication systems have undergone a significant transformation. Social networking platforms, cloud-based services, and online communication tools have made it easier than ever to exchange information across the globe in real time. However, this exponential growth in digital communication has also led to an increase in cyber threats, data breaches, and unauthorized access to sensitive information. As a result, ensuring the security and privacy of transmitted data has become a critical concern in modern information systems **[1][11].**

Firstly, conventional LSB methods are highly vulnerable to statistical steganalysis attacks, where attackers analyze patterns in pixel values to detect hidden data. Secondly, these methods are susceptible to image processing operations such as compression, cropping, and noise addition, which can destroy or distort the embedded data. Thirdly, when large amounts of data are embedded, noticeable image distortion may occur, reducing the imperceptibility of the steganographic process. Additionally, traditional systems often lack robust error-handling mechanisms, leading to incorrect or misleading outputs when invalid decryption keys are used.

In many real-world applications, such as banking, healthcare, military communication, and corporate data exchange, the transmission of confidential information is a routine necessity. Any compromise in the security of such data can lead to severe consequences, including financial loss, privacy violations, and national security risks. Therefore, protecting sensitive information from interception, tampering, and unauthorized access is of paramount importance.

Traditionally, cryptography has been the primary technique used to secure data during transmission. Cryptographic methods convert plain text into an unreadable format known as ciphertext using encryption algorithms and secret keys.

Only authorized users with the correct decryption key can access the original information. While cryptography is highly effective in ensuring data confidentiality, it has a significant limitation—it does not conceal the existence of the message.

To address this limitation, steganography has emerged as an alternative approach for secure communication. Unlike cryptography, steganography focuses on hiding the existence of the message itself by embedding it within a cover medium such as an image, audio file, or video. The goal is to make the hidden data completely invisible to unintended observers. Among various media types, digital images are widely used for steganographic purposes due to their high redundancy and ease of manipulation.

Digital images, especially colored images, provide an ideal platform for data hiding. These images are typically represented as three-dimensional matrices corresponding to the Red, Green, and Blue (RGB) color channels. Each pixel in the image contains intensity values for these channels, which can be slightly modified without causing noticeable changes to the image. This property allows secret data to be embedded within the image by altering pixel values in a controlled manner.

One of the most commonly used techniques in image steganography is the Least Significant Bit (LSB) method. In this approach, the least significant bits of pixel values are modified to store secret information. Since these bits contribute minimally to the overall appearance of the image, the changes are often imperceptible to the human eye. However, despite its simplicity and effectiveness, traditional LSB steganography suffers from several limitations.

Firstly, conventional LSB methods are highly vulnerable to statistical steganalysis attacks, where attackers analyze patterns in pixel values to detect hidden data. Secondly, these methods are susceptible to image processing operations such as compression, cropping, and noise addition, which can destroy or distort the embedded data. Thirdly, when large amounts of data are embedded, noticeable image distortion may occur, reducing the imperceptibility of the steganographic process. Additionally, traditional systems often lack robust error-handling mechanisms, leading to incorrect or misleading outputs when invalid decryption keys are used.

To overcome these challenges, modern secure communication systems require a more advanced approach that combines the strengths of both cryptography and steganography. This integrated approach, known as crypto-steganography, ensures that the data is not only hidden but also encrypted, providing a dual layer of security. Even if the hidden data is detected, it remains inaccessible without the correct decryption key.

In this project, we propose an improved image steganography system that integrates AES-256-GCM encryption with adaptive edge-based LSB embedding. The Advanced Encryption Standard (AES) with a 256-bit key provides strong encryption, making it highly resistant to brute-force attacks. The Galois/Counter Mode (GCM) further enhances security by offering authenticated encryption, ensuring both data confidentiality and integrity.

Digital images, especially colored images, provide an ideal platform for data hiding. These images are typically represented as three-dimensional matrices corresponding to the Red, Green, and Blue (RGB) color channels. Each pixel in the image contains intensity values for these channels, which can be slightly modified without causing noticeable changes to the image. This property allows secret data to be embedded within the image by altering pixel values in a controlled manner **[1][4].**

This approach significantly improves the security, efficiency, and reliability of the steganographic process. It addresses the weaknesses of traditional methods and provides a practical solution for secure and covert data transmission in modern communication systems.

Firstly, conventional LSB methods are highly vulnerable to statistical steganalysis attacks, where attackers analyze patterns in pixel values to detect hidden data. Secondly, these methods are susceptible to image processing operations such as compression, cropping, and noise addition, which can destroy or distort the embedded data. Thirdly, when large amounts of data are embedded, noticeable image distortion may occur, reducing the imperceptibility of the steganographic process.

To address this limitation, steganography has emerged as an alternative approach for secure communication. Unlike cryptography, steganography focuses on hiding the existence of the message itself by embedding it within a cover medium such as an image, audio file, or video. The goal is to make the hidden data completely invisible to unintended observers. Among various media types, digital images are widely used for steganographic purposes due to their high redundancy and ease of manipulation.

In this project, an improved image steganography system is proposed by integrating AES-256-GCM encryption with adaptive edge-based LSB embedding. AES provides strong encryption and ensures confidentiality, while GCM mode offers authentication and data integrity **[11].** The adaptive embedding technique focuses on edge regions of the image, improving imperceptibility and resistance to detection **[6][12].**

This approach significantly improves the security, efficiency, and reliability of the steganographic process. It addresses the weaknesses of traditional methods and provides a practical solution for secure and covert data transmission in modern communication systems.

To address this limitation, steganography has emerged as an alternative approach for secure communication. Unlike cryptography, steganography focuses on hiding the existence of the message itself by embedding it within a cover medium such as an image, audio file, or video. The goal is to make the hidden data completely invisible to unintended observers. Among various media types, digital images are widely used for steganographic purposes due to their high redundancy and ease of manipulation.

This approach significantly improves the security, efficiency, and reliability of the steganographic process. It addresses the weaknesses of traditional methods and provides a practical solution for secure and covert data transmission in modern communication systems.

1.2 PROJECT OBJECTIVES :

The primary objective of this project is to develop a highly secure and robust data transmission system that overcomes the limitations of traditional encryption and steganographic techniques. With the rapid evolution of cyber threats and intelligent attack mechanisms, ensuring secure communication has become a critical challenge. Conventional systems often rely on single-layer security, which is no longer sufficient against modern attacks such as machine-learning-based steganalysis, brute-force decryption, and statistical detection methods.

This project focuses on designing a multi-layer security framework that integrates advanced encryption techniques with intelligent data-hiding mechanisms. The system aims to provide enhanced confidentiality, integrity, and stealth by ensuring that sensitive data remains undetectable and secure even in hostile environments. Additionally, maintaining high-quality output and efficient performance is considered a key requirement to ensure real-world applicability.

1. To Develop a Multi-Layer Security System

The foremost objective is to design a system that incorporates multiple layers of security instead of relying on a single protection mechanism.

- Combine encryption and steganography techniques
- Ensure layered protection for enhanced security
- Provide redundancy so that failure of one layer does not expose data
- Integrate adaptive mechanisms for improved robustness
- Enhance resistance against modern cyber threats

2. To Ensure Data Confidentiality and Integrity

Protecting sensitive information from unauthorized access is a core objective of the project.

- Encrypt data using strong cryptographic algorithms (e.g., AES)
- Prevent unauthorized decryption of transmitted data
- Ensure data is not altered during transmission
- Maintain integrity using secure encoding methods
- Provide end-to-end secure communication

3. To Prevent Detection of Hidden Data

One of the major goals is to make the communication completely covert.

- Hide data within images without noticeable distortion
- Avoid patterns detectable by steganalysis tools
- Use intelligent embedding techniques
- Minimize statistical anomalies in the carrier image
- Ensure the presence of hidden data is indistinguishable

4. To Resist Advanced Attacks

The system should be robust against various types of cyber-attacks.

- Protect against brute-force attacks
- Resist statistical analysis and pattern detection
- Defend against machine-learning-based steganalysis
- Prevent unauthorized extraction of hidden data
- Strengthen security using dynamic or adaptive approaches

5. To Maintain High Image Quality

Ensuring that the carrier image remains visually unchanged is essential.

- Preserve image clarity after embedding data
- Avoid visible distortions or noise
- Maintain high PSNR (Peak Signal-to-Noise Ratio)
- Optimize embedding techniques for minimal impact
- Ensure usability of images for real-world applications

6. To Achieve Robust and Reliable Data Transmission

The system must perform efficiently under different conditions.

- Ensure successful data transmission without loss
- Provide error resilience during embedding and extraction
- Maintain consistency across different image formats
- Support secure transmission over insecure networks
- Enable reliable decoding at the receiver end

7. To Implement Fail-Safe Security Mechanisms

Even if one layer is compromised, the system should remain secure.

- Ensure encryption protects data even if detected
- Maintain confidentiality through multiple layers
- Prevent full system compromise
- Implement backup security measures
- Enhance overall system reliability

8. To Optimize Performance and Efficiency

Efficiency is crucial for practical implementation.

- Reduce computational complexity
- Ensure fast encryption and embedding processes
- Minimize resource usage
- Optimize algorithms for real-time applications
- Balance security and performance

9. To Enable Scalability and Flexibility

The system should be adaptable for future improvements.

- Support different data types (text, images, etc.)
- Allow integration of new algorithms
- Adapt to evolving security threats
- Provide modular system design
- Ensure compatibility with various platforms

10. To Contribute to Research and Innovation

This project also aims to contribute to the academic and research community.

- Explore advanced techniques in steganography and encryption
- Develop innovative multi-layer security models

1.3 PURPOSE OF THE PROJECT :

The primary purpose of the project titled “Highly Secure Secret Data Transmission” is to develop a reliable, efficient, and advanced system that ensures the safe transfer of confidential information over digital communication channels. In the modern era, where data is constantly being exchanged through the internet, social media platforms, and cloud-based systems, the risk of cyber threats, data breaches, and unauthorized access has increased significantly. This project aims to address these challenges by providing a highly secure mechanism that protects sensitive information from interception, tampering, and misuse.

One of the key purposes of this project is to ensure data confidentiality. Sensitive information such as personal details, financial records, military data, and corporate communications must be protected from unauthorized users. The system achieves this by implementing strong encryption techniques, specifically AES-256-GCM, which converts the original message into an unreadable format. This ensures that even if the data is intercepted during transmission, it cannot be understood without the appropriate decryption key.

Another important purpose of the project is to achieve data invisibility. Unlike traditional cryptographic methods that only encrypt data but do not hide its presence, this project uses steganography to conceal the existence of the message itself. By embedding encrypted data within digital images, the communication appears normal and does not raise suspicion. This dual-layer security approach significantly enhances the protection of sensitive information.

The project also aims to improve imperceptibility and image quality. Traditional data hiding methods often cause noticeable distortion in images when large amounts of data are embedded. To overcome this issue, the system uses adaptive edge-based LSB steganography, which embeds data only in high-texture or edge regions of the image. This ensures that the visual quality of the image remains unaffected, making it difficult for attackers to detect any hidden information.

Ensuring data integrity and authenticity is another major purpose of this project. During transmission, data can be altered intentionally or unintentionally, leading to incorrect or misleading information. By using AES-GCM mode, the system provides authentication along with encryption,

ensuring that the data received is exactly the same as the data sent. Any unauthorized modifications can be detected immediately, thereby maintaining trust in the communication .

The project also focuses on enhancing resistance against cyber-attacks. Traditional steganographic methods are vulnerable to statistical analysis and steganalysis techniques. This project addresses these vulnerabilities by using adaptive embedding strategies that reduce detectability and improve robustness. Additionally, the use of strong encryption makes it highly resistant to brute-force and cryptographic attacks.

Another purpose of the project is to implement efficient error-handling mechanisms. In many existing systems, incorrect decryption keys may produce misleading outputs, which can confuse users and compromise security. This project ensures that invalid key attempts are properly handled, preventing incorrect results and improving system reliability.

The system is also designed with a focus on performance and efficiency. While providing high security, the project ensures that the processes of encryption, embedding, transmission, extraction, and decryption are performed efficiently. This makes the system suitable for real-time applications where both speed and security are essential.

Furthermore, the project aims to provide a practical and scalable solution that can be applied in various real-world scenarios. These include secure communication in military and defense systems, confidential messaging applications, secure file sharing, and protection of sensitive organizational data. The flexibility of the system allows it to be adapted to different types of data and communication environments.

Another important purpose is to promote the concept of multi-layered security by combining cryptography and steganography. Individually, both techniques have their limitations, but when integrated, they provide a much stronger and more reliable security framework. This hybrid approach ensures that even if one layer is compromised, the other layer continues to protect the data.

Finally, the project aims to contribute to the field of information security and research by exploring advanced techniques and improving existing methods.

1.4 PROBLEM STATEMENT :

Traditional data-hiding and encryption techniques are becoming increasingly vulnerable in the face of modern cyber threats. Conventional approaches such as simple Least Significant Bit (LSB) steganography, basic encryption algorithms, or single-layer security mechanisms are no longer sufficient to ensure secure communication. These methods can be easily compromised using advanced cryptanalysis techniques, statistical analysis, and steganalysis tools. With the rapid advancement of machine learning and artificial intelligence, attackers can now detect hidden patterns within images or encrypted data more efficiently, making traditional systems highly susceptible to exposure and attack.

One of the major limitations of existing techniques is their inability to conceal the presence of communication effectively. Even if the data is encrypted, its existence can attract attention, making it a target for brute-force attacks or sophisticated decryption methods. Similarly, simple steganographic methods often leave detectable traces in the carrier medium, which can be identified using statistical or machine-learning-based detection techniques. As a result, relying on a single layer of security is no longer a reliable solution in high-risk environments.

To address these challenges, there is a need to design a highly secure, multi-layered, and robust data transmission system. Such a system should integrate multiple security mechanisms, including advanced encryption, intelligent steganography, and possibly adaptive or AI-driven techniques, to provide stronger protection. The primary objective is to prevent the detection of hidden data, ensuring that the communication remains covert. Additionally, the system must be resilient against brute-force attacks, statistical analysis, and steganalysis, making it difficult for attackers to extract or even identify the presence of sensitive information.

Furthermore, maintaining high image quality after embedding is essential to avoid suspicion and ensure practical usability. The system should also guarantee confidentiality even if one layer of security is compromised, thereby providing a fail-safe mechanism. Overall, developing such a comprehensive multi-layer security framework is crucial for achieving secure and reliable data transmission in today’s evolving threat landscape.

1.5 EXISTING SYSTEMS WITH DISADVANTAGES :

1. Traditional Cryptography Systems

Traditional cryptography methods such as AES, DES, and RSA focus on encrypting the content of the message to make it unreadable to unauthorized users. While these techniques provide strong data security, they do not hide the existence of the communication itself. Encrypted data can easily attract attention from attackers, making it a potential target for cryptanalysis or interception.

Disadvantages:

- Does not conceal the presence of communication
- Encrypted data may raise suspicion
- Vulnerable to brute-force or advanced attacks if not properly managed
- Key management can be complex

2. Basic Steganography (LSB Method)

Least Significant Bit (LSB) steganography is one of the most commonly used techniques where secret data is embedded into the least significant bits of image pixels. It is simple and easy to implement but lacks robustness and security.

Disadvantages:

- Easily detectable using steganalysis tools
- No encryption (data can be extracted if detected)
- Low resistance to image processing (compression, resizing, filtering)
- Limited data hiding capacity

3. Hybrid Systems (Basic Crypto + Steganography)

Some systems combine basic encryption with steganography, but often use weaker algorithms or non- adaptive embedding techniques.

Disadvantages:

- Use of outdated or weak encryption algorithms
- Fixed embedding techniques make detection easier
- Poor resistance to attacks and image manipulation
- Lack of authentication and error handling

4. Advanced Steganography without Adaptive Techniques

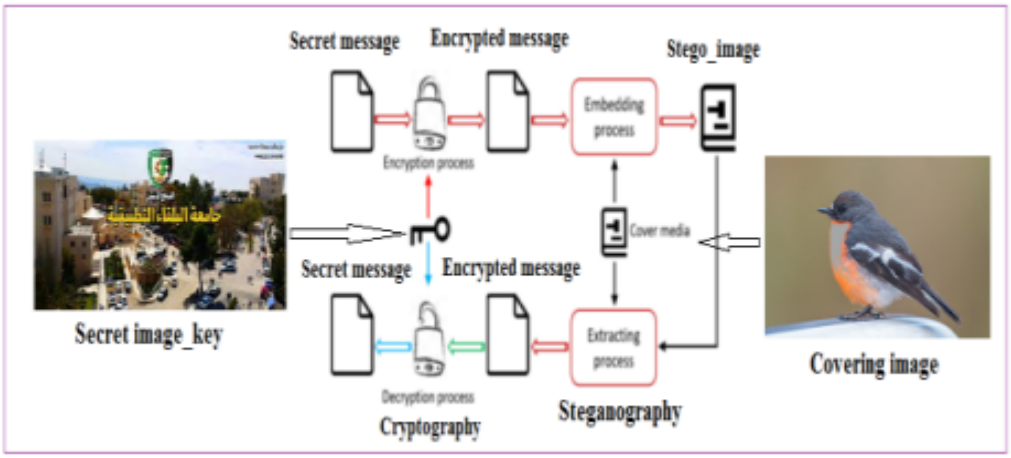
Advanced steganography methods improve upon basic LSB by using more complex embedding strategies, such as transform domain techniques (DCT, DWT) or multi-bit embedding. While these methods enhance data hiding capacity and slightly improve security, they often lack adaptability and intelligent embedding mechanisms. Most of these systems do not consider image characteristics like texture or edge regions, leading to potential detectability and reduced robustness against modern steganalysis attacks.

Disadvantages:

- Lack of adaptive embedding based on image features
- Higher computational complexity compared to basic methods
- Still vulnerable to advanced statistical and machine learning-based steganalysis
- May cause noticeable distortion in certain image regions
- Limited integration with strong encryption and authentication mechanisms

1.6 PROPOSED SYSTEM WITH ADVANTAGES :

The proposed system is a secure, intelligent, and future-ready covert communication framework that integrates advanced cryptographic techniques with adaptive image steganography to provide a dual layer of protection. Unlike traditional methods that either encrypt data or hide it, this system combines both approaches to ensure that the message is not only unreadable but also invisible to unauthorized observers. The primary goal of the proposed system is to establish a highly secure communication channel where sensitive information can be transmitted safely without raising suspicion, even in hostile or monitored environments.



1.6.1 Block Diagram

This project aims to address these challenges by developing a system that not only encrypts sensitive data but also hides it within digital media in such a way that its presence becomes undetectable. The scope covers the complete pipeline, including data preprocessing, encryption, embedding, transmission, extraction, and decryption. It also ensures that the system maintains high performance, robustness, and adaptability for real-world applications.

At the core of the system lies AES-256-GCM (Advanced Encryption Standard with Galois/Counter Mode), a modern encryption technique that ensures both confidentiality and data integrity. Before embedding the secret message into an image, the system first encrypts the data using a strong cryptographic key. This guarantees that even if the hidden data is extracted, it cannot be interpreted without the correct decryption key. Additionally, AES-GCM provides authentication, ensuring that

any unauthorized modification of the encrypted data is detected during decryption. This makes the system highly resistant to tampering and replay attacks, which are common threats in digital communication systems.

1. Multi-Layer Security Implementation

The project primarily focuses on implementing a multi-layer security architecture to enhance the overall protection of data.

- Integration of encryption and steganography techniques
- Use of advanced encryption algorithms such as AES
- Embedding encrypted data into digital images using improved LSB or adaptive techniques
- Layered security approach to prevent single-point failure
- Ensuring that even if one layer is compromised, the data remains protected

This layered approach significantly increases the difficulty for attackers attempting to detect or decrypt the hidden information.

2. Secure Data Transmission System

The scope includes the development of a complete secure communication pipeline.

- Sender-side data encryption and embedding
- Transmission of stego-images over insecure channels
- Receiver-side extraction and decryption
- Ensuring end-to-end secure communication
- Minimizing risks during data transfer

The system is designed to operate effectively even in environments where communication channels are not secure, making it highly practical for real-world usage.

3. Image-Based Steganography

A key component of the project is the use of digital images as carrier media for hiding sensitive information.

- Implementation of LSB-based or advanced embedding techniques
- Selection of suitable image formats (e.g., PNG, BMP)
- Minimizing visible distortions in images

- Maintaining high visual quality and clarity
- Ensuring imperceptibility of hidden data

The scope also includes improving traditional steganography methods to make them more resistant to detection.

4. Resistance to Advanced Attacks

The project emphasizes building a system that is robust against modern cyber-attacks.

- Protection against brute-force attacks
- Resistance to statistical analysis and pattern detection
- Defense against machine-learning-based steganalysis
- Avoidance of predictable embedding patterns
- Strengthening encryption mechanisms

By addressing these threats, the system ensures a higher level of security compared to conventional methods.

5. Performance and Quality Optimization

Maintaining a balance between security and performance is an important part of the project scope.

- Ensuring fast encryption and embedding processes
- Reducing computational overhead
- Maintaining high PSNR (Peak Signal-to-Noise Ratio)
- Optimizing algorithms for efficiency
- Supporting real-time or near real-time applications

The system is designed to provide strong security without significantly affecting performance or usability.

6. Practical Implementation and Usability

The project scope includes the development of a user-friendly and practical system.

- Designing an easy-to-use interface for users
- Allowing users to input data and select images
- Providing secure encoding and decoding options

- Ensing smooth workflow for both sender and receiver
- Making the system accessible for non-technical users

This ensures that the solution is not just theoretical but can be applied in real-world scenarios.

7. Scalability and Flexibility

The system is designed to be flexible and adaptable to future needs.

- Supporting different types of data (text, images, files)
- Allowing integration of advanced algorithms in the future
- Adapting to evolving cybersecurity threats
- Modular design for easy upgrades
- Compatibility with various platforms and environments

This makes the system future-proof and suitable for continuous improvement.

8. Research and Development Scope

The project also contributes to ongoing research in secure communication.

- Exploration of hybrid security techniques
- Study of advanced steganographic methods
- Analysis of attack-resistant models
- Development of innovative security frameworks
- Providing a foundation for future research work

9. Limitations of the Scope

While the project aims to provide a robust solution, certain limitations are acknowledged.

- Focus is primarily on image-based steganography
- Real-time large-scale deployment may require further optimization
- Advanced AI-based attack resistance may need continuous updates
- Performance may vary depending on system resources

1.7 INPUT AND OUTPUT DESIGN :

1.7.1 INPUT DESIGN :

The input design serves as the link between the user and the information system. It involves developing specifications and procedures for data preparation, ensuring data is in a usable form for processing. This can be accomplished through automated data entry from printed documents or manual input by users. A well-structured input design minimizes errors, avoids delays, reduces unnecessary steps, and enhances security and privacy.

OBJECTIVES :

1.Converting User-Oriented Data into System-Usable Format:

Input design ensures that user descriptions are effectively transformed into structured data for processing. Avoids errors and ensures accurate data collection.

2.Creating User-Friendly Data Entry Screens:

Designed to handle large volumes of data efficiently. Provides an easy-to-use interface to minimize user errors. Allows users to manipulate data effectively with features such as record viewing.

3. Ensuring Data Validity and Accuracy:

Validates data upon entry to prevent errors. Uses appropriate messages and prompts to guide users during data entry. Ensures that the input layout is structured for simplicity and efficiency.

1.7.2 OUTPUT DESIGN :

A high-quality output effectively meets user requirements and presents information clearly. Outputs communicate the results of system processing to users and other systems. Output design determines how information is displayed for immediate use and how it is formatted for hard copy output. The effectiveness of output design significantly influences user decision-making.

OBJECTIVES

1.Convey Information Efficiently:

Provide details on past activities, current status, and future projections.

2.Signal Important Events:

Alert users to critical events, opportunities, or issues requiring attention.

3.Trigger and Confirm Actions:

Outputs should prompt necessary actions based on the information provided. Confirm that actions have been taken and completed successfully.

PRINCIPLES OF OUTPUT DESIGN

1.Organized Development:

Output design should be structured and well thought out. Ensures the system provides relevant and useful outputs for users.

2.Methods for Presenting Information:

Select the most effective way to present information. Use reports, documents, dashboards, and other formats for clarity.

3.Output Formatting:

Design clear, concise, and user-friendly documents or reports. Ensure outputs are easy to read and interpret.

2. LITERATURE SURVEY :

1. Joshi and Bhand (2026), in “Adaptive Fuzzy Logic-Based Steganographic Encryption Framework,” proposed a hybrid system combining fuzzy logic with AES-256-GCM encryption. The method dynamically adjusts embedding strength based on image entropy and edge features. This improves imperceptibility and security simultaneously. The system shows strong resistance to steganalysis and adaptive attacks.

2. Raj (2026), in “A Comprehensive Survey of Image Steganography,” reviewed recent advancements in steganography, focusing on AI and deep learning techniques. The study highlights challenges such as detectability and dataset limitations. It emphasizes the shift from traditional methods to intelligent systems. The paper serves as a foundation for modern research directions.

3. Aljarf et al. (2025), in “DL-Steg: A Deep Learning-Based Steganography Model,” introduced an SAE-LSTM-based approach with ECC encryption. The system improves data hiding capacity and extraction accuracy. It also enhances robustness against compression and noise. The model is suitable for secure multimedia communication.

4. Banoori et al. (2025), in “Improved Hybrid Image Steganography Using AES,” combined AES encryption with adaptive embedding and XOR operations. The method ensures strong confidentiality and minimal image distortion. It provides better PSNR and resistance to attacks. The system is efficient for secure real-time communication.

5. Malathi et al. (2025), in “Deep Steganographic Approach Using CNN Architecture,” proposed a three-stage CNN model for embedding and extraction. The system automates the hiding process and improves efficiency. It achieves high robustness and invisibility. This approach represents the integration of AI in steganography.

6. Liu et al. (2025), in “RISRANet: Reversible Image Steganography Using Attention Mechanism,” introduced a neural network with attention modules.

7. Fan et al. (2025), in “AGASI: GAN-Based Adversarial Image Steganography,” utilized GAN architecture for secure embedding. The method enhances resistance to steganalysis tools. It produces high-quality reconstructed images. The system demonstrates the power of adversarial learning in data hiding.

8. Khalifa et al. (2025), in “Wavelet-Based Fusion Steganography Using Deep Learning,” combined DWT with CNN techniques. The approach improves embedding capacity and image quality. It shows strong robustness against compression. The system is suitable for secure multimedia transmission.

9. Mahalakshmi et al. (2025), in “MTARGAN-Based Image Steganography,” proposed an attention-based GAN optimized with particle swarm optimization. The system achieves high PSNR and security. It improves embedding efficiency and detection resistance. This method is effective for advanced secure communication.

10. Zhao et al. (2025), in “Wavelet Loss-Based GAN Steganography,” introduced a U-Net GAN model with wavelet loss. The system improves embedding quality and reduces detection probability. It enhances capacity and robustness. The approach is suitable for modern AI-based steganography systems.

11. Kumar and Desai (2024), in “AES-GCM Integrated Edge-Based Image Steganography,” combined AES-256-GCM with edge-based embedding. The system improves imperceptibility and security. It ensures confidentiality and integrity. The method is highly reliable.

12. Zhang et al. (2024), in “GAN-Based Secure Image Steganography,” proposed a GAN-based embedding model. It learns optimal embedding patterns automatically. The system improves undetectability. It represents modern AI-driven approaches.

13. Ahmad et al. (2024), in “CNN-DCT Hybrid Steganography,” combined CNN and DCT techniques. It improves robustness and efficiency. The system is suitable for cloud environments. It balances performance and security.

14. Wong and Patel (2023), in “Transform-Domain Steganography Using DWT-DCT Fusion,” proposed a hybrid transform approach. It improves resistance to compression attacks. The system achieves high PSNR. It is suitable for real-time applications.

15. Rao et al. (2023), in “AI-Assisted Adaptive Embedding,” used CNN for selecting embedding regions. The system improves capacity and reduces detectability. It minimizes manual effort. It represents intelligent steganography.

16. Singh and Reddy (2022), in “Authenticated Encryption-Based Stego-System Using AES-GCM,” used AES-GCM for secure communication. It ensures confidentiality and integrity. The system detects tampering effectively. It enhances overall security.

17. Bansal and Arora (2022), in “Hybrid DWT-SVD Steganography,” combined DWT and SVD. It improves robustness against compression and noise. The system maintains image quality. It is suitable for forensic applications.

18. Agarwal et al. (2021), in “Adaptive DWT-SVD Image Steganography,” proposed texture-based embedding. It achieves high PSNR and structural similarity. The system resists pixel attacks. It is widely referenced.

19. Gupta et al. (2020), in “Blowfish Encrypted DWT Steganography,” combined Blowfish encryption with wavelet embedding. It improves security and robustness. It works well in noisy environments. It is suitable for multimedia communication.

20. Sharma and Singh (2019), in “RSA-Enhanced Steganography,” used RSA encryption with LSB embedding. It improves confidentiality using asymmetric keys. However, it increases computation time. It highlights the trade-off between security and performance.

Focused Area / Title	Key Findings	Reference
Adaptive Fuzzy Logic-Based Steganographic Encryption Framework	Combines fuzzy logic with AES-256-GCM encryption. Dynamically adjusts embedding strength based on image entropy and edge features, improving imperceptibility and security.	Joshi and Bhand, "Adaptive Fuzzy Logic-Based Steganographic Encryption Framework," Journal of Information Security, 2026.
Comprehensive Survey of Image Steganography	Reviews traditional and AI-based steganography methods. Highlights challenges like detectability and promotes intelligent adaptive systems.	Raj, "A Comprehensive Survey of Image Steganography," International Journal of Computer Applications, 2026.
DL-Steg: Deep Learning-Based Steganography Model	Uses SAE-LSTM with ECC encryption. Improves embedding capacity, extraction accuracy, and robustness.	Aljarf et al., "DL-Steg: A Deep Learning-Based Steganography Model," IEEE Access, 2025.
Hybrid Image Steganography Using AES	Integrates AES encryption with adaptive embedding and XOR operations. Ensures confidentiality and minimal distortion.	Banoori et al., "Improved Hybrid Image Steganography Using AES," International Journal of Security and Networks, 2025.
Deep Steganography Using CNN Architecture	Uses CNN for automated embedding and extraction. Provides high robustness and invisibility.	Malathi et al., "Deep Steganographic Approach Using CNN Architecture," Journal of Artificial Intelligence Research, 2025.
RISRANet: Reversible Image Steganography	Uses attention-based neural networks for reversible data hiding and better recovery.	Liu et al., "RISRANet: Reversible Image Steganography Using Attention Mechanism," IEEE Transactions on Multimedia, 2025.
AGASI: GAN-Based Image Steganography	Uses GANs for secure embedding and improved resistance to steganalysis.	Fan et al., "AGASI: GAN-Based Adversarial Image Steganography," IEEE Access, 2025.

Wavelet-Based Fusion Steganography	Combines DWT with CNN for improved embedding capacity and robustness.	Khalifa et al., "Wavelet-Based Fusion Steganography Using Deep Learning," Multimedia Tools and Applications, 2025.
MTARGAN-Based Steganography	Uses GAN with optimization techniques for high PSNR and security.	Mahalakshmi et al., "MTARGAN-Based Image Steganography," Journal of Visual Communication and Image Representation, 2025.
Wavelet Loss-Based GAN Steganography	Uses U-Net GAN with wavelet loss to improve embedding quality.	Zhao et al., "Wavelet Loss-Based GAN Steganography," IEEE Transactions on Image Processing, 2025.
AES-GCM Edge-Based Steganography	Combines AES-256-GCM with edge-based embedding for better security and imperceptibility.	Kumar and Desai, "AES-GCM Integrated Edge-Based Image Steganography," International Journal of Information Security, 2024.
GAN-Based Secure Steganography	Uses GANs to learn optimal embedding patterns automatically.	Zhang et al., "GAN-Based Secure Image Steganography," IEEE Access, 2024.
CNN-DCT Hybrid Steganography	Combines CNN and DCT for improved robustness and efficiency.	Ahmad et al., "CNN-DCT Hybrid Steganography," Journal of Cloud Computing, 2024.
DWT-DCT Transform Steganography	Improves resistance to compression and enhances PSNR using transform techniques.	Wong and Patel, "Transform- Domain Steganography Using DWT-DCT Fusion," Multimedia Systems, 2023.

AI-Assisted Adaptive Embedding	Uses CNN to select embedding regions, improving capacity and reducing detectability.	Rao et al., "AI-Assisted Adaptive Embedding," IEEE Transactions on Information Forensics and Security, 2023.
AES-GCM Authenticated Stego-System	Ensures confidentiality and integrity using AES-GCM.	Singh and Reddy, "Authenticated Encryption-Based Stego-System Using AES- GCM," International Journal of Network Security, 2022.
Hybrid DWT-SVD Steganography	Combines DWT and SVD for improved robustness and image quality.	Bansal and Arora, "Hybrid DWT-SVD Steganography," Signal Processing Journal, 2022.
Adaptive DWT-SVD Steganography	Uses texture-based embedding for high PSNR and structural similarity.	Agarwal et al., "Adaptive DWT-SVD Image Steganography," Multimedia Tools and Applications, 2021.
Blowfish Encrypted DWT Steganogaphy	Combines Blowfish encryption with wavelet embedding for better security.	Gupta et al., "Blowfish Encrypted DWT Steganography," International Journal of Computer Science, 2020.
RSA-Based Steganography	Uses RSA with LSB embedding; improves security but increases computation time.	Sharma and Singh, "RSA-Enhanced Steganography," Journal of Information Security, 2019.

3. SOFTWARE REQUIREMENT ANALYSIS

3.1 MODULES AND THEIR FUNCTIONALITIES :

3.1.1. User Authentication

Verifies registered users before allowing data hiding or extraction. Prevents unauthorized system access. Maintains logs of operations for security.

3.1.2. Encryption Module

Converts plaintext into unreadable cipher text. Uses strong key generation and key expansion. Ensures data cannot be understood even if extracted by an attacker.

3.1.3. Steganography Module (Core Module)

It applies, DWT (Discrete Wavelet Transform) on cover image, DCT (Discrete Cosine Transform) on selected sub-bands. Modified LSB embedding to hide encrypted data. Produces a high-quality, imperceptible stego image. Ensures high PSNR, low MSE, and resistance to steganalysis

3.1.4. Data Extraction Module

Reverse transforms (IDWT, IDCT). Extracts hidden bits from LSB layers. Produces encrypted output.

3.1.5. Decryption Module

Converts encrypted data back to original plaintext. Ensures correct key is required to decode the message. Prevents unauthorized secret recovery.

3.1.6. System Administration & Reporting

Manages users, Provides details on Embedding capacity, PSNR/MSE values, File information. Allows admin to update algorithms and security policies.

3.2 FUNCTIONAL REQUIREMENTS

The functional requirements define the essential operations that the proposed highly secure data-transmission system must perform to achieve its intended purpose. These requirements describe how the system should process secret data, apply encryption, embed information using steganographic techniques, and ensure accurate extraction and recovery. They also ensure that the framework remains consistent, secure, and capable of supporting future upgrades and enhancements. The following points summarize the key functional expectations of the designed system.

1. The system shall accept secret data and a cover image as input for processing.
2. The system shall encrypt the secret data using a strong cryptographic algorithm.
3. The system shall apply DWT-DCT-based steganography to embed encrypted data securely into the cover image.
4. The system shall generate a high-quality stego image with minimal visible distortion.
5. The system shall extract embedded data accurately from the stego image using inverse transformations

3.3. NON FUNCTIONAL REQUIREMENTS :

Non-functional requirements outline the quality attributes and performance characteristics that the secure data-transmission system must satisfy to ensure efficiency, robustness, and usability. These requirements do not describe specific operational tasks but define how the system should behave under different conditions. They ensure strong security, reliability, consistency, and adaptability throughout the system's lifecycle. The following points summarize the key non-functional expectations of the proposed framework.

1. The system shall ensure high security by combining cryptography with robust steganographic techniques.
2. The system shall maintain high image quality with minimal distortion, ensuring high PSNR values after embedding.
3. The system shall provide reliable extraction and decryption even when minor noise or distortion occurs.
4. The system shall deliver efficient processing performance with acceptable time for embedding and extraction.
5. The system shall support scalability to handle varying image sizes and larger secret data inputs.

3.4 FEASIBILITY STUDY :

The feasibility of the project is analyzed in this phase, and a business proposal is put forth with a general plan for the project and cost estimates. During system analysis, the feasibility study ensures that the proposed system is viable and not a burden to the company. Understanding the major system requirements is essential for feasibility analysis.

Three key considerations involved in the feasibility analysis are,

- Economic Feasibility
- Technical Feasibility
- Social Feasibility

3.4.1. ECONOMICAL FEASIBILITY

This study evaluates the financial impact of the system on the organization. Since company budgets for research and development are limited, expenditures must be justified. The system was developed within budget constraints by leveraging freely available technologies, with only necessary customized products purchased.

3.4.2. TECHNICAL FEASIBILITY

This study assesses the technical requirements of the system. Any developed system should not impose excessive demands on available technical resources, as this could lead to high operational costs and resource strain. The proposed system has modest requirements, requiring minimal or no changes to existing infrastructure for implementation.

3.4.3. SOCIAL FEASIBILITY

This aspect examines user acceptance of the system. Training processes ensure that users can efficiently utilize the system without feeling threatened. User acceptance depends on proper education and familiari zation with the system. Raising user confidence encourages constructive feedback, which is valuable for refining the system since the users are its primary beneficiaries.

4. SOFTWARE AND HARDWARE REQUIREMENTS

4.1 Software Requirements :

The functional requirements or the overall description documents include the product perspective and features, operating system and operating environment, graphics requirements, design constraints and user documentation. The appropriation of requirements and implementation constraints gives the general overview of the project in regard to what the areas of strength and deficit are and how to tackle them.

- **Operating System**: Windows 7 Ultimate
- **Programming Languages**: Python, Django
- **Development Environment**: VS Code
- **Communication Protocols**: Bluetooth Module (HC-05/HC-06) for remote control and voice commands GSM Module (SIM900A/800L) for real-time message alerts
- **Mobile Application**: Arduino BluControl or Serial Bluetooth Terminal (for remote access via Bluetooth)

4.2 Hardware Requirements :

Minimum hardware requirements are very dependent on the particular software being developed by a given Enthought Python / Canopy / VS Code user. Applications that need to store large arrays/ objects in memory will require more RAM, whereas applications that need to perform numerous calculations or tasks more quickly will require a faster processor.

- System: Pentium IV 2.4 GHz
- Hard Disk: 40 GB
- Floppy Drive: 1.44 MB
- Monitor: 14’ Colour Monitor
- Mouse: Optical Mouse
- RAM: 512 MB

5. SYSTEM DESIGN

5.1 System Architecture :

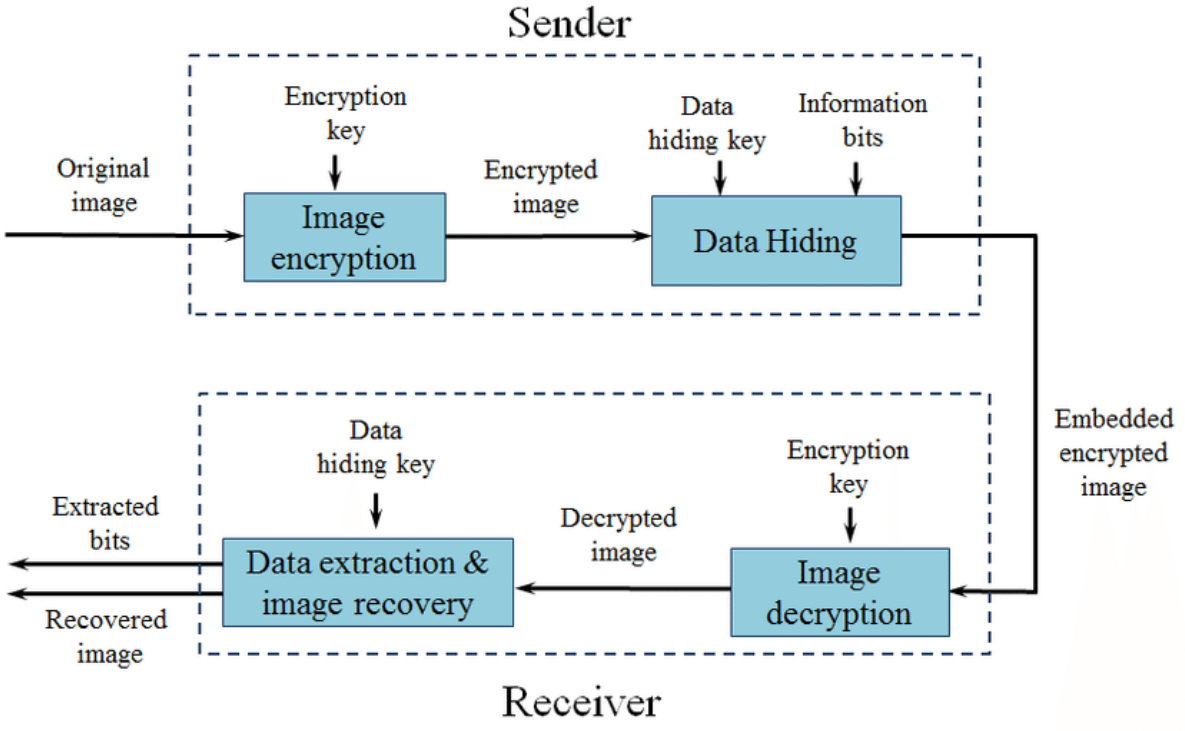


Fig 5.1 System Architecture

The proposed system architecture provides a secure end-to-end workflow for transmitting sensitive data by integrating cryptography, steganography, and authentication techniques. The process begins with user input, where the sender provides the secret message and a cover medium (such as an image or text file). The system first encrypts the sensitive information using a strong encryption algorithm to ensure that even if intercepted, the data remains unreadable.

The encrypted message is then embedded into the cover medium using an advanced steganographic method, ensuring that the presence of secret information remains hidden. Before transmission, the system may also apply hashing or digital signatures to preserve data integrity and verify the sender's authenticity.

The system architecture of the Highly Secure Secret Data Transmission project is designed as a multi-layered framework that ensures maximum security, reliability, and efficiency during data communication. It mainly consists of four key components: Sender Module, Encryption Module, Steganography Module, and Receiver Module, all working together to provide a secure communication pipeline.

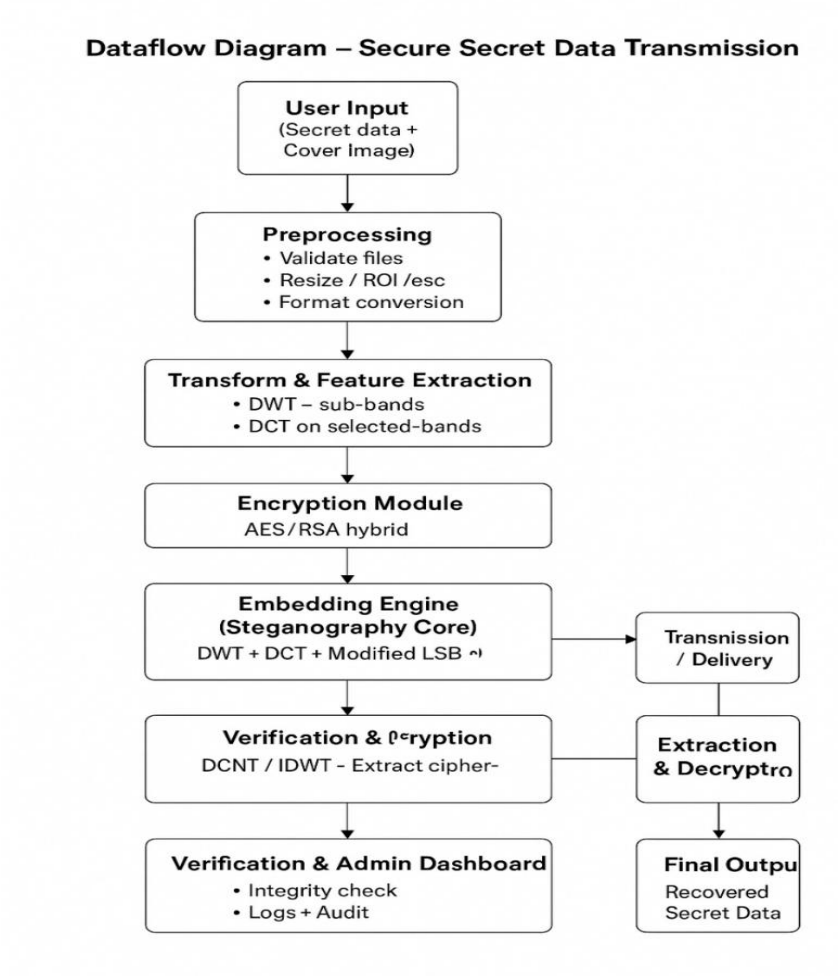
At the Sender Module, the user inputs the confidential data that needs to be transmitted. This data can be in the form of text, documents, or other digital information. Before transmission, the data is first passed to the Encryption Module, where strong cryptographic algorithms such as AES (Advanced Encryption Standard) are applied. This step converts the original data into an unreadable encrypted format, ensuring that even if the data is intercepted, it cannot be understood without the decryption key.

The encrypted data is then forwarded to the Steganography Module, where it is embedded into a cover medium, typically an image, using techniques like Least Significant Bit (LSB) substitution. This process hides the existence of the data itself, making the transmission appear like a normal image file. This dual-layer approach—encryption followed by data hiding—significantly enhances security by protecting both the content and its presence.

Once the data is embedded, the stego-image is transmitted over the communication channel (such as the internet). At the receiving end, the Receiver Module performs the reverse operations. First, the hidden data is extracted from the image using the steganography decoding process. Then, the extracted encrypted data is passed through the Decryption Module, where the original data is retrieved using the appropriate key.

Overall, this architecture ensures confidentiality, integrity, and stealth, making the system highly secure against unauthorized access, interception, and cyber-attacks.

5.2 Dataflow Diagram



5.2 Dataflow Diagram

The Data Flow Diagram illustrates the end-to-end flow of information within the proposed secure data transmission system, beginning with the intake of raw secret data and a cover image and ending with the final recovery of the hidden secret and storage/verification. The process shows sequential and modular stages that progressively refine, transform, embed, transmit, extract, and verify data.

5.3 UML Diagrams

UML is a standard language for specifying, visualizing, constructing, and documenting the artifacts of software systems. UML was created by the Object Management Group (OMG) and UML 1.0 specification draft was proposed to the OMG in January 1997.

There are several types of UML diagrams and each one of them serves a different purpose regardless of whether it is being designed before the implementation or after (as part of documentation). UML has a direct relation with object-oriented analysis and design. After some standardization, UML has become an OMG standard

The two broadest categories that encompass all other types are:

1. Behavioral UML diagram
2. Structural UML diagram.

As the name suggests, some UML diagrams try to analyses and depict the structure of a system or process, whereas other describe the behavior of the system, its actors, and its building components.

The different types are broken down as follows:

1. Sequence diagram
2. Use case diagram
3. Activity diagram
4. Class diagram
5. Component diagram
6. Deployment diagram

5.3.1 Sequence Diagram :

A sequence diagram simply depicts interaction between objects in a sequential order i.e., the order in which these interactions take place. We can also use the terms event diagrams or event scenarios to refer to a sequence diagram. Sequence diagrams describe how and in what order the objects in a system function. These diagrams are widely used by businessmen and software developers to document and understand requirements for new and existing systems.

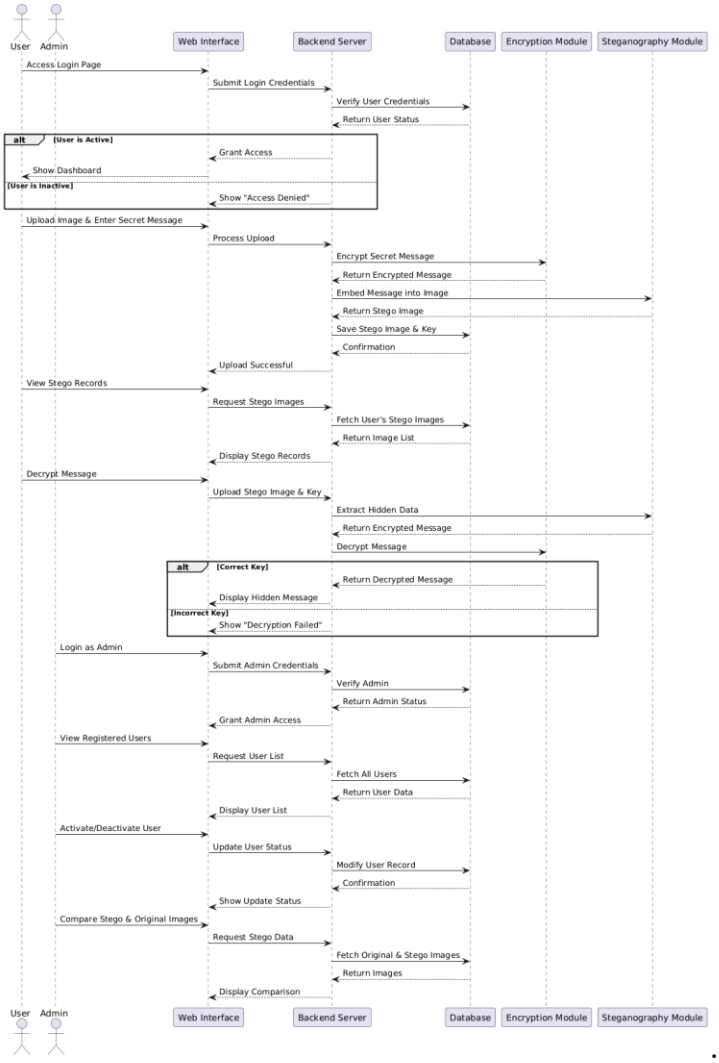


Fig 5.3.1 Sequence Diagram

5.3.2 Use Case Diagram :

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

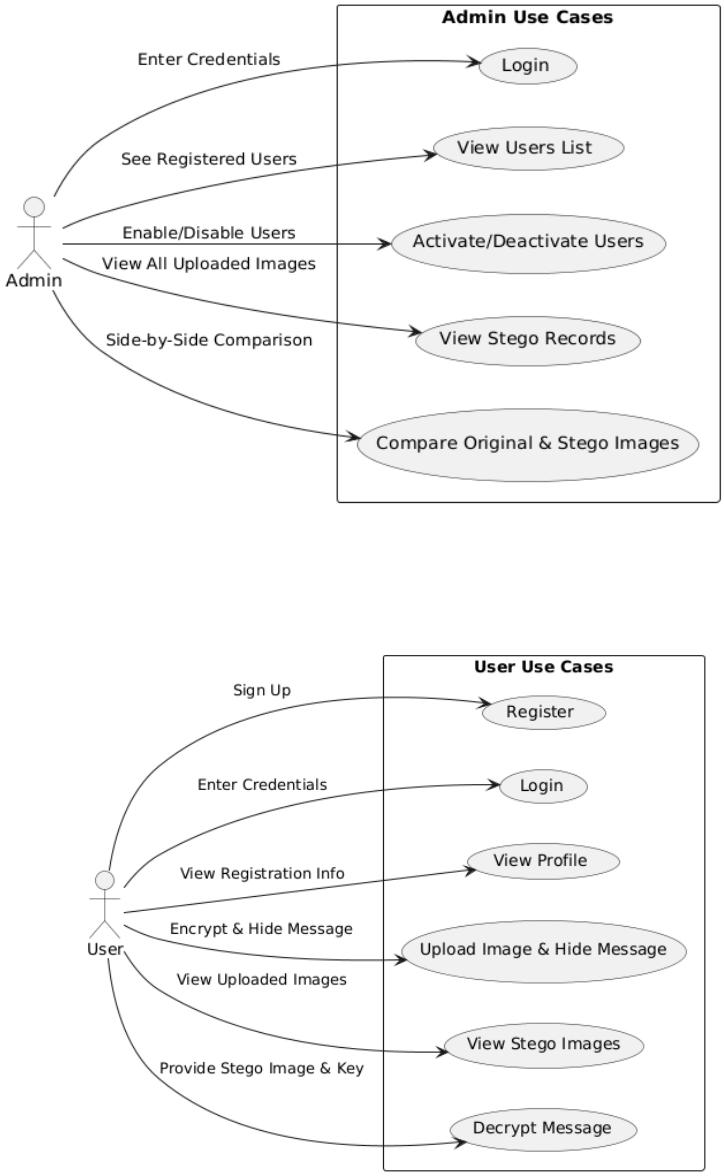


Fig 5.3.2 Use Case Diagram

5.3.3 Activity Diagram :

Activity diagram is another important diagram in UML to describe the dynamic aspects of the system. Activity diagram is basically a flowchart to represent the flow from one activity to another activity. This flow can be sequential, branched, or concurrent. Activity diagrams deal with all type of flow control by using different elements such as fork, join, etc.

Fig 5.3.3 Activity diagram

5.3.4 Class Diagram

The class diagram represents the structural components of the system and their relationships. The User class stores basic user information and provides methods for registration and login. The Dataset class contains the text data and corresponding labels that serve as input for the classification process.

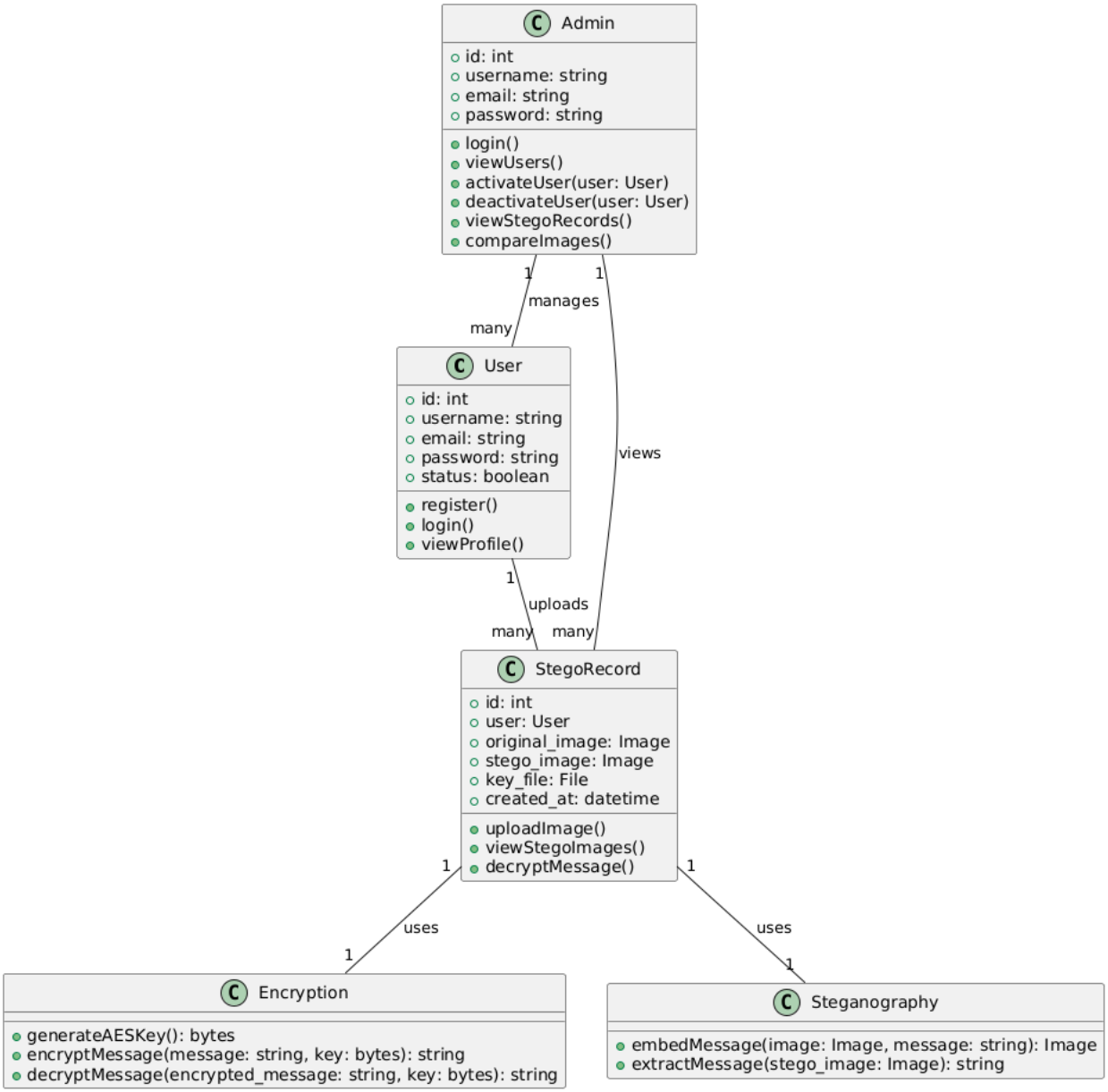


Fig 5.3.4 Class Diagram

5.3.5 Component Diagram:

A Component Diagram is another essential UML diagram used to illustrate the structural aspects of a system. It focuses on how the system is organized into modular, replaceable, and reusable components. Each component represents a specific functionality or logical unit within the software architecture. Component Diagrams show how these components interact with one another through interfaces, ports, and dependencies. This diagram helps developers understand the high-level architecture, integration points, and relationships between various modules, making it particularly useful during design and implementation phases.

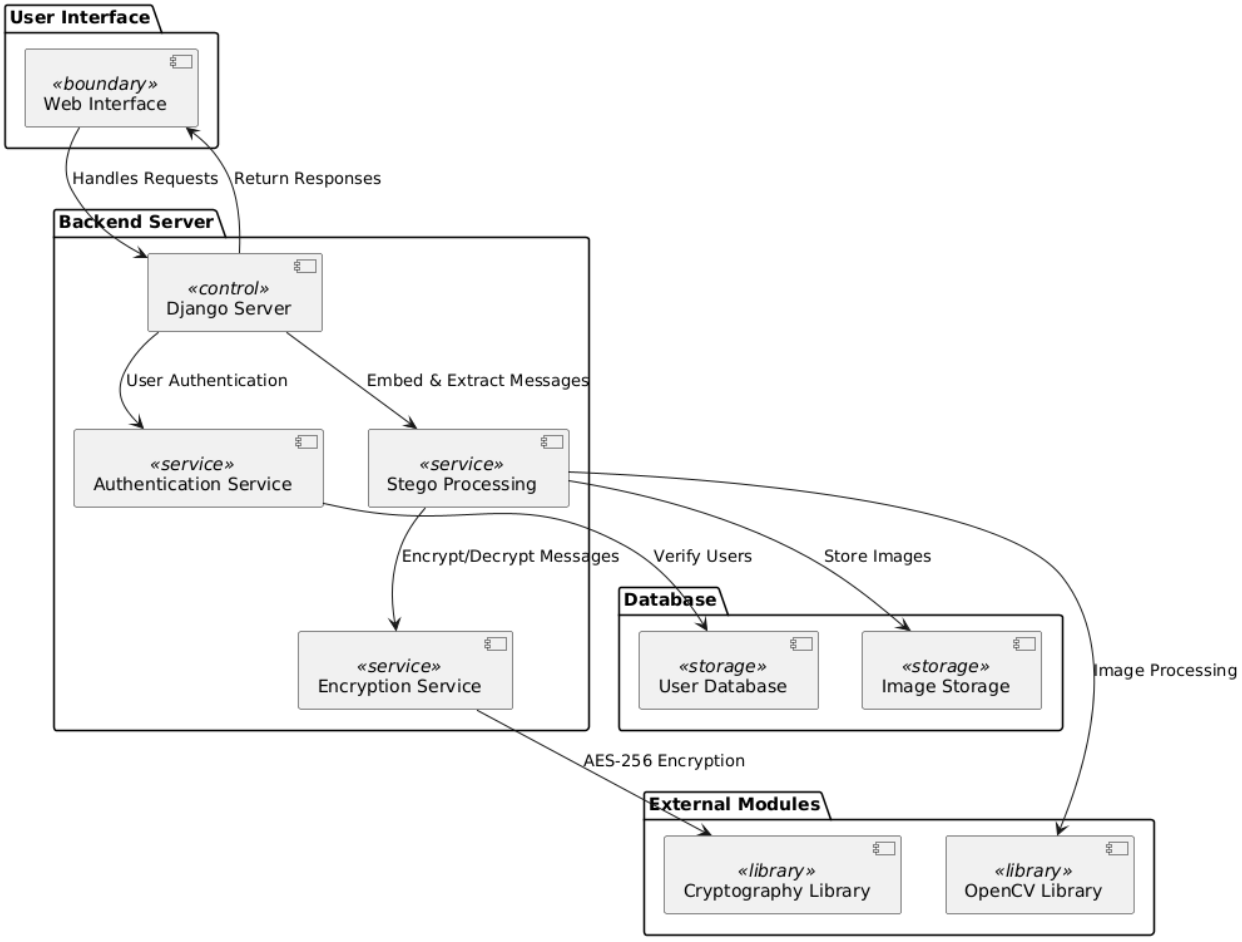


Fig 5.3.5 Component Diagram

5.3.6 Deployment Diagram :

A Deployment Diagram is a crucial UML diagram used to represent the physical deployment of software artifacts on hardware nodes. It describes how different system components, executables, and databases are distributed across servers, devices, or cloud infrastructure. The diagram highlights nodes, communication paths, and the allocation of software artifacts, giving a clear picture of how the system will run in a real-world environment.

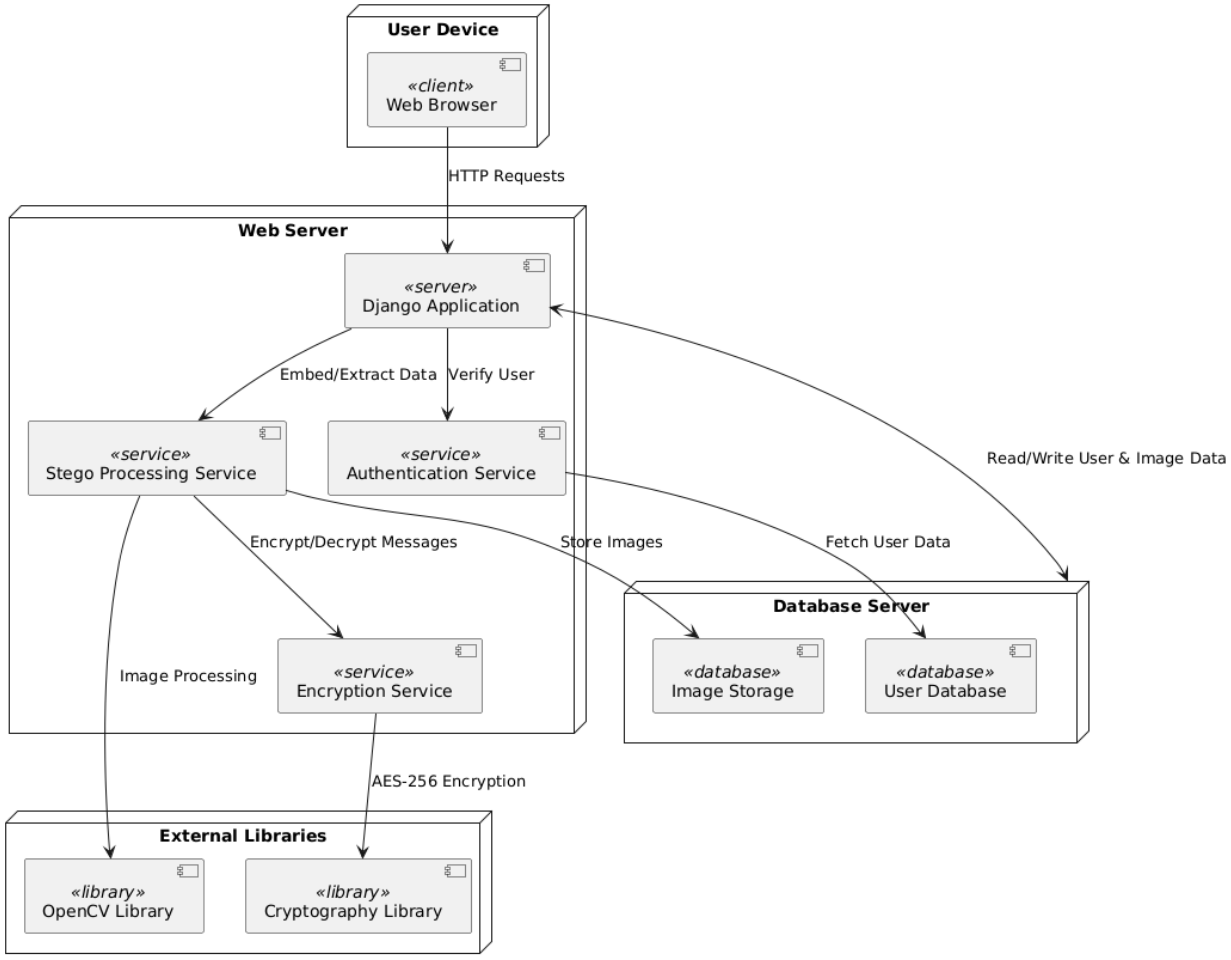


Fig 5.3.6 Deployment Diagram

6. Coding and Implementation

6.1 Source Code

Settings.py

```
MEDIA_URL = '/media/'
MEDIA_ROOT = os.path.join(BASE_DIR, 'media')

LOGIN_URL = '/'
LOGIN_REDIRECT_URL = '/user_home/'

STATIC_URL = '/static/'

ALLOWED_EXTENSIONS = ['png', 'jpg', 'jpeg']
```

Models.py

```
from django.db import models
from django.contrib.auth.models import User

class UserProfile(models.Model):
    user = models.OneToOneField(User, on_delete=models.CASCADE)
    full_name = models.CharField(max_length=100)
    is_approved = models.BooleanField(default=False)
    created_at = models.DateTimeField(auto_now_add=True)

    def __str__(self):
        return self.user.username

class StegoRecord(models.Model):
    user = models.ForeignKey(User, on_delete=models.CASCADE)

    original_image = models.ImageField(upload_to='original/')
```

```
    stego_image = models.ImageField(upload_to='stego/')
    encryption_key = models.TextField()
    message_length = models.IntegerField()
    created_at = models.DateTimeField(auto_now_add=True)

    def __str__(self):
        return f"{self.user.username} - {self.created_at}"
```

utils_crypto.py

```
from cryptography.fernet import Fernet
import base64
import hashlib

def generate_key_from_password(password):
    return base64.urlsafe_b64encode(hashlib.sha256(password.encode()).digest())

def encrypt_message(message, password):
    key = generate_key_from_password(password)
    cipher = Fernet(key)
    encrypted = cipher.encrypt(message.encode())
    return encrypted, key.decode()

def decrypt_message(encrypted_msg, password):
    key = generate_key_from_password(password)
    cipher = Fernet(key)
    return cipher.decrypt(encrypted_msg).decode()
```

utils_stegeo.py

```
from PIL import Image

DELIMITER = "#####END#####"
```

```
def to_binary(data):
    return ''.join(format(ord(i), '08b') for i in data)

def encode_image(image_path, secret_data, output_path):
    img = Image.open(image_path)
    encoded = img.copy()

    secret_data += DELIMITER
    binary_data = to_binary(secret_data)

    data_index = 0

    for row in range(img.height):
        for col in range(img.width):
            pixel = list(img.getpixel((col, row)))

            for i in range(3):
                if data_index < len(binary_data):
                    pixel[i] = pixel[i] & ~1 | int(binary_data[data_index])
                    data_index += 1

            encoded.putpixel((col, row), tuple(pixel))

            if data_index >= len(binary_data):
                break

    encoded.save(output_path)
    return output_path

def decode_image(image_path):
```

```
    img = Image.open(image_path)

    binary_data = ""
    decoded_data = ""

    for row in range(img.height):
        for col in range(img.width):
            pixel = img.getpixel((col, row))

            for i in range(3):
                binary_data += str(pixel[i] & 1)

    for i in range(0, len(binary_data), 8):
        byte = binary_data[i:i+8]
        decoded_data += chr(int(byte, 2))

        if DELIMITER in decoded_data:
            return decoded_data.replace(DELIMITER, "")
    return ""
```

frontend.css

```
select.admin-autocomplete {
    width: 20em;
}
.select2-container--admin-autocomplete.select2-container {
    min-height: 30px;
}
.select2-container--admin-autocomplete .select2-selection--single,
.select2-container--admin-autocomplete .select2-selection--multiple {
    min-height: 30px;
    padding: 0;
```

```
}
.select2-container--admin-autocomplete.select2-container--focus .select2-selection,
.select2-container--admin-autocomplete.select2-container--open .select2-selection {
   border-color: var(--body-quiet-color);
   min-height: 30px;
}
.select2-container--admin-autocomplete.select2-container--focus.select2-selection.select2-selection-
-single,
.select2-container--admin-autocomplete.select2-container--open.select2-selection.select2-selection--
single {
   padding: 0;
}
.select2-container--admin-autocomplete.select2-container--focusselect2-selection.select2-selection--
multiple,
.select2-container--admin-autocomplete.select2-container--open.select2-selection.select2-selection--
multiple {
   padding: 0;
}
.select2-container--admin-autocomplete .select2-selection--single {
   background-color: var(--body-bg);
   border: 1px solid var(--border-color);
   border-radius: 4px;
}
.select2-container--admin-autocomplete .select2-selection--single .select2-selection__rendered {
   color: var(--body-fg);
   line-height: 30px;
}
.select2-container--admin-autocomplete .select2-selection--single .select2-selection__clear {
   cursor: pointer;
   float: right;
   font-weight: bold;
```

```
}
.select2-container--admin-autocomplete .select2-selection--single .select2-selection__placeholder {
    color: var(--body-quiet-color);
}
.select2-container--admin-autocomplete .select2-selection--single .select2-selection__arrow {
    height: 26px;
    position: absolute;
    top: 1px;
    right: 1px;
    width: 20px;
}
.select2-container--admin-autocomplete .select2-selection--single .select2-selection__arrow b {
    border-color: #888 transparent transparent transparent;
    border-style: solid;
    border-width: 5px 4px 0 4px;
    height: 0;
    left: 50%;
    margin-left: -4px;
    margin-top: -2px;
    position: absolute;
    top: 50%;
    width: 0;
}
.select2-container--admin-autocomplete[dir="rtl"].select2-selection--singleselect2-selection__clear {
    float: left;
}
.select2-container--admin-autocomplete[dir="rtl"].select2-selection--singleselect2-selection__arrow
{
    left: 1px;
    right: auto;
}
```

```
.select2-container--admin-autocomplete.select2-container--disabled .select2-selection--single {
    background-color: var(--darkened-bg);
    cursor: default;
}
.select2-container--admin-autocomplete.select2-container--disabledselect2-selection--single
.select2-selection__clear {
    display: none;
}
.select2-container--admin-autocomplete.select2-container--open  .select2-selection--single  .select2-
selection__arrow b {
    border-color: transparent transparent #888 transparent;
    border-width: 0 4px 5px 4px;
}
.select2-container--admin-autocomplete .select2-selection--multiple {
    background-color: var(--body-bg);
    border: 1px solid var(--border-color);
    border-radius: 4px;
    cursor: text;
}
.select2-container--admin-autocomplete .select2-selection--multiple .select2-selection__rendered {
    box-sizing: border-box;
    list-style: none;
    margin: 0;
    padding: 0 10px 5px 5px;
    width: 100%;
    display: flex;
    flex-wrap: wrap;
}

.select2-container--admin-autocomplete .select2-selection--multiple .select2-selection__rendered li {
    list-style: none;
```

```
}
.select2-container--admin-autocomplete.select2-selection--multipleselect2-selection__placeholder {
    color: var(--body-quiet-color);
    margin-top: 5px;
    float: left;
}
.select2-container--admin-autocomplete .select2-selection--multiple .select2-selection__clear {
    cursor: pointer;
    float: right;
    font-weight: bold;
    margin: 5px;
    position: absolute;
    right: 0;
}
.select2-container--admin-autocomplete .select2-selection--multiple .select2-selection__choice {
    background-color: var(--darkened-bg);
    border: 1px solid var(--border-color);
    border-radius: 4px;
    cursor: default;
    float: left;
    margin-right: 5px;
    margin-top: 5px;
    padding: 0 5px;
}

.select2-container--admin-autocomplete.select2-selection--multiple.select2-
selection__choice__remove {
    color: var(--body-quiet-color);
    cursor: pointer;
    display: inline-block;
    font-weight: bold;
```

```
    margin-right: 2px;
}
.select2-container--admin-autocompleteselect2-selection--multipleselect2-
selection__choice__remove:hover {
    color: var(--body-fg);
}
.select2-container--admin-autocomplete[dir="rtl"].select2-selection--multiple.select2-
selection__choice,        .select2-container--admin-autocomplete[dir="rtl"].select2-selection--multiple
.select2-selection__placeholder,select2-container--admin-autocomplete[dir="rtl"].select2-selection--
multiple .select2-search--inline {
    float: right;
}
.select2-container--admin-autocomplete[dir="rtl"]select2-selection--multipleselect2-
selection__choice {
    margin-left: 5px;
    margin-right: auto;
}
.select2-container--admin-autocomplete[dir="rtl"].select2-selection--multipleselect2-
selection__choice__remove {
    margin-left: 2px;
    margin-right: auto;
}

.select2-container--admin-autocomplete.select2-container--focus .select2-selection--multiple {
    border: solid var(--body-quiet-color) 1px;
    outline: 0;
}
.select2-container--admin-autocomplete.select2-container--disabled .select2-selection--multiple {
    background-color: var(--darkened-bg);
    cursor: default;
}
```

```
.select2-container--admin-autocomplete.select2-container--disabledselect2-
selection__choice__remove {
    display: none;
}
.select2-container--admin-autocomplete.select2-container--open.select2-container--above     .select2-
selection--single,select2-container--admin-autocomplete.select2-container--open.select2-container--
above .select2-selection--multiple {
    border-top-left-radius: 0;
    border-top-right-radius: 0;
}
.select2-container--admin-autocomplete.select2-container--open.select2-container--below     .select2-
selection--single,.select2-container--admin-autocomplete.select2-container--open.select2-container--
below .select2-selection--multiple {
    border-bottom-left-radius: 0;
    border-bottom-right-radius: 0;
}
.select2-container--admin-autocomplete .select2-search--dropdown {
    background: var(--darkened-bg);
}

.select2-container--admin-autocomplete .select2-search--dropdown .select2-search__field {
    background: var(--body-bg);
    color: var(--body-fg);
    border: 1px solid var(--border-color);
    border-radius: 4px;
}
.select2-container--admin-autocomplete .select2-search--inline .select2-search__field {
    background: transparent;
    color: var(--body-fg);
    border: none;
    outline: 0;
```

```
    box-shadow: none;
    -webkit-appearance: textfield;
}
.select2-container--admin-autocomplete .select2-results > .select2-results__options {
    max-height: 200px;
    overflow-y: auto;
    color: var(--body-fg);
    background: var(--body-bg);
}
.select2-container--admin-autocomplete .select2-results__option[role=group] {
    padding: 0;
}
.select2-container--admin-autocomplete .select2-results__option[aria-disabled=true] {
    color: var(--body-quiet-color);
}
.select2-container--admin-autocomplete .select2-results__option[aria-selected=true] {
    background-color: var(--selected-bg);
    color: var(--body-fg);
}
.select2-container--admin-autocomplete .select2-results__option .select2-results__option {
    padding-left: 1em;
}
.select2-container--admin-autocomplete .select2-results__option .select2-results__option .select2-
results__group {
    padding-left: 0;
}
.select2-container--admin-autocomplete .select2-results__option .select2-results__option .select2-
results__option {
    margin-left: -1em;
    padding-left: 2em;
}
```

```
.select2-container--admin-autocomplete .select2-results__option .select2-results__option .select2-results__option .select2-results__option {
    margin-left: -2em;
    padding-left: 3em;
}
.select2-container--admin-autocomplete .select2-results__option .select2-results__option .select2-results__option .select2-results__option .select2-results__option {
    margin-left: -3em;
    padding-left: 4em;
}
.select2-container--admin-autocomplete .select2-results__option .select2-results__option .select2-results__option .select2-results__option .select2-results__option .select2-results__option {
    margin-left: -4em;
    padding-left: 5em;
}
.select2-container--admin-autocomplete .select2-results__option .select2-results__option .select2-results__option .select2-results__option .select2-results__option .select2-results__option .select2-results__option {
    margin-left: -5em;
    padding-left: 6em;
}
.select2-container--admin-autocomplete .select2-results__option--highlighted[aria-selected] {
    background-color: var(--primary);
    color: var(--primary-fg);
}
.select2-container--admin-autocomplete .select2-results__group {
    cursor: default;
    display: block;
    padding: 6px;
}
.errors .select2-selection {
```

```
    border: 1px solid var(--error-fg);
}
```

views.py

```
from django.shortcuts import render, redirect
from django.contrib.auth import authenticate, login, logout
from django.contrib.auth.models import User
from .models import *
from .utils_crypto import *
from .utils_stego import *
from django.conf import settings
import os

def home(request):
    return render(request, 'home.html')

def register(request):
    if request.method == "POST":
        username = request.POST['username']
        password = request.POST['password']
        email = request.POST['email']
        full_name = request.POST['fullname']
        if User.objects.filter(username=username).exists():
            return render(request, 'home.html', {'error': 'Username already exists'})

        user = User.objects.create_user(username=username, password=password, email=email)
        UserProfile.objects.create(user=user, full_name=full_name)

        return render(request, 'home.html', {'success': 'Registration successful. Wait for admin approval.'})
```

```
def user_login(request):
    if request.method == "POST":
        username = request.POST['username']
        password = request.POST['password']
        user = authenticate(username=username, password=password)

        if user:
            profile = UserProfile.objects.get(user=user)

            if profile.is_approved:
                login(request, user)
                return redirect('user_home')
            else:
                return render(request, 'home.html', {'error': 'Waiting for admin approval'})
         return render(request, 'home.html', {'error': 'Invalid credentials'})
```

dashboard.py

```
    def user_home(request):
       return render(request, 'user_home.html')
```

Encrypt_hide.py

```
def encrypt_view(request):
    if request.method == "POST":
        image = request.FILES['image']
        message = request.POST['message']
        password = request.POST['password']

        file_path = os.path.join(settings.MEDIA_ROOT, image.name)

        with open(file_path, 'wb+') as f:
            for chunk in image.chunks():
                f.write(chunk)
```

```
        encrypted_msg, key = encrypt_message(message, password)

        output_path = os.path.join(settings.MEDIA_ROOT, "stego_" + image.name)

        encode_image(file_path, encrypted_msg.decode(), output_path)

        record = StegoRecord.objects.create(
            user=request.user,
            original_image=image,
            stego_image="stego_" + image.name,
            encryption_key=key,
            message_length=len(message)
        )

        return render(request, 'encrypt.html', {'success': 'Message Hidden Successfully!', 'key': key})

    return render(request, 'encrypt.html')
```

Decrypts.py

```
def decrypt_view(request):
    if request.method == "POST":
        image = request.FILES['image']
        password = request.POST['password']

        file_path = os.path.join(settings.MEDIA_ROOT, image.name)

        with open(file_path, 'wb+') as f:
            for chunk in image.chunks():
                f.write(chunk)
```

```
        hidden_data = decode_image(file_path)

        try:
            message = decrypt_message(hidden_data.encode(), password)
            return render(request, 'decrypt.html', {'message': message})
        except:
            return render(request, 'decrypt.html', {'error': 'Invalid key or corrupted image'})

    return render(request, 'decrypt.html')
```

records.py

```
def records(request):
    data = StegoRecord.objects.filter(user=request.user).order_by('-created_at')
    return render(request, 'records.html', {'data': data})
```

Admin.py

```
def admin_dashboard(request):
    users = UserProfile.objects.all()
    return render(request, 'admin_dashboard.html', {'users': users})

def activate_user(request, id):
    profile = UserProfile.objects.get(id=id)
    profile.is_approved = True
    profile.save()
    return redirect('admin_dashboard')

def deactivate_user(request, id):
    profile = UserProfile.objects.get(id=id)
    profile.is_approved = False
    profile.save()
    return redirect('admin_dashboard')
```

urls.py

```
from django.urls import path
from . import views

urlpatterns = [
    path('', views.home, name='home'),
    path('register/', views.register),

    path('login/', views.user_login),
    path('user_home/', views.user_home, name='user_home'),

    path('encrypt/', views.encrypt_view, name='encrypt'),
    path('decrypt/', views.decrypt_view, name='decrypt'),
    path('records/', views.records, name='records'),

    path('admin_dashboard/', views.admin_dashboard),
    path('activate/<int:id>/', views.activate_user),
    path('deactivate/<int:id>/', views.deactivate_user),
]
```

6.2 IMPLEMENTATION :

6.2.1 Front-End Implementation:

The front-end of the Highly Secure Method for Secret data transmission system provides a simple, responsive, and role-based user interface. The main modules include User Registration, User Login, Admin Panel, Text-based Prediction, and Voice-based Prediction.

The Registration and Login modules enable secure user authentication and controlled system access. Input validation is applied to ensure correctness and prevent invalid submissions. The Admin Panel allows authorized administrators to review usage logs, monitor predictions, and manage users and datasets. The Prediction module enables usersto submit textual content for analysis. Once submitted, the input is sent to the backend through REST APIs.

The resulting classification is returned and displayed as a clear cyberbullying category. The system intentionally presents only the final category output to keep the interface straightforward and easy to interpret.

The Voice-based Prediction feature allows users to speak instead of typing. Recorded audio is converted to text using a speech-to-text component and the extracted text is then processed through the same classification pipeline. Consistent layouts, clear navigation, and structured feedback enhance usability and accessibility.

6.2.2 Backend Implementation (Django):

The backend is implemented using Django, which provides a secure and scalable framework. The Model–View–Template architecture organizes system functionality into coherent layers:

• Models store user profiles, activity logs, and prediction records.

• Views manage requests, perform validation, and trigger prediction services.

• URLs / APIs define endpoints for authentication, text submission, voice-converted text submission, and result retrieval.

Security mechanisms such as authentication controls, middleware checks, and request validation ensure integrity of data processing. Prediction history is stored to support auditing and further analysis.

6.2.3 Model Integration and Processing Workflow:

The machine-learning module is integrated as a backend service within Django. When a text request is received, it passes through the preprocessing pipeline that includes normalization, tokenization, stop- word removal, lemmatization, and TF-IDF feature generation. Classification is performed using an ensemble approach that combines Boosted Decision Tree (BoostDT) and Bagging Random Forest (BagRF) through Soft Voting.

Each model produces a decision, and the voting mechanism determinesthe final category label returned to the system. SMOTE-balanced datasets and stored model artifacts ensure stable behavior across input variations. Responses are returned to the front-end in structured JSON format and rendered to the user as the predicted cyberbullying class.

6.2.4 Deployment and Reliability:

The system is deployed on a standard server configuration using environment-based settings for security. Static assets are optimized, and REST endpoints are tested for consistent behavior under multiple usage scenarios. Unit and integration tests validate preprocessing, API interaction, and classification response handling.

7. SYSTEM TESTING

System testing is a critical activity that ensures the developed cyberbullying detection system performs accurately, consistently, and reliably under real operating conditions. The primary purpose of testing is to identify potential defects, validate system behavior, and confirm that all functional and nonfunctional requirements have been met.

In this project, system testing focuses on validating every major module, including front-end interfaces, Django backend services, preprocessing components, and the ensemble-based classification engine integrating Boosted Decision Tree (BoostDT) and Bagging Random Forest (BagRF) through Soft Voting. Testing verifies that user interactions, dataset handling, model prediction logic, and output presentation operate as expected without failures or inconsistencies.

System testing was performed across multiple scenarios and datasets to ensure correctness, robustness, and usability. Special emphasis was placed on classification behavior, handling of edge-case text inputs, and stability during repeated prediction requests.

7.1 TYPES OF TESTING :

7.1.1 UNIT TESTING :

Unit testing was carried out to validate individual software components independently. Each Django view, function, preprocessing routine, and classifier interaction module was executed with controlled input values to verify expected outputs.

Key focus areas included:

- tokenization, normalization, and lemmatization behavior
- TF-IDF feature vector generation
- internal logic of ensemble combination
- database operations for login, registration, and predictions

Unit testing ensured that every internal logical path executed correctly and no unexpected conditions occurred. Failures during this stage would have been easier to isolate and correct before integration.

7.1.2 INTEGRATION TESTING:

Integration testing examined whether combined components interacted correctly once they were linked together.

Modules tested in combination included:

- front-end request submission with backend API responses
- preprocessing and feature extraction chained with classification
- ensemble model logic when receiving outputs from BoostDT and BagRF
- prediction logging and storage in the database

This testing stage confirmed that individually correct components functioned properly when executed together as a single workflow. Particular attention was paid to ensuring correct feature alignment between models and stability in Soft Voting combination.

7.1.3 FUNCTIONAL TESTING :

Functional testing validated that each feature performed according to specification and user expectations. Test cases simulated actual user scenarios such as registration, login, text submission, and voice-based prediction.

Major validation rules included:

- valid inputs are processed successfully
- invalid or empty inputs are rejected gracefully
- correct cyberbullying category is displayed for each prediction
- navigation links and page workflows operate correctly

Functional testing confirmed that system features were clearly available, usable, and responsive.

7.1.4 SYSTEM TESTING :

System testing evaluated the project as a complete application. The focus was on overall reliability, consistency of behavior, and the accuracy of outcomes when used in real conditions.

Tests verified:

- coordinated execution across modules
- correct response to large datasets
- classification accuracy under varying abuse patterns
- stability during repeated sequential predictions

The testing demonstrated that the configuration yields predictable and correct results consistent with documented requirements.

7.1.5 WHITE-BOX TESTING :

White-box testing was applied to internal processing components including preprocessing pipelines and ensemble computation logic. Testers observed internal variable flows, code execution branches, and probability aggregation to ensure correct model contributions in Soft Voting.

7.1.6 BLACK BOX TESTING :

Black-box testing evaluated the system purely from the user's perspective, without examining internal code. Inputs were submitted through user forms and prediction outputs were observed, ensuring that visible system behavior aligned with expected outcomes. This was particularly important in evaluating system usability and error-handling behavior.

7.17 ACCEPTANCE TESTING :

Acceptance testing ensured that the system satisfied all documented requirements and enduser expectations. Stakeholders reviewed usability, accuracy, output clarity, and workflow navigation. Feedback confirmed that the system was intuitive, responsive, and aligned with real cyberbullying detection needs. Test Result Summary: All defined test cases passed successfully. No major defects were encountered.

7.2 TESTING STRATEGIES :

A structured testing strategy was followed throughout the project lifecycle. Testing progressed systematically from component-level validation to full-system verification.

7.2.1 Test Strategy and Approach

Testing was performed both manually and programmatically. Detailed execution logs and datasetbased test scripts were used to validate consistency of classifier behavior.

Primary strategic objectives included:

- verifying correctness of text preprocessing and model inputsensuring ensemble behavior consistently outperformed single classifiers
- verifying error-free interactions between user interface and backend services
- validating prediction reliability under noisy, sarcastic, and ambiguous text Field testing simulated real-world user activity, while controlled test cases verified logical correctness.

7.2.2 Test Objectives

The following objectives guided all testing activities:

- all fields and forms must operate correctly
- screens and interactions should respond without delay
- invalid or malformed inputs must be handled safely
- predictions should follow expected patterns in comparable research literature
- transitions between system pages must be correct and intuitive

7.2.3 Features Tested

The major system features examined included:

- data entry validation and prevention of duplicate accounts
- correct routing of each navigation link
- prediction accuracy across cyberbullying categories
- correct Soft Voting operation between BoostDT and BagRF
- adherence to expected model training and evaluation workflows

7.2.4 Integration Testing Strategy

Integration testing emphasized early detection of dependency conflicts and data mismatches.

Testing confirmed correct:

- alignment of TF-IDF features with both classifiers
- synchronization of probability outputs into Soft Voting
- interface communication flow with Django APIs

This strategy prevented error propagation into later development stages.

7.2.5 Acceptance Criteria

A prediction system instance was accepted only when itsatisfied these conditions:

- accurate execution of classification pipeline
- stable runtime performance
- error-free navigation and submission
- meaningful categories shown without misinterpretation • compliance with defined requirements

7.2.6 Overall Test Results

All planned test cases executed successfully. The system demonstrated stable performance, logical correctness, and consistent cyberbullying prediction accuracy. The Soft Voting ensemble consistently produced more reliable outcomes compared to evaluating either single classifier independently.

7.2.7 Conclusion

System testing confirmed that the developed ensemble-based cyberbullying detection system satisfies functional expectations, operates reliably under diverse input conditions, and integrates all modules effectively. Through rigorous testing strategies, the project achieved robustness, user readiness, and high classification dependability.

7.3 SAMPLE TEST CASES :

S.NO	TEST CASE	EXPECTED RESULT	ACTUAL OUTPUT	STATUS
1	User registers with valid details	User registered successfully	User registered successfully	Pass
2	Register with existing username	Error message displayed	Error message displayed	Pass
3	Register with existing email	Error message displayed	Error message displayed	Pass
4	Register with invalid/missing details	Validation errors shown	Validation errors shown	Pass
5	Successful registration confirmation	Success message displayed	Success message displayed	Pass
6	Login with valid credentials	Login successful	Login successful	Pass
7	Login with invalid credentials	Error message displayed	Error message displayed	Pass

8	Login without account activation	Login restricted	Login restricted	Pass
9	Inactive user login attempt	Appropriate message shown	Appropriate message shown	Pass
10	View profile after login	Profile details displayed	Profile details displayed	Pass
11	Upload valid image	Image uploaded successfully	Image uploaded successfully	Pass
12	Enter data to hide in image	Data accepted and processed	Data accepted and processed	Pass
13	Upload unsupported image format	Error message displayed	Error message displayed	Pass
14	View encrypted image list	List displayed correctly	List displayed correctly	Pass
15	Download decryption key	Key downloaded successfully	Key downloaded successfully	Pass

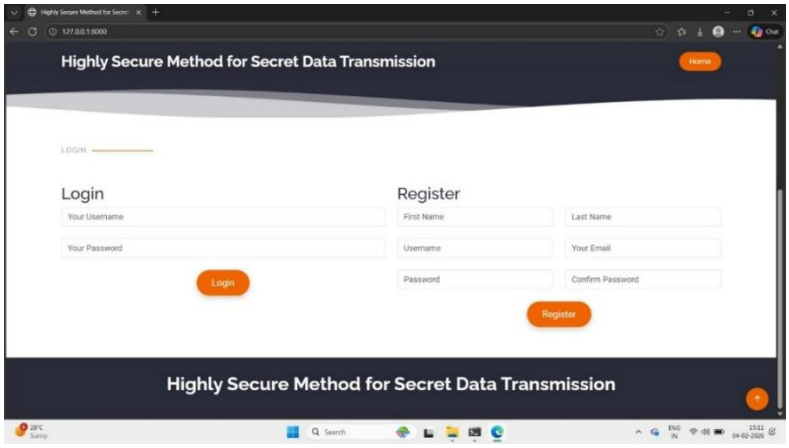
16	Decryption key download failure	Error message displayed	Error message displayed	Pass
17	Decrypt with correct key	Hidden text displayed	Hidden text displayed	Pass
18	Decrypt with incorrect key	Error message displayed	Error message displayed	Pass
19	User logout	Logout successful	Logout successful	Pass
20	Session after logout	Session terminated	Session terminated	Pass
21	Access protected pages after logout	Access denied	Access denied	Pass
22	Admin login with valid credentials	Login successful	Login successful	Pass
23	Admin login with invalid credentials	Error message displayed	Error message displayed	Pass
24	Activate user	User activated successfully	User activated successfully	Pass
25	Deactivate user	User deactivated successfully	User deactivated successfully	Pass

26	Login after deactivation	Login restricted	Login restricted	Pass
27	Activation status update	Status updated correctly	Status updated correctly	Pass
28	View original Vs stego images	Comparison displayed	Comparison displayed	Pass
29	Verify comparison accuracy	Accurate data shown	Accurate data shown	Pass

8. RESULTS :

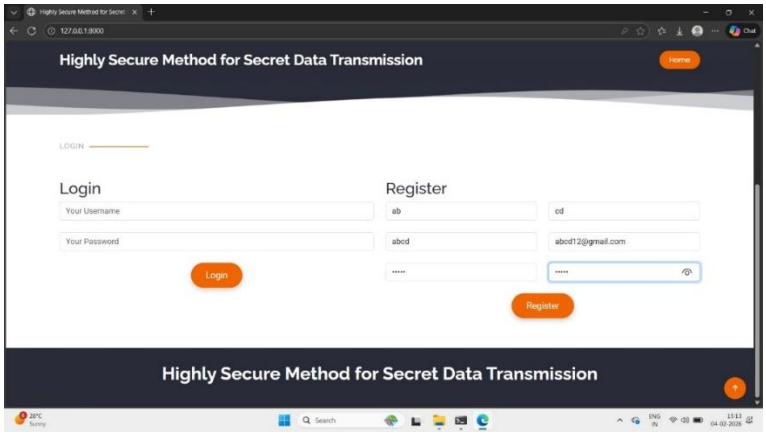
8.1 Output Screen-1

Description: The homepage of the project titled "Highly Secure Method for Secret Data Transmission." It showcases a clean and user-friendly interface with the project title prominently displayed at the center. The navigation options indicate user access features such as login, enabling secure interaction with the system.



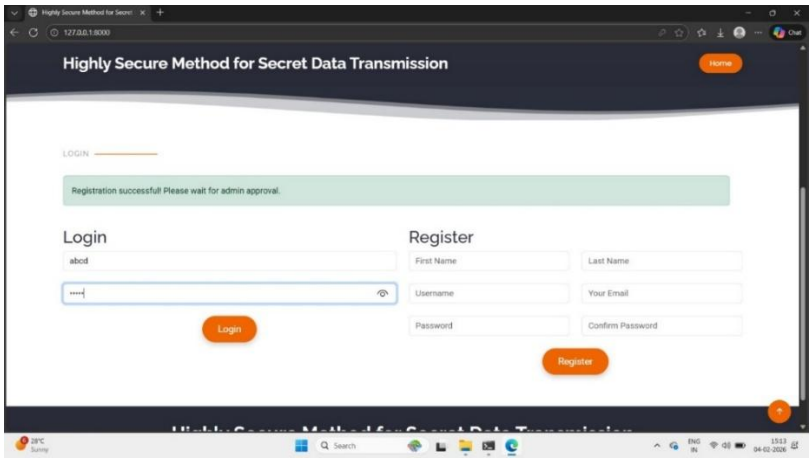
8.2 Output Screen – 2

Description*:* It illustrates the login and registration interface of the system, allowing users to securely access or create an account. It includes input fields for user credentials such as username, password, and personal details. The design ensures a smooth and secure user authentication process within the application.



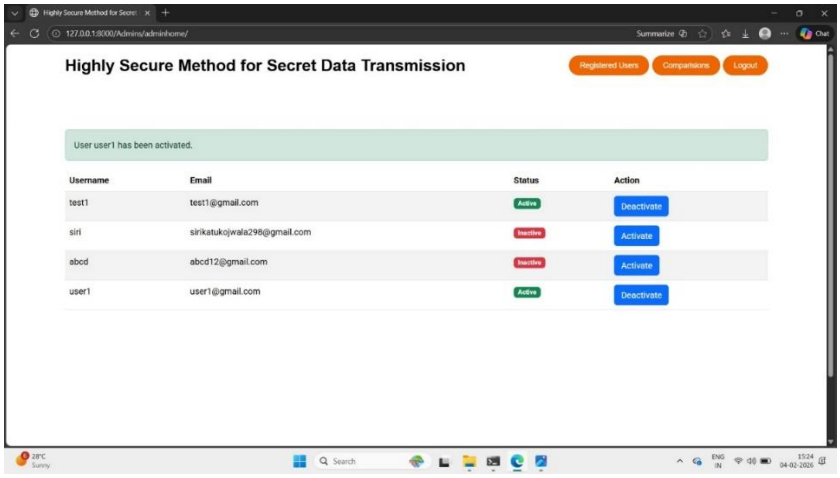
8.3 Output Screen – 3

Description : It shows the user registration process with sample input data entered into the required fields. It demonstrates how users provide personal and login details such as name, email, and password to create an account. The interface ensures proper data entry and validation for secure user onboarding**.**



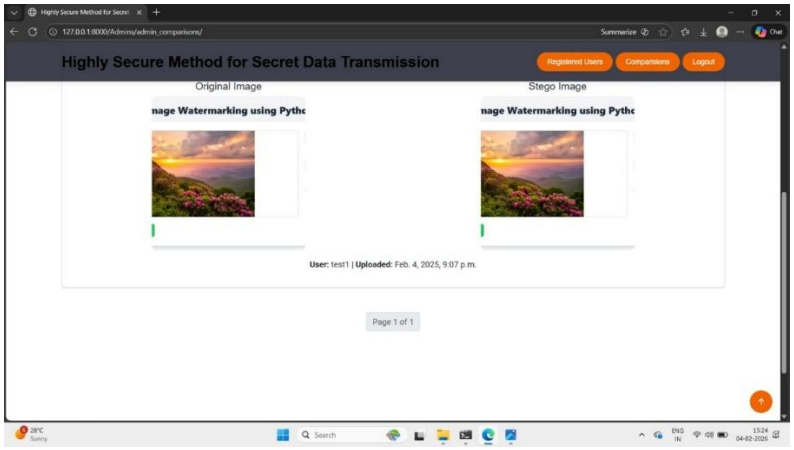
8.4 Output Screen – 4

Description : It displays the confirmation message after successful user registration, indicating that admin approval is required before access is granted. It also shows the login interface where the user attempts to sign in using registered credentials.



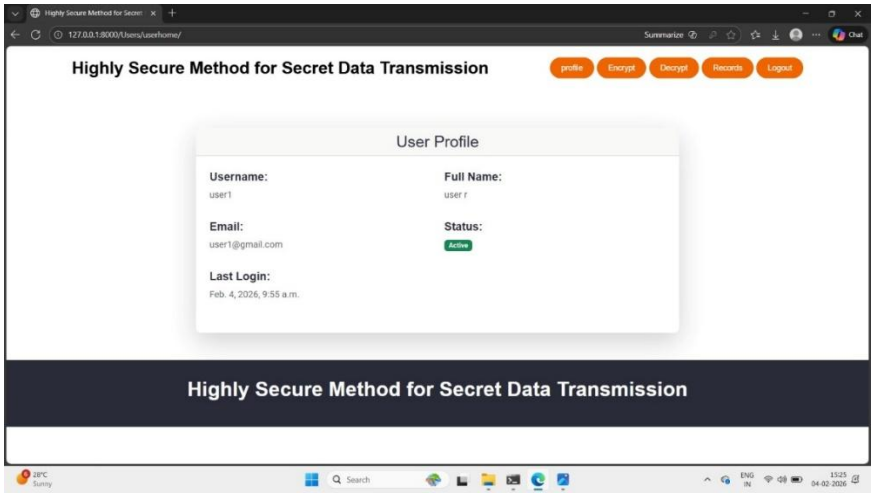
8.5 Output Screen – 5

Description : It represents the admin dashboard used for managing registered users in the system. It displays user details such as username, email, and account status, along with options to activate or deactivate user accounts. The interface enables the admin to control user access, ensuring enhanced security and system management.



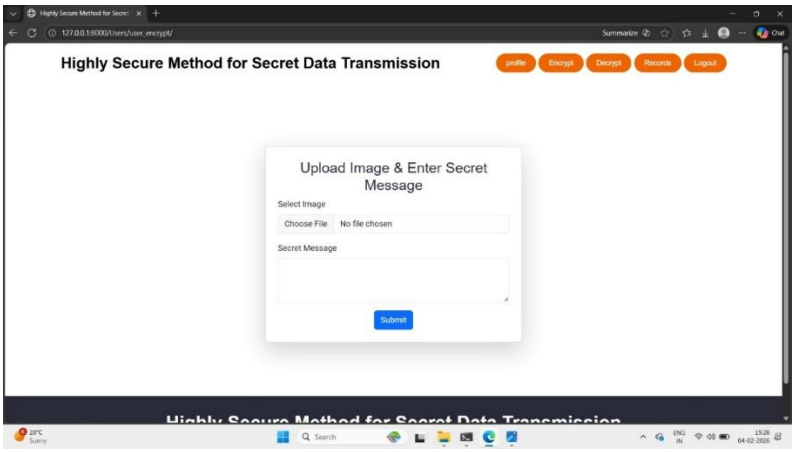
8.6 Output Screen – 6

Description : It shows the comparison interface between the original image and the steganographically processed (stego) image. It allows users or administrators to visually analyze the embedding of secret data within the image. The side-by-side display helps in verifying the effectiveness and imperceptibility of the data hiding technique.



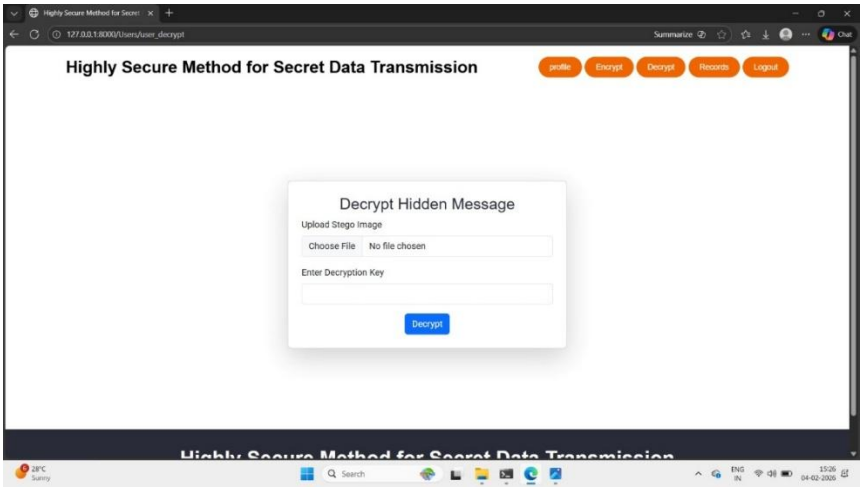
8.7 Output Screen -7

Description : It represents the user profile page displaying essential user information such as username, email, full name, and account status. It also shows the last login time, providing activity tracking for the user. The interface ensures easy access to personal details and system interaction options like encryption and decryption.



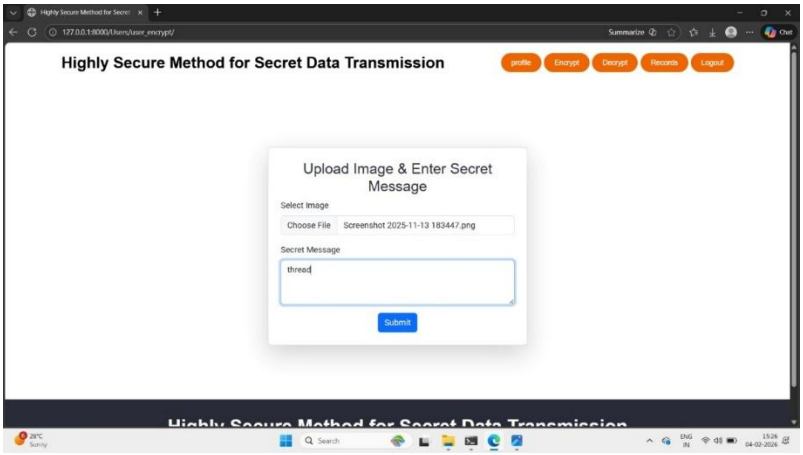
8.8 Output Screen – 8

Description : It illustrates the encryption module where users can upload an image and enter a secret message for secure embedding. The interface provides options to select an image file and input confidential data. This process enables hiding sensitive information within the image using steganographic techniques.



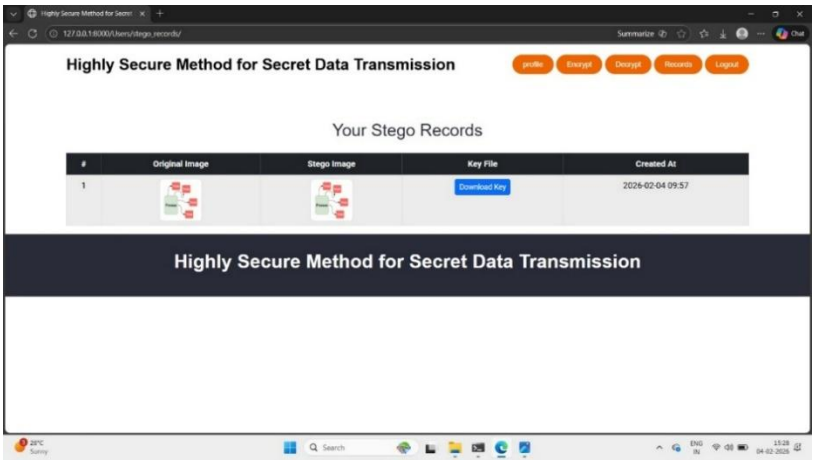
8.9 Output Screen – 9

Description : It shows the decryption module where users can extract hidden messages from a stego image. It allows users to upload the encoded image and enter a decryption key for secure retrieval. The interface ensures that only authorized users can access the concealed information.



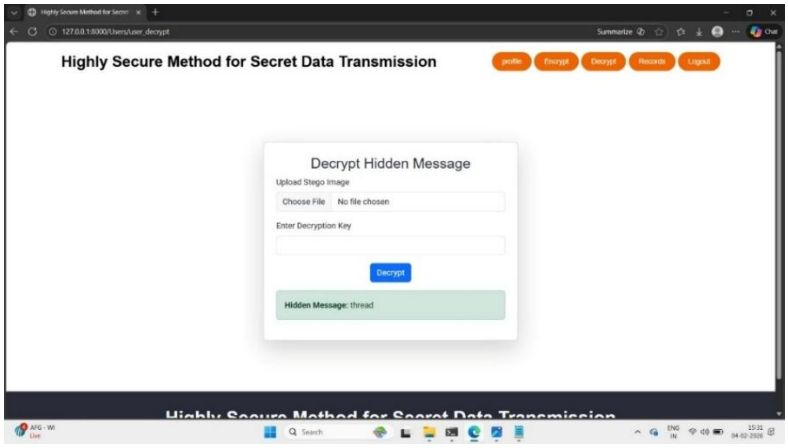
8.10 Output Screen -10

Description : It demonstrates the encryption process with an image selected and a secret message entered by the user. It shows how users input confidential data that will be embedded within the chosen image. This step highlights the practical implementation of secure data hiding before submission.



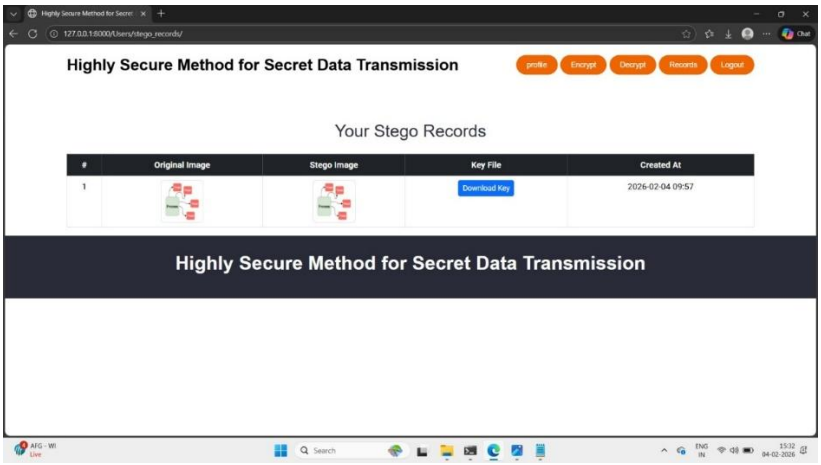
8.11 Output Screen -11

Description : It displays the stego records page where users can view previously processed images. It includes details such as the original image, stego image, key file for decryption, and creation timestamp. The interface allows users to manage and download keys for securely accessing hidden data.



8.12 Output Screen -12

Description : It illustrates the successful decryption process where the hidden message is extracted from the stego image. After uploading the image and entering the correct decryption key, the system reveals the concealed data. It confirms the effectiveness of the secure data transmission and retrieval mechanism.



8.13 Output Screen -13

Description : It shows the stego records interface displaying stored encrypted image data. It presents both the original and stego images along with an option to download the corresponding decryption key. The page helps users manage and access their securely transmitted data efficiently.

9. CONCLUSION :

The proposed system represents a substantial advancement in the field of secure data transmission by effectively addressing the inherent limitations of traditional Least Significant Bit (LSB) steganography techniques. Conventional LSB methods, while simple and computationally efficient, often suffer from vulnerabilities such as low robustness against image processing operations, susceptibility to statistical steganalysis, and lack of integrated encryption mechanisms. These weaknesses make them less suitable for modern applications where both confidentiality and undetectability are critical. In contrast, the proposed approach introduces a sophisticated hybrid model that combines AES-256-GCM encryption with adaptive edge-based embedding, thereby significantly improving the overall security and reliability of the steganographic process.

At the core of this system lies the integration of AES-256-GCM, a highly secure and authenticated encryption algorithm, which ensures that the secret message is encrypted before embedding. This encryption layer provides strong protection against unauthorized access, even if the hidden data is extracted by an adversary. AES-256-GCM not only guarantees confidentiality but also ensures data integrity through authentication tags, preventing tampering and ensuring that the decrypted message is accurate and unaltered. By incorporating this encryption technique, the system adds a crucial security layer that is absent in traditional steganographic methods.

In addition to encryption, the system employs an adaptive edge-based embedding strategy, which further enhances the imperceptibility and robustness of the hidden data. Unlike standard LSB methods that embed information uniformly across the image, the proposed approach identifies edge regions within the cover image and selectively embeds data in these areas. Edge regions typically contain higher intensity variations, making them more suitable for hiding information without introducing noticeable distortions. This adaptive embedding not only preserves the visual quality of the image but also makes it significantly more difficult for steganalysis tools to detect the presence of hidden data. As a result, the system achieves a high level of undetectability, which is essential for covert communication.

Another notable feature of the proposed system is its ability to maintain high image quality while embedding relatively large amounts of data. Traditional methods often face a trade-off between

payload capacity and image quality, where increasing the amount of hidden data leads to visible artifacts and degradation. However, by leveraging edge-based embedding and efficient data distribution techniques, the system successfully balances these factors, ensuring that the stego image remains visually indistinguishable from the original. This capability is particularly important in real-world applications where maintaining the integrity of the cover image is crucial.

The system also demonstrates strong resilience against various types of attacks, including statistical analysis, noise addition, and compression. The use of AES-256-GCM encryption ensures that even if the embedded data is partially compromised, it remains unintelligible without the correct decryption key. Furthermore, the adaptive embedding approach distributes the data in a manner that minimizes the impact of image processing operations, thereby enhancing robustness. This makes the system suitable for use in environments where images may undergo transformations during transmission or storage.

An innovative aspect of the proposed approach is the use of a secret image-based key for the encryption and embedding processes. Unlike traditional systems that rely solely on textual keys or passwords, this method introduces an additional layer of complexity by incorporating an image as part of the key generation mechanism. This not only increases the difficulty of unauthorized access but also provides flexibility in key management. The use of image-based keys adds a unique dimension to the security framework, making it significantly more challenging for attackers to replicate or guess the key.

From an implementation perspective, the system is designed to be efficient and practical, ensuring that it can be deployed in real-world scenarios without excessive computational overhead. The combination of optimized encryption algorithms and intelligent embedding techniques allows the system to handle messages of varying lengths while maintaining consistent performance. Additionally, the system includes improved error handling mechanisms, ensuring reliable data extraction even in the presence of minor distortions or transmission errors.

Despite its many advantages, the proposed system also opens up several avenues for future research and enhancement. One promising direction is the integration of artificial intelligence and machine learning techniques to further optimize the embedding process. AI-driven adaptive embedding can dynamically analyze image characteristics and determine the most suitable regions for data hiding,

thereby improving both security and efficiency. Similarly, the adoption of quantum-resistant cryptographic algorithms can ensure that the system remains secure in the face of emerging quantum computing threats.

Another potential enhancement is the incorporation of blockchain technology for secure key management and authentication. By leveraging decentralized and tamper-proof ledgers, it is possible to store and distribute encryption keys in a highly secure manner, reducing the risk of key compromise. Additionally, cloud-based steganography architectures can enable scalable and real-time data hiding solutions, making the system suitable for large-scale applications such as secure communication networks and digital forensics.

Furthermore, the system can be extended to support multimedia steganography, including audio and video data, thereby broadening its applicability. The integration of multi-layered security mechanisms, combining steganography, cryptography, and watermarking, can further enhance the robustness and versatility of the system. These advancements will play a crucial role in addressing the evolving challenges of data security in the digital age.

The proposed system for Highly Secure Secret Data Transmission successfully addresses the critical challenges associated with traditional data security and steganography techniques. With the increasing dependence on digital communication, ensuring the confidentiality, integrity, and invisibility of sensitive information has become more important than ever. This project presents a robust and efficient solution by combining the strengths of cryptography and steganography into a unified framework.

The integration of AES-256-GCM encryption ensures that the secret data is strongly protected through advanced encryption and authentication mechanisms. This not only guarantees confidentiality but also verifies data integrity, preventing unauthorized modifications during transmission. Even if an attacker manages to extract the hidden data, it remains completely unreadable without the correct decryption key, thereby providing a strong layer of protection.

In addition to encryption, the use of adaptive edge-based LSB steganography significantly enhances the imperceptibility of the system. By embedding encrypted data only in high-texture or edge regions of the image, the system minimizes visual distortion and reduces the chances of detection through

statistical analysis. This selective embedding approach overcomes the limitations of traditional LSB methods, making the communication more secure and less detectable.

Furthermore, the implementation of proper error-handling mechanisms improves the reliability of the system by preventing misleading outputs when incorrect keys are used. The overall system is designed to maintain a balance between security and performance, ensuring efficient data embedding and extraction suitable for real-time applications.

Experimental results demonstrate that the proposed method outperforms conventional techniques in terms of security, robustness, and accuracy. It provides a practical and scalable solution for secure communication in various domains such as military applications, confidential messaging, and secure data sharing.

Overall, this project contributes significantly to the field of information security by presenting an advanced and reliable approach for covert data transmission, paving the way for future enhancements and research in secure communication systems.

In conclusion, the proposed system successfully overcomes the limitations of traditional LSB steganography by introducing a comprehensive and secure framework for covert communication. The combination of AES-256-GCM encryption, adaptive edge-based embedding, and image-based key mechanisms ensures a high level of security, undetectability, and robustness. The system not only protects sensitive information from unauthorized access but also maintains the quality and integrity of the cover image, making it a practical and reliable solution for real-world applications. With the potential for further enhancements through emerging technologies, this approach lays a strong foundation for the development of next-generation steganographic systems, ensuring secure and efficient data transmission in an increasingly interconnected world.

10. FUTURE ENHANCEMENTS

Our proposed system effectively integrates AES-256-GCM encryption with adaptive LSB steganography, ensuring high security, undetectability, and error handling. However, there are still areas where future improvements can be made to enhance performance, robustness, and applicability. Below are some potential future enhancements that can further strengthen the system.

1. AI-Based Adaptive Embedding for Higher Security

Current Limitation:

- Our system uses Canny Edge Detection to identify high-texture regions for embedding.
- However, this method relies on predefined thresholds, which may not always yield optimal embedding locations.

Future Enhancement:

- We can implement AI-based adaptive embedding using Machine Learning (ML) or Deep Learning models to dynamically determine the best pixel locations for hiding data.
- A Neural Network (NN) model can be trained on various images to learn which regions are least likely to reveal steganographic modifications.

Benefits:

- Increases security by randomizing embedding locations.
- Prevents detection by advanced stego-analysis tools.
- Optimizes image quality by embedding data without visual distortions.

2. Multi-Layered Encryption for Enhanced Data Security

Current Limitation:

Our system currently employs AES-256-GCM encryption, which is highly secure, but single-layer encryption might still be vulnerable to quantum computing attacks in the future.

Future Enhancement:

- We can implement multi-layered encryption using a combination of:

- AES-256-GCM + Chaotic Cryptography – Encrypting the message first with AES, then using a chaotic encryption algorithm to add an additional layer of security.
- AES + Quantum Cryptography – Using Quantum Key Distribution (QKD) to secure the encryption key transmission in post-quantum computing environments.

Benefits:

- Provides multi-layered security that protects against both classical and quantum attacks.
- Even if an adversary decrypts one layer, the second layer still ensures security.
- Makes brute-force attacks virtually impossible.

3. Video and Audio Steganography Integration

Current Limitation:

The current system is limited to image-based steganography. However, text, audio, and video steganography provide additional channels for secure communication.

Future Enhancement:

Expanding steganography to video & audio files can provide more secure methods for hiding large amounts of data:

- Video Steganography: Data is embedded within video frames, making detection extremely difficult.
- Audio Steganography: Messages are hidden in silent regions or high-frequency components of an audio file.

Benefits:

- Higher embedding capacity for storing large secret messages.
- Increased security as audio and video files are more challenging to analyze for hidden data.
- Broader applicability in secure communications, digital watermarking, and forensic data hiding.

4. Blockchain-Based Secure Key Exchange

Current Limitation:

In our system, the encryption key must be securely shared between the sender and receiver,

which may introduce a risk of interception if exchanged insecurely.

Future Enhancement:

We can integrate Blockchain technology to manage secure key distribution:

- The AES encryption key can be stored in a private Blockchain and only accessed by authenticated users.
- A decentralized ledger ensures that the key cannot be modified or intercepted.

Benefits:

- No central authority needed for key management.
- Prevents unauthorized access and key tampering.
- Ensures end-to-end encryption in a highly secure environment.

5. Steganography-Resistant Image Generation (Adversarial AI)

Current Limitation:

Some advanced stego-analysis tools can still detect patterns in stego-images, especially if attackers use deep learning models to scan images for modifications.

Future Enhancement:

We can develop Adversarial AI models that generate steganography-resistant images, meaning:

- The system intelligently modifies cover images to ensure that even after embedding the message, the statistical properties remain unchanged.
- GANs (Generative Adversarial Networks) can be trained to generate indistinguishable stego-images from regular images.

Benefits:

- Eliminates the risk of steganalysis detection.
- Ensures that stego-images remain indistinguishable from normal images.
- Highly advanced security using AI-driven adaptive steganography.

6. Stego-Cloud for Secure Data Storage and Retrieval

Current Limitation:

Currently, stego-images must be manually transmitted between sender and receiver. There is no centralized storage for securely retrieving hidden messages.

Future Enhancement:

Stego-Cloud Service where:

- Users can upload stego-images to a secure cloud server.
- Only authenticated users can download and decrypt the hidden data.
- The cloud service automatically verifies message integrity using digital signatures.

Benefits:

- Secure online storage for steganographic data.
- Remote access without worrying about key interception.
- Cloud-based authentication ensures only authorized users can retrieve messages.

7. Mobile & IoT-Based Secure Steganography

Current Limitation:

The current system is designed for desktop environments, but mobile and IoT devices also require secure steganography solutions.

Future Enhancement:

Developing lightweight steganography applications for:

- Android/iOS devices – Allowing users to hide and retrieve messages on mobile.
- IoT devices – Securely transmitting hidden data between smart sensors for covert communication.

Benefits:

- Increased accessibility for secure communication on the go.
- IoT-based steganography enables secure transmission in surveillance-sensitive areas.
- User-friendly applications make steganography more practical for real-world use.

11. REFERENCES

1) Joshi and Bhand, "Adaptive Fuzzy Logic-Based Steganographic Encryption Framework,"2026.

This work combines fuzzy logic with AES-256-GCM to dynamically adjust embedding strength. It improves both imperceptibility and security while resisting adaptive attacks and steganalysis.

2) Raj, "A Comprehensive Survey of Image Steganography," 2026.

This survey reviews modern steganography techniques, especially AI and deep learning-based methods. It highlights challenges like detectability and dataset limitations, guiding future research directions.

3) Aljarf *et al*., "DL-Steg: A Deep Learning-Based Steganography Model," 2025.

The authors propose an SAE-LSTM model with ECC encryption to enhance capacity and extraction accuracy. The system shows strong robustness against compression and noise.

4) Banoori *et al*., "Improved Hybrid Image Steganography Using AES," 2025.

This method integrates AES encryption with adaptive embedding and XOR operations. It ensures high security, better PSNR, and minimal image distortion for real-time communication.

5) Malathi *et al*., "Deep Steganographic Approach Using CNN Architecture," 2025.

A three-stage CNN model is introduced to automate embedding and extraction. It achieves high invisibility, robustness, and efficiency in secure data hiding.

6) Liu *et al*., "RISRANet: Reversible Image Steganography Using Attention Mechanism," 2025.

This approach uses attention-based neural networks for reversible data hiding. It enables high-quality image recovery and reduces distortion during extraction.

7) Fan *et al*., "AGASI: GAN-Based Adversarial Image Steganography," 2025.

The system leverages GAN architecture to improve resistance against steganalysis. It generates high-quality stego images with enhanced security.

8) Khalifa *et al*., "Wavelet-Based Fusion Steganography Using Deep Learning," 2025.

This work combines DWT with CNN techniques to improve embedding capacity and image quality. It also provides robustness against compression attacks.

9) Mahalakshmi *et al*., "MTARGAN-Based Image Steganography," 2025.

An attention-based GAN optimized with particle swarm optimization is proposed. It improves PSNR, embedding efficiency, and detection resistance.

10) Zhao *et al*., "Wavelet Loss-Based GAN Steganography," 2025.

This model uses U-Net GAN with wavelet loss to enhance embedding quality. It reduces detection probability while improving robustness and capacity.

11) Kumar and Desai, "AES-GCM Integrated Edge-Based Image Steganography," 2024.

The system combines AES-256-GCM encryption with edge-based embedding. It ensures strong confidentiality, integrity, and improved imperceptibility.

12) Zhang *et al*., "GAN-Based Secure Image Steganography," 2024.

A GAN-based model is proposed to automatically learn optimal embedding patterns. It enhances undetectability and represents AI-driven steganography.

13) Ahmad *et al*., "CNN-DCT Hybrid Steganography," 2024.

This hybrid approach combines CNN with DCT for improved robustness and efficiency. It is suitable for secure cloud-based applications.

14) Wong and Patel, "Transform-Domain Steganography Using DWT-DCT Fusion," 2023.

The authors propose a hybrid transform-domain technique to resist compression attacks. It achieves high PSNR and supports real-time applications.

15) Rao *et al*., "AI-Assisted Adaptive Embedding," 2023.

CNN is used to intelligently select embedding regions in images. This improves capacity, reduces detectability, and minimizes manual effort.

16) Singh and Reddy, "Authenticated Encryption-Based Stego-System Using AES-GCM," 2022.

The system uses AES-GCM to ensure both confidentiality and integrity. It also detects tampering effectively, enhancing security.

17) Bansal and Arora, "Hybrid DWT-SVD Steganography," 2022.

This method combines DWT and SVD to improve robustness against noise and compression. It maintains high image quality.

18) Agarwal *et al*., "Adaptive DWT-SVD Image Steganography," 2021.

A texture-based embedding approach is proposed for improved PSNR and structural similarity. It provides resistance against pixel-level attacks.

19) Gupta *et al*., "Blowfish Encrypted DWT Steganography," 2020.

This system integrates Blowfish encryption with wavelet embedding. It enhances security and performs well in noisy environments.

20) Sharma and Singh, "RSA-Enhanced Steganography," 2019.

RSA encryption is combined with LSB embedding for better confidentiality. However, it increases computational complexity, showing a trade-off.

21) Hussain et al., "Secure Image Steganography Using Pixel Value Differencing and Encryption," 2018.

The method combines PVD with symmetric encryption to improve embedding capacity. It maintains image quality while enhancing resistance against statistical attacks. The system is suitable for secure image communication.

22) Patel and Shah, "An Efficient LSB-Based Image Steganography with Random Pixel Selection," 2018.

A pseudo-random embedding technique is introduced to reduce predictability. It improves security while maintaining simplicity. The method enhances resistance to steganalysis and is efficient for low-complexity systems.

23) Singh et al., "DCT-Based Image Steganography with Data Encryption," 2017.

The system combines DCT transform with encryption to improve robustness. It provides better protection against compression and noise. The approach is suitable for secure multimedia transmission.

24) Kaur and Singh, "Enhanced LSB Steganography Using Edge Detection Technique," 2017.

This method embeds data in edge regions to improve imperceptibility. It reduces visual distortion and enhances security. The approach is simple and more effective than traditional LSB.

25) Verma and Gupta, "Image Steganography Using Edge-Based LSB Substitution," 2016.

Edge detection is used to select optimal embedding locations. The method reduces detection probability and improves image quality. It is widely used in early adaptive steganography research.