International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Smart Stegoguard an AI Powered System for Steganography Detection, Prevention, Secure Image Generation and Transmission

Ms.Vedanti Manoj Patekar **Exam No: B400400370**
Ms.Apurva Bharat Thorat **Exam No: B400400405**
Ms.Shreya Yogesh Khadilkar **Exam No: B400400347**
Ms.Diksha Dipak Jadhav **Exam No: B400400335**

Under the Guidance of

Prof. Radhika Balmuri

Department of Computer Engineering
JSPM's Jayawantrao Sawant College of Engineering, Pune
Hadapsar, Tal-Haveli, Pin- 411028, India

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

ABSTRACT

Smart StegoGuard is an AI-powered cybersecurity system developed to detect, prevent, and secure steganographic content hidden within digital images. As steganography techniques become increasingly sophisticated, hidden information can be used for unauthorized communication and malicious activities, posing significant security threats. The proposed system provides an intelligent framework to identify such hidden content and ensure secure image transmission.

The system utilizes image processing and machine learning techniques for effective steganography detection. Discrete Wavelet Transform (DWT) is employed to analyze image frequency components and detect subtle modifications caused by data embedding. Histogram Analysis is used to examine pixel intensity distributions and identify abnormalities that may indicate the presence of hidden information. These methods enable accurate and efficient analysis of digital images.

To enhance performance, the Salp Swarm Optimization Algorithm (SSOA) is used for selecting the most relevant features, while the XGBoost classifier accurately distinguishes between clean and steganographic images. This combination improves detection accuracy and reduces false classifications.

Additionally, Smart StegoGuard supports secure image generation and transmission through a user-friendly interface. The system is implemented using Python along with libraries such as NumPy, Pandas, scikit-learn, Matplotlib, and XGBoost. With applications in law enforcement, defense, healthcare, education, and corporate sectors, Smart StegoGuard provides a reliable, scalable, and efficient solution for secure digital communication and steganography prevention.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

INDEX

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Chapter 1

Introduction

1.1 Introduction

Steganography is the practice of concealing information within digital media such as images, audio, or video files in a manner that hides the existence of the secret data. Although it is widely used for privacy protection and secure communication, it can also be misused for unauthorized data exchange, cybercrime, and malicious activities. With the rapid growth of digital communication and the availability of advanced steganography tools, detecting hidden information has become a major challenge in the field of cybersecurity.

To address this issue, Smart StegoGuard is proposed as an AI-powered system designed to detect, prevent, and secure against steganographic content in digital images. The system employs image processing techniques such as Discrete Wavelet Transform (DWT) and Histogram Analysis, along with machine learning models like XGBoost and Salp Swarm Optimization Algorithm (SSOA), to accurately identify hidden data. It also provides secure image generation and transmission, ensuring safe, reliable, and trustworthy digital communication across various domains.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Chapter 2

Literature Survey

Sr no	Author	Paper Title	Year	Description	Advantages	Disadvantages
1	Kai Gao , Ching-Chun Chang , Ji-Hwei Horng, and Isao Echizen	Steganographic secret sharing via AI-generated photorealistic images[3]	2022	An authentication-based method using CNNs to map and share secrets without a traditional carrier image.	An authentication-based method using CNNs to map and share secrets without a traditional carrier image.	Operates within a narrow scope of secret sharing and fails to address broader malware or sanitization threats.
2	Mahjabin, Olteanu, Xiao, Han, Li, Sun	A survey on DNA based cryptography and steganography[2]	2023	A theoretical approach utilizing natural and pseudo-DNA structures to encrypt and hide digital information.	Offers virtually limitless storage density and a unique biological layer of encryption that is computationally hard to break.	Remains largely restricted to theoretical surveys and lacks practical, real-world frameworks for threat detection.
3	Angelica Liguori ,· Marco Zuppelli · Daniela Gallo · Massimo Guarascio · Luca Caviglione	A deep learning-based approach for stego malware sanitization in digital images[1]	31 March 2025	A deep-learning framework designed to disrupt hidden malicious payloads while maintaining the original image quality.	Effectively "cleans" files by neutralizing embedded threats without degrading the host medium's visual integrity.	Functions as a reactive cleaning tool rather than a proactive system with optimized features for early-stage detection.

Table 2.1: Literature Survey

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Chapter 3

Problem Defination and Scope

3.1 Problem Statement

To design and develop an AI-based system that can detect and prevent steganography in multimedia files using advanced machine learning techniques. The system should analyze and identify hidden data patterns, prevent unauthorized data transmission, and ensure secure communication channels through intelligent monitoring and adaptive learning. i want to this code in the uploaded image

3.2 Project Scope

An **AI-powered steganography detection, prevention, and secure transmission system**. The project aims to identify hidden data within multimedia files and prevent unauthorized information exchange using intelligent machine learning techniques.

In-Scope:

Steganography Detection:

Development of an AI-based detection module capable of analyzing image files to identify hidden or suspicious data patterns using machine learning and optimization techniques.

Prevention Mechanism:

Integration of a real-time prevention system that blocks or isolates files containing detected steganographic content before transmission or storage.

Secure Transmission:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Implementation of secure data transmission protocols ensuring that only verified and clean files are allowed for communication, minimizing data leakage risks.

Implementation Platform:

- **Programming Languages:** Python for AI model development and system integration.
- **Frameworks/Libraries:** NumPy, Pandas, Scikit-learn, Matplotlib, XGBoost, and Flask for data analysis, machine learning, and web application development.
- **Front-end/Interface:** Web-based dashboard for uploading images, viewing analysis results, and secure file transmission.
- **Testing and Validation:** Verification of system accuracy, detection rate, false-positive rate, and efficiency using benchmark steganographic datasets.

Out of Scope:

1. Development of new multimedia encryption algorithms (existing encryption standards will be used).
2. Detection of steganography in live network traffic or cloud-based communication systems.
3. Physical security measures or device-level protection mechanisms.
4. Large-scale blockchain integration for file validation and tracking.
5. Analysis of audio and video steganography (current implementation focuses primarily on image files).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Chapter 4

Software Requirement and Specification

4.1 Introduction

The Software Requirement and Specification (SRS) defines the overall functionality, performance, and constraints of the proposed system. It acts as a blueprint for system development, validation, and deployment, ensuring that every module operates according to the defined objectives. The primary goal of this project is to design and implement a secure AI-based steganography system that ensures data confidentiality and controlled access through the integration of cryptographic authentication and intelligent image processing. This chapter outlines the algorithms, hardware-software requirements, and quality parameters that govern the operation and performance of the system. The Smart StegoGuard system is developed using Python with Flask for AI-based image embedding and extraction, integrated with cryptographic modules for authentication and security validation. The implementation is carried out on a Windows/Linux platform, providing a secure and scalable environment for testing and analysis.

4.2 Algorithm Selection

‘

4.2.1 Algorithm – I : DWT (Discrete Wavelet Transform)

Purpose:

Used to extract frequency-domain features from images to detect hidden steganographic data.

Working Principle:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

- The input image is resized and converted to grayscale for uniform processing.
- A single-level 2D Discrete Wavelet Transform (DWT) is applied using the Haar wavelet.
- The image is decomposed into LL, LH, HL, and HH sub-bands.
- Each sub-band captures unique spatial-frequency information useful for steganography detection.

Advantages:

- High security and imperceptibility.
- Robust against compression and noise.
- Higher embedding capacity than LSB methods.

4.2.2 Algorithm – II : Histogram Analysis

Purpose:

Used to identify irregularities in pixel intensity distribution caused by hidden data embedding.

Working Principle:

- Compute pixel intensity histograms from images.
- Analyze frequency distribution patterns.
- Detect anomalies that indicate hidden information.
- Generate statistical features for classification.

Advantages:

- Simple and computationally efficient.
- Effective for detecting steganographic modifications.
- Provides useful statistical features.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

4.2.3 Algorithm – III : SSOA (Salp Swarm Optimization Algorithm)

Purpose:

Used to select the most relevant features for steganography detection.

Working Principle:

- Initialize a population of salps representing feature subsets.
- Evaluate each subset using a fitness function.
- Leader salps guide the search toward optimal solutions.
- Follower salps update their positions accordingly.
- The process continues until the best feature subset is obtained.

Advantages:

- Reduces feature redundancy.
- Improves detection accuracy.
- Reduces computational complexity.

4.2.4 Algorithm – IV : XGBoost (Extreme Gradient Boosting)

Purpose:

Acts as the primary classifier for distinguishing between clean and stego images.

Working Principle:

- Start with an initial prediction.
- Calculate prediction errors (residuals).
- Train a decision tree to correct errors.
- Update predictions iteratively.
- Repeat until optimal performance is achieved.

Advantages:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

- High classification accuracy.
- Handles large datasets efficiently.
- Reduces overfitting through regularization.

4.2.5 Algorithm – V : DNA-Based Encryption and Decryption

Purpose:

Used to secure secret information before transmission.

Working Principle:

1. Convert binary data into DNA sequences using mapping rules.
2. Apply DNA operations such as complement, substitution, and XOR.
3. Generate encrypted DNA sequences.
4. Reverse the operations during decryption.
5. Recover the original data securely.

Advantages:

- Provides strong security.
- Resistant to cryptanalysis attacks.
- Suitable for secure data transmission.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

4.3 Design and Implementation Constraints:

- **Computational Overhead:** AI-based image generation and authentication code embedding introduce additional computation, which may slightly increase processing time for large multimedia files.
- **Key Storage Security:** Storing access keys or authentication metadata requires secure storage to prevent unauthorized extraction, tampering, or loss.
- **Integration Complexity:** Integrating DWT, SSOA, and XGBoost models with feature extraction, feature selection, and access control layers requires an in-depth understanding of machine learning workflows and system design.
- **Performance Trade-off:** Real-time verification and extraction introduce a minor delay during data retrieval, although it remains acceptable for secure multimedia applications.

4.4 System Features:

- **Secure Data Embedding:** Ensures that secret information is securely hidden within AI-generated photorealistic images, preventing unauthorized detection or extraction.
- **Authentication Code Verification:** Uses CNN-based embedded authentication codes to verify the integrity and authenticity of stego images before data retrieval.
- **Key-Based Access Control:** Allows only authorized users with valid access keys to extract hidden data, preventing unauthorized access.
- **Lightweight and Scalable Design:** Designed to efficiently handle images, audio, or video files without heavy computational overhead, making it scalable for real-world applications.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

4.5 Hardware Requirements (Minimum Requirement):

Component	Requirement
Processor	Intel Core i5 or Higher
RAM	8 GB Minimum (16 GB Recommended)
Storage	256 GB SSD or Higher
Display	1366 × 768 Resolution or Above
Network	Stable Internet Connection
Input Devices	Keyboard and Mouse

4.6 Software Requirements (Minimum Requirement):

Component	Requirement
Programming Language	Python 3.10+
Deep Learning Framework	TensorFlow / PyTorch
Machine Learning Algorithm	XGBoost
Feature Selection Technique	SSOA (Salp Swarm Optimization Algorithm)
Image Processing Techniques	DWT (Discrete Wavelet Transform), Histogram Analysis
Steganography Technique	LSB (Least Significant Bit)
Libraries	NumPy, Pandas, Matplotlib, Scikit-learn
Database	PostgreSQL
Version Control	Git and GitHub

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

4.7 Software Quality Attributes:

- **Security:** Ensures strong protection against unauthorized data embedding and extraction through DNA-based encryption and AI-driven detection mechanisms.
- **Reliability:** Maintains consistent performance and accuracy in steganographic detection under varying image types and noise conditions.
- **Integrity:** Guarantees that the embedded or extracted data remains unaltered during transmission and processing.
- **Maintainability:** Modular design allows easy updates of encryption keys, feature extraction modules, or classifiers without affecting the overall system.
- **Performance Efficiency:** Utilizes optimized algorithms like DWT and XGBoost to ensure fast execution with minimal computational overhead.
- **Scalability:** Supports extension to large-scale datasets and integration with cloud-based image security systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

4.8 Analysis Model

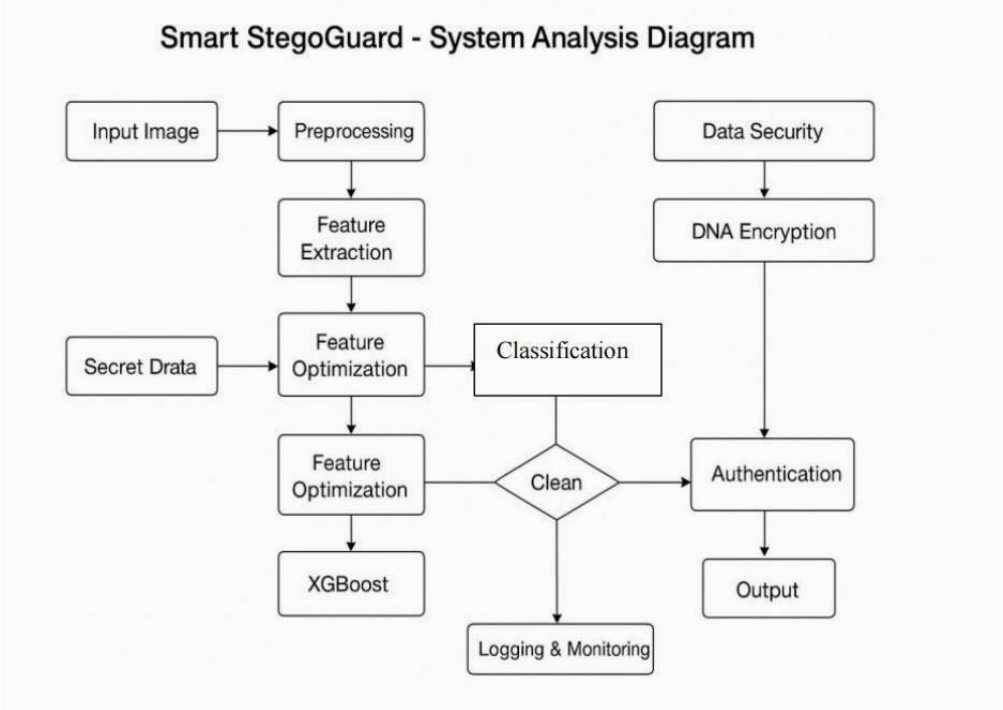

Figure 4.1: Analysis Model

This system analysis diagram, titled Smart StegoGuard, illustrates a data security and steganography process. It begins with an Input Image that undergoes Preprocessing and Feature Extraction. Separately, Data Security is applied through DNA Encryption. The extracted features and a Secret Data are combined in Feature Optimization before being processed by ClassiScoop. An additional Feature Optimization step then feeds into a decision point, which checks if the data is Clean. If clean, it proceeds to Authentication and produces the Output. If not clean, it is sent for Logging Monitoring. The second feature optimization also directly feeds into an XGBoost model for classification. The process integrates image feature analysis, secret data embedding, DNA encryption for security, and a classification/authentication mechanism to produce a secured output

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Chapter 5

Project Plan

5.1 Project Plan for Project

5.2 Project Plan

A well-structured project plan ensures systematic development, testing, and successful deployment of the **Smart StegoGuard System**. The project is executed through a series of well-defined stages, ensuring reliability, scalability, and robust security against steganographic threats. It follows standard software engineering methodologies to achieve accurate detection, prevention, and secure data transmission.

Project Overview

The project aims to develop and integrate an **AI-powered security framework** capable of detecting, preventing, and securing data against **steganography-based attacks**. The **Smart StegoGuard** system combines **machine learning algorithms, optimization techniques, and cryptographic modules** to analyze digital images, identify hidden data patterns, and ensure secure communication across networks.

The development is divided into six major phases:

1. **Requirement Analysis:** Gathering project requirements, studying steganography techniques, and identifying system objectives.
2. **System Design:** Designing the architecture, workflow, database structure, and user interface of the proposed system.
3. **Implementation:** Developing modules for DWT feature extraction, Histogram

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Analysis, SSOA optimization, XGBoost classification, and DNA-based encryption.

4. **Integration:** Combining all modules into a unified system and ensuring smooth communication between components.
5. **Testing & Validation:** Evaluating system performance, detection accuracy, false-positive rate, and overall reliability using benchmark datasets.
6. **Documentation and Maintenance:** Preparing project documentation, user manuals, and ensuring future scalability and maintenance of the system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

5.3 SDLC

The Agile Model

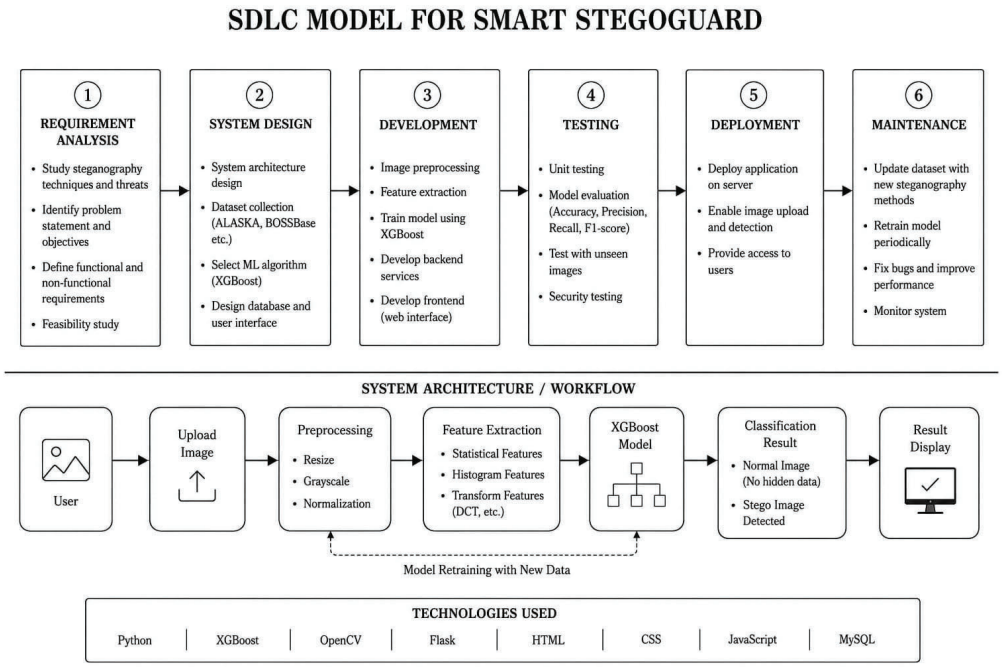

Figure 5.1: SDLC Diagram

The diagram illustrates the complete SDLC model and workflow of the Smart StegoGuard system. The development process follows six phases: Requirement Analysis, System Design, Development, Testing, Deployment, and Maintenance to ensure a reliable and secure steganography detection solution. The workflow begins with image upload and preprocessing, followed by feature extraction and classification using the XGBoost machine learning model. Based on the analysis, the system determines whether the image is normal or contains hidden steganographic content and displays the result to the user. The model can also be retrained with new data to improve detection accuracy and adapt to emerging steganography techniques.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Chapter 6

Block Diagram

6.1 Block Diagram for the Project

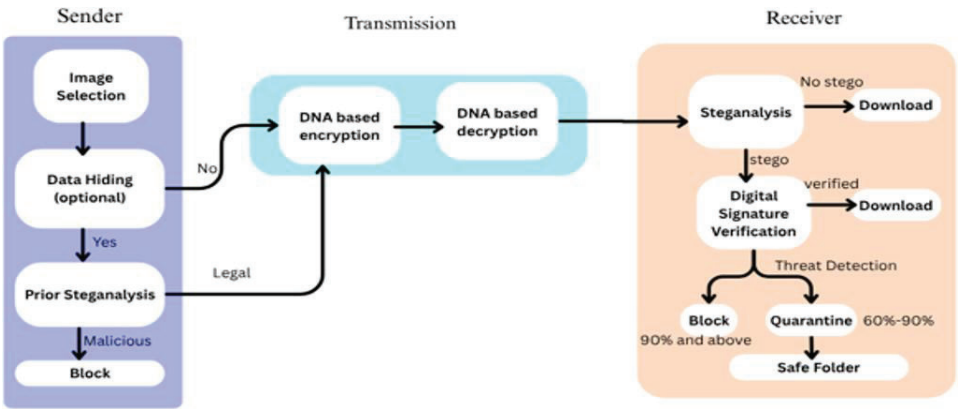

Figure 6.1: Block Diagram

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Description

The proposed **Smart StegoGuard** system consists of three major phases: **Sender**, **Transmission**, and **Receiver**. The system is designed to detect, prevent, and secure steganographic content during image transmission.

At the **Sender** side, the user first selects an image for transmission. Data hiding is optional and may be performed if secret information needs to be embedded within the image. Before transmission, the image undergoes **Prior Steganalysis**, where the system analyzes the image for suspicious or malicious steganographic content. If malicious content is detected, the image is immediately blocked from further processing. If the image is verified as legal and safe, it proceeds to the transmission phase.

During the **Transmission** phase, the image is protected using **DNA-based Encryption**, which converts the image data into a secure encrypted format. This encryption enhances confidentiality and prevents unauthorized access during communication. At the receiving end, **DNA-based Decryption** is performed to restore the original image data for further analysis.

At the **Receiver** side, the decrypted image undergoes **Steganalysis** to determine whether steganographic content is present. If no hidden data is detected, the image is considered safe and is directly available for download. If steganographic content is identified, the image is passed to the **Digital Signature Verification** module to verify its authenticity and legitimacy.

Based on the threat detection results, the system takes appropriate action. Images with a threat level of **90% or above** are automatically **blocked**, while images with a threat level between **60% and 90%** are moved to a **quarantine area (Safe Folder)** for further inspection. Verified and trusted images are allowed for download. This workflow ensures secure image transmission, effective steganography detection, and protection against unauthorized data communication.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Chapter 7

System Design

7.0.1 DFD Level 2 Diagram

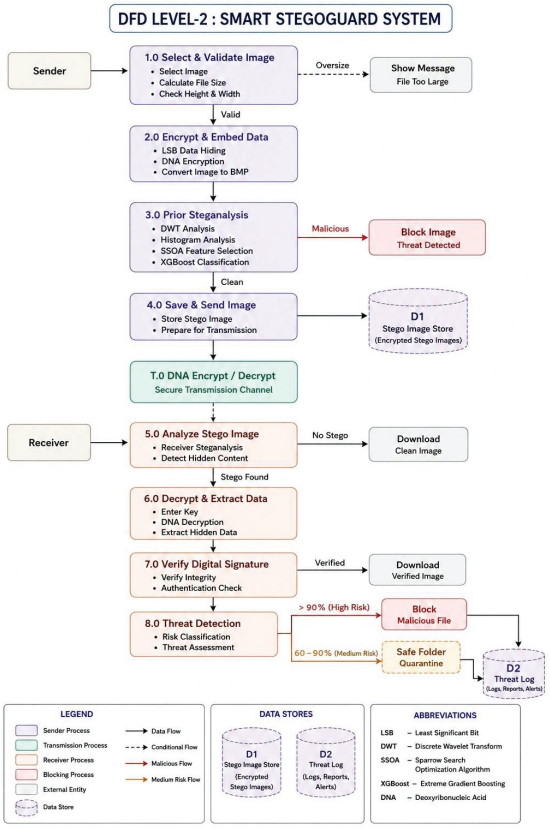

Figure 7.1: DFD Level 2 Diagram

The DFD Level-2 of the Smart StegoGuard System illustrates the complete workflow for secure image transmission with steganography detection and threat prevention. The process begins at the sender side, where the selected image is validated by check-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

ing its size and dimensions. If the image exceeds the allowed limits, a warning message is displayed; otherwise, the image proceeds to the encryption and data embedding stage, where LSB steganography and DNA encryption are applied. The image then undergoes Prior Steganalysis using techniques such as DWT Analysis, Histogram Analysis, SSOA Feature Selection, and XGBoost Classification to identify malicious hidden content. If a threat is detected, the image is blocked; otherwise, it is stored in the Stego Image Store (D1) and transmitted through a secure DNA-encrypted communication channel. At the receiver side, the image is analyzed for hidden data, and if steganographic content is found, the system decrypts and extracts the embedded information. A digital signature verification process ensures data integrity and authenticity before allowing the verified image to be downloaded. Finally, the system performs threat detection and risk assessment, where high-risk files are blocked and medium-risk files are quarantined in a safe folder, with all incidents recorded in the Threat Log (D2) for monitoring and security reporting.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

7.1 Class Diagram for Project

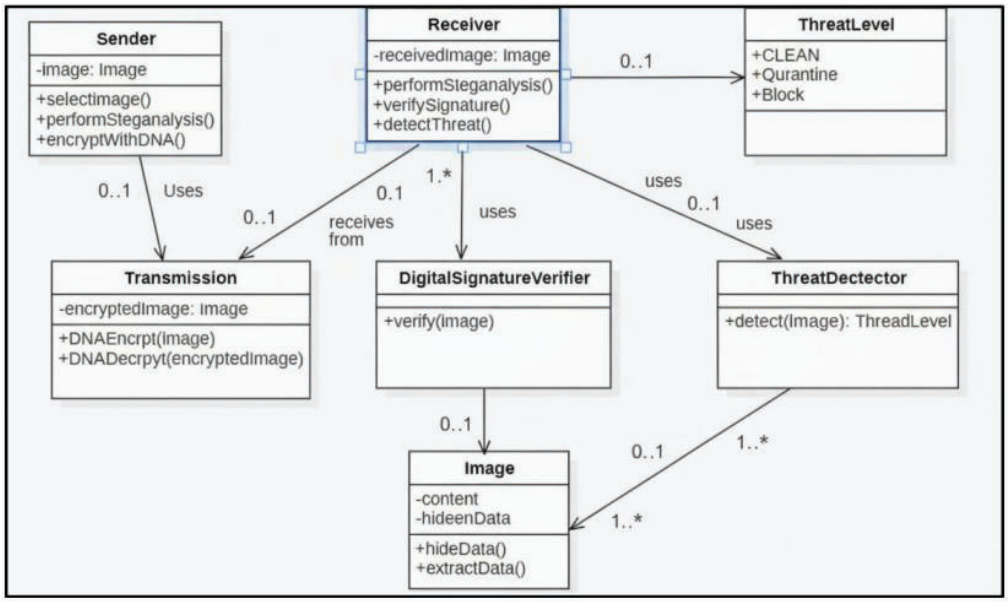

Figure 7.2: Class Diagram

The class diagram of this system illustrates the structural design and interactions among various components involved in threat prevention and steganography. The ImageHandler class is responsible for receiving, loading, and preprocessing images using techniques such as DWT and Histogram analysis. The StegoProcessor class performs steganographic operations, including LSB overwriting, JPEG compression, and extraction of hidden data from images. The ThreatDetector class analyzes image content using deep learning frameworks like TensorFlow or PyTorch to identify malicious patterns and potential threats. The LogManager class manages the generation and maintenance of system logs, reports, and threat visualizations using tools such as SQLite and Chart.js. The TransmissionManager ensures the secure transmission of analyzed or sanitized data through HTTPS and other communication protocols. Finally, the OutputGenerator class produces the processed results in multiple formats, including PDF, DOCX, and TXT, providing flexible and user-friendly output options.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

7.2 Use Case Diagram

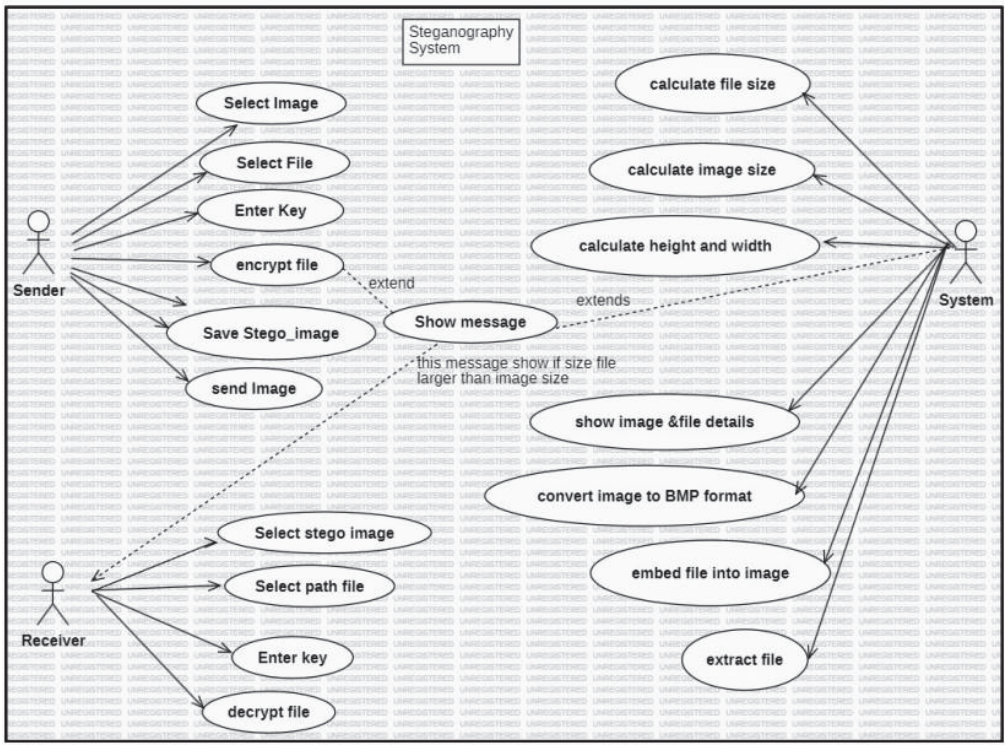

Figure 7.3: Use Case Diagram

The use case diagram illustrates the interaction between external actors and the steganography system, focusing on how data is hidden and retrieved securely. There are two main actors in this system: the Sender and the Receiver, along with the System which manages all operations. The Sender initiates the process by selecting an image, selecting the file to be hidden, and entering a security key. The system calculates the file size, image size, and image dimensions to verify if embedding is possible. Once validated, the file is encrypted and embedded into the image, converting it into BMP format for better stability. If the file size is larger than the image capacity, the system shows a message alerting the sender. After successful embedding, the sender can save the stego-image and send it to the receiver

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

7.3 Activity Diagram for Project

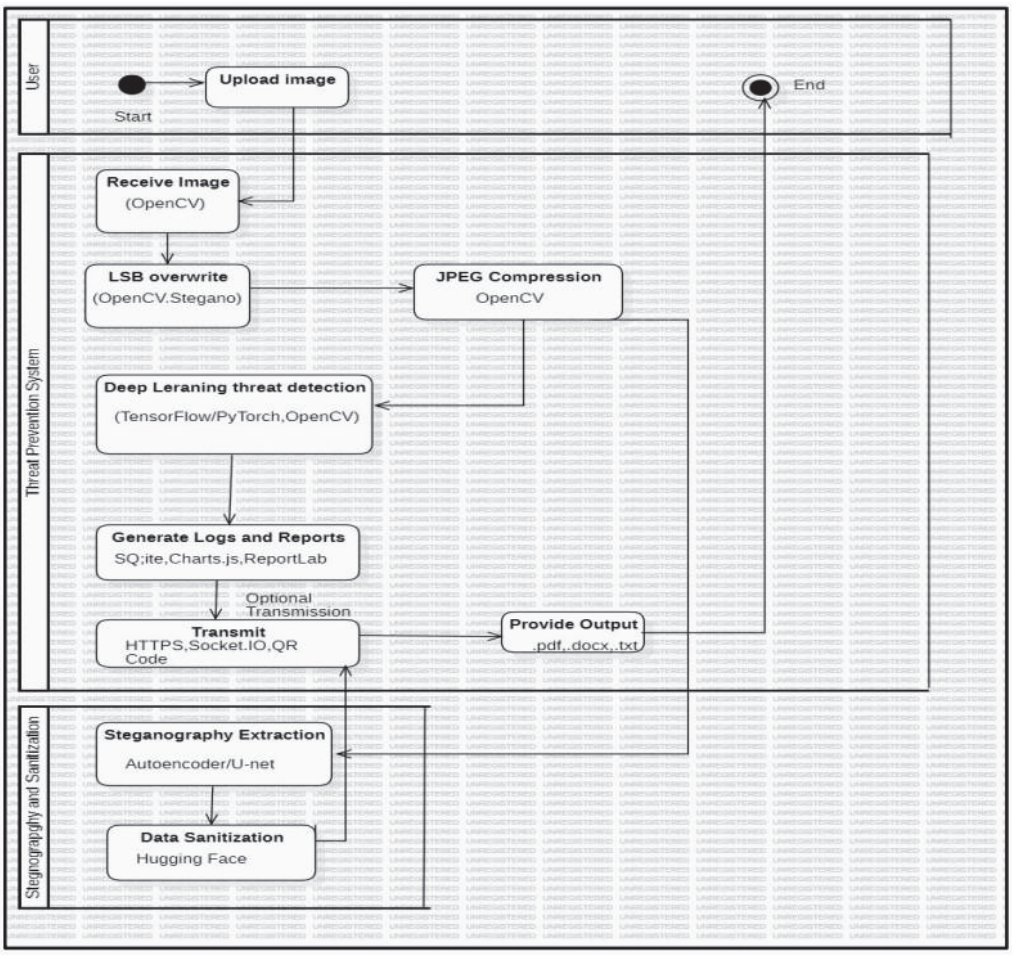

Figure 7.4: Activity Diagram

The activity diagram represents the step-by-step workflow of the steganography threat prevention and data sanitization system. The process starts with the user uploading an image, which is then received by the system for further processing. The uploaded image undergoes LSB (Least Significant Bit) overwrite and JPEG compression, both of which are techniques used to detect or remove any hidden information that might be embedded inside the image. After preprocessing, the system uses deep learning–based threat detection methods implemented with DWT, SSOA,XGBoost to identify any malicious or hidden steganographic content.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Chapter 8

Result

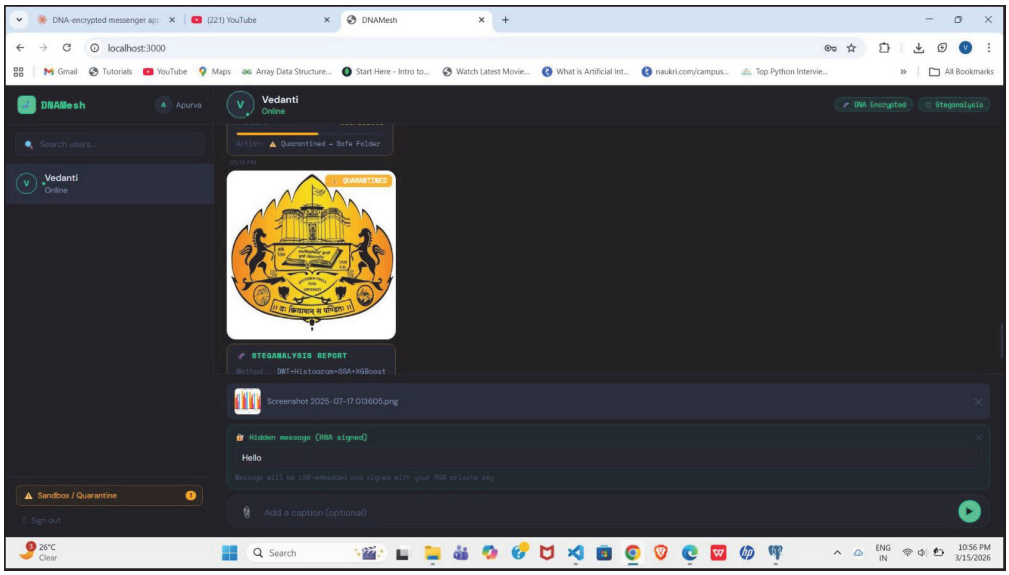

Figure 8.1: User 1 Chat Window

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

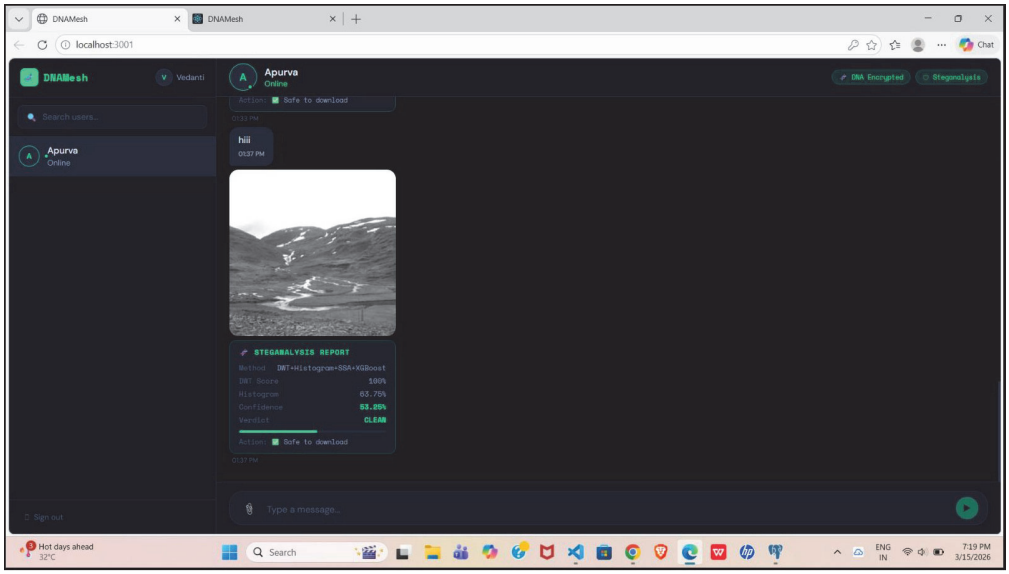

Figure 8.2: User 2 Chat Window

The above figures illustrate the chat interface of the proposed DNAMesh secure communication system for two different users, User 1 and User 2. The interface enables secure image sharing and message exchange while integrating steganography-based threat detection mechanisms. When an image is sent, the system automatically analyzes it and generates a Steganalysis Report displaying details such as detection status, confidence score, threat level, and verification results. The first figure shows User 1 (Vedanti) receiving an image that has been scanned and verified by the system, while the second figure shows User 2 (Apurva) viewing another image along with its corresponding analysis report. The chat window also includes options for secure transmission, image encryption status, and threat notifications. These screenshots demonstrate the system's ability to provide real-time threat detection, secure image communication, and detailed analysis reports to ensure safe and trustworthy data exchange between users.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Chapter 9

Technical Specification

9.1 Advantages:

- **High Detection Accuracy:** AI-driven classification using XGBoost ensures precise identification of steganographic images.
- **Enhanced Security:** DNA-based encryption safeguards image data from unauthorized access or tampering.
- **Optimized Performance:** SSOA (Seagull Search Optimization Algorithm) improves feature selection, reducing computation time.
- **Robust Data Protection:** Ensures secure image transmission with end-to-end encryption.
- **Scalability:** Can be extended to handle large datasets and integrated into various digital communication systems.
- **Automation:** AI-based detection and alert generation operate without manual intervention.
- **User-Friendly Interface:** Integrated WhatsApp-like module allows easy communication and instant alert notifications.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

9.2 Disadvantages:

- **High Computational Demand:** AI training and encryption require powerful hardware for faster processing.
- **Storage Requirement:** Large datasets and model files increase storage needs.
- **Complex Implementation:** Integration of multiple modules such as DWT, SSOA, XGBoost, and DNA-based encryption increases design complexity.
- **Limited Real-Time Capability:** Processing speed may decrease when handling high-resolution images or large volumes of image data.
- **Dependency on Dataset Quality:** Detection accuracy and model performance depend heavily on the quality, diversity, and size of the training dataset.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

9.3 Applications:

- **Messaging Applications:** Detect and block hidden malicious data embedded within images shared through messaging platforms.
- **Social Media Platforms:** Prevent covert communication, unauthorized information exchange, and illegal data sharing through image files.
- **Media Platforms:** Detect copyright violations, unauthorized hidden watermarks, and manipulated multimedia content.
- **Twitter (X) Memes:** Prevent attackers from embedding hidden instructions, malicious payloads, or secret messages within viral meme images.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Chapter 10

Conclusion

10.1 Conclusion

Smart StegoGuard is an intelligent security solution developed to address the increasing threats of steganography in digital communication. By integrating artificial intelligence with advanced image processing techniques such as DWT, Histogram Analysis, SSOA, XGBoost, and LSB steganography, the system effectively detects hidden information, identifies malicious content, and sanitizes suspicious images. It also ensures secure image generation and transmission, providing users with a reliable platform for safe digital communication. The system's modular architecture allows it to operate efficiently across various domains, including cybersecurity, law enforcement, healthcare, education, and social media platforms.Furthermore, Smart StegoGuard overcomes the limitations of traditional steganalysis methods by offering automated, real-time threat detection and comprehensive security reporting. The generated steganalysis reports help users understand the security status of images before sharing or receiving them, thereby reducing the risk of data leakage and covert communication. With its scalable design, high detection accuracy, and secure transmission capabilities, the proposed system contributes significantly to enhancing digital security and lays a strong foundation for future advancements in AI-driven steganography detection and cyber threat prevention.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Chapter 11

Bibliography

11.1 References

1. Khan, N., Haan, R., Boktor, G., McComas, M., Daneshi, R. (2020). *Steganography GAN: Cracking Steganography with CycleGANs*. arXiv:2006.04008. Demonstrates using CycleGANs to detect and break classical LSB steganography techniques.

2. Liu, M., Zhang, M., Liu, J., Yang, X. (2018). *Generative Steganography Based on GANs*. In Cloud Computing and Security (ICCCS 2018), Lecture Notes in Computer Science. Proposes GAN architectures for embedding secret data securely within synthesized images.

3. Guan, Y., Tan, S., Li, Q. (2023). *Binary Steganography Based on Generative Adversarial Nets*. Multimedia Tools and Applications, 82, 6687–6706. Applies GANs for binary data embedding using syndrome-trellis codes and distortion minimization.

4. Kaneria, S., Jotwani, V. (2024). *Comparative Performance of U-Net, V-Net, and U-Net++ for Deep Learning-Based Image Steganography*. Journal of Advanced Zoology, 45(3). Evaluates different encoder architectures for embedding and reconstruction quality.

5. *Edge-Guided Dual-Stream U-Net for Secure Image Steganography*. (2023). Applied Sciences, 15(8), 4413. Uses a dual-stream U-Net architecture to improve imperceptibility and resistance against steganalysis.

6. Yangjie, Z., Jia, L., Meiqi, L., Ke, Y., Zhang, M. (2024). *Generative Image*

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Steganography Based on Point Cloud. arXiv preprint arXiv:2410.11673. Introduces a point-cloud-based representation for secure steganographic embedding.

7. Wang, X., Chen, K., Qi, Y., Liu, R., Zhang, W., Yu, N. (2025). *GIFDL: Generated Image Fluctuation Distortion Learning for Enhancing Steganographic Security*. arXiv preprint arXiv:2504.15139. Proposes a distortion-learning method using generated image fluctuations to improve resistance to steganalysis.

8. Zhang, K.A., Cuesta-Infante, A., Xu, L., Veeramachaneni, K. (2019). arXiv preprint arXiv:1901.03892. This paper introduces a GAN-based approach achieving high embedding capacity and imperceptibility in stego-images.