Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

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

Radhika Balmuri
Department of Computer Engineering
Jayawantrao Sawant College of Engineering Hadapsar, Pune, India

Vedanti Patekar
Department of Computer Engineering
Jayawantrao Sawant College of Engineering Hadapsar, Pune, India

Apurva Thorat
Department of Computer Engineering
Jayawantrao Sawant College of Engineering Hadapsar, Pune, India

Shreya Khadilkar
Department of Computer Engineering
Jayawantrao Sawant College of Engineering
Hadapsar, Pune, India

Diksha Jadhav
Department of Computer Engineering
Jayawantrao Sawant College of Engineering
Hadapsar, Pune, India

***Abstract*—**In today's digital world, steganography—hiding data inside images—has become both a useful way to protect privacy and a growing cybersecurity concern. Traditional steganalysis methods rely on manual rules or predefined patterns and are not effective against modern, evolving steganographic techniques. To tackle this issue, this paper proposes Smart StegoGuard, an AI-powered is detected, the system immediately alerts the user and blocks the image from being shared, ensuring safe communication. The platform supports realtime scanning and reporting, while unsupervised anomaly detection and sandbox-based behavioral analysis help identify and isolate suspicious images proactively. In addition, Smart StegoGuard uses DNA-based encryption to provide an extra layer of security during transmission.

***Index Terms*—**Steganography, Image Security, Deep Learning, DWT, XGBoost, Anomaly Detection, Encryption, Cybersecurity, Secure Communication, AI-based Detection, Data Privacy

I. INTRODUCTION

With the rapid spread of digital image sharing across corporate, academic, and research environments, steganography—the practice of hiding secret data inside images—has become both a tool for privacy and a serious cybersecurity threat. As organizations increasingly rely on digital media exchange, the need for accurate and efficient steganalysis has become critically important. Proper detection ensures that hidden data, covert instructions, and malicious content embedded in images are identified before causing harm. However, traditional steganalysis methods remain highly inefficient, often relying on predefined rules that fail against modern steganographic techniques [1].

The process of manually examining the images is an arduous task that demands great knowledge of how steganography works, takes a lot of time, and cannot be scaled up to handle all the images being posted online today.

system that can detect, prevent, and secure hidden information in digital images. It combines Discrete Wavelet Transform (DWT), histogram-based feature extraction, the Seagull Search Optimization Algorithm (SSOA) for selecting the most relevant features, and XGBoost for accurate classification. Whenever hidden data

In addition, the current digital security tools that try to solve this problem through providing encryption services do not perform any detection of steganographic contents and lack any reporting mechanism [2].

The current proposed method does not have the inclusion of a complete process involving the detection of the steganography, the detection of anomalies, actions taken against them, and the encryption of the data. These can pose their own set of risks. To address the issues mentioned earlier, Smart StegoGuard is introduced as an artificial intelligence system of image security that will have the following features:

- Real-time image scanning based on hybrid AI models of steganalysis
- Feature extraction through DWT and histogram analysis techniques
- Selection of optimal features by Seagull Search Optimization Algorithm (SSOA)
- Precise classification of clean, suspicious, or stego images using XGBoost
- Automated security response by blocking high-risk and quarantining medium-risk images

By integrating these components into a unified platform, Smart StegoGuard eliminates the need for manual inspection and ensures consistent, accurate, and well-structured image security. The system not only enhances cybersecurity posture but also reduces the cognitive load on analysts, allowing them to focus entirely on verified threats rather than routine scanning [3].

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

In Section II, we review the five critical literature reviews that inspire and underpin Smart StegoGuard. In Section III, we provide a comparison between these approaches. The research gaps that need to be filled are identified in Section IV for which Smart StegoGuard has been conceived. Section V is explaining the architecture of the system.

II. LITERATURE REVIEW

A. Secured and High-Quality Steganography for IoT Dhawan et al.The concept of SSII was suggested by [1], and intelligent hybrid optimization techniques are used for securing and optimizing the quality of IoT-based steganographic data embedding. The system is efficient and accurate enough in terms of embedding. Although it represents a new approach to data hiding within IoT applications, it addresses solely the issue of data embedding but lacks any tools to detect, prevent, or combat threats related to steganography. It is the motivation behind Smart StegoGuard.

B. DNA-Based Cryptography and Steganography Mahjabin et al. [2] conducted a comprehensive survey on DNA-based cryptography and steganography, demonstrating how biological encoding structures can be harnessed for secure data protection. Their work highlights the theoretical robustness of DNA encoding but does not provide a complete implementation pipeline for real-world, real-time image security. Smart StegoGuard draws on these foundations by integrating DNA-based encryption directly into its secure transmission module.

C. Secure Image Steganography Using LSB and AES The approach suggested by Jalal et al. [3] involves the use of a combination of the LSB technique and AES cryptography for concealing data within images. Although this method guarantees that any embedded data will always be secured using encryption, it is lacking an effective steganalysis defense. The Smart StegoGuard system incorporates the same idea but implements a detection mechanism.

D. SSII for Wireless Personal Communications Rani et al. [4] presented improvements to the SSII framework specifically targeting wireless communication environments. Their work achieves high embedding accuracy in constrained wireless settings but remains focused on secure embedding, lacking a complete anomaly detection and quarantine mechanism. Smart StegoGuard addresses this gap through its integrated sandbox-based behavioral analysis and automated multi-tier threat response.

E. Universal Image Vaccine Against Steganography Wei et al. [5] introduced universal image vaccine that uses adversarial perturbations to immunize images against steganographic embedding. This preventive approach is innovative but has variable effectiveness across different steganography methods and does not handle posttransmission detection or provide secure communication channels. Smart StegoGuard complements this preventive approach by providing detection, classification, encrypted transmission, and automated quarantine in a unified pipeline.

III. RESEARCH GAP

The surveyed literature reveals five persistent gaps that collectively motivate the Smart StegoGuard system.

A. No Unified End-to-End Security Pipeline Each surveyed work addresses a specific component in isolation: secure embedding [1], [4], theoretical DNA frameworks [2], encryption-focused steganography [3], or preventive immunization [5]. A real-world image security system must simultaneously handle real-time steganalysis detection, intelligent threat classification, automated blocking and quarantine, and secure encrypted transmission. No existing work presents a single jointlyoptimised pipeline covering all these stages within a practical, deployable system. Smart StegoGuard is specifically designed to close this gap by unifying all stages into a single modular platform.

B. Lack of Anomaly Detection for Unknown Attacks Existing systems do not adequately address zero-day or previously unseen steganographic techniques. Most methods rely on known patterns or predefined signatures and fail when confronted with novel embedding algorithms. No surveyed work provides adaptive mechanisms for these environmental variabilities. Smart StegoGuard addresses this through integrated unsupervised anomaly detection and sandbox-based behavioral analysis that can identify suspicious images without relying on predefined patterns.

C. Absence of Automated Threat Response Mechanisms None of the surveyed works integrates automated blocking and quarantine as part of the security pipeline [1]–[5]. This gap means that even when detection is performed, the threat response action remains a manual task, reducing the overall efficiency and practical value of these systems. Smart StegoGuard eliminates this bottleneck through a multi-tiered automated response: images with high confidence of hidden data (>90%) are blocked immediately; moderate-risk images (60–90%) are quarantined for human review.

D. Insufficient Robustness Under Real-World Conditions Existing steganalysis evaluations are predominantly conducted in controlled environments with clean, highquality images. Real-world scenarios frequently involve compressed images, varying formats, and sophisticated embedding techniques. Dhawan et al. [1] and Rani et al. [4] acknowledge performance variation in constrained environments, while Jalal et al. [3] do not evaluate multitechnique resilience. No surveyed work provides domainadaptation mechanisms for these variabilities. Smart StegoGuard addresses this through a

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

hybrid feature extraction pipeline (DWT + histogram analysis) combined with SSOA-based feature selection.

Privacy and Data Sovereignty Concerns Systems relying on cloud-based APIs for image analysis raise significant privacy concerns, particularly for sensitive corporate, healthcare, or defence discussions. The surveyed literature does not adequately address on-device or privacy-preserving alternatives for the full security pipeline [5]. Smart StegoGuard acknowledges this limitation and identifies on-device processing and federated-learning-based analysis as a key direction for future work, ensuring that sensitive image data can eventually be processed without leaving the user's device.

These five gaps collectively define the design space that Smart StegoGuard occupies and provide the criteria against which its contributions will be evaluated in future experimental work.

TABLE I
COMPARATIVE SUMMARY OF RELATED WORK VS. SMART STEGOGUARD (PROPOSED)

Work	Task / Domain	Method	Platform	Speed	Accuracy	End-to-End Pipeline
Dhawan et al. [1]	Secure steganography for IoT	Hybrid optimization (SSII)	Edge / Cloud	Not reported	High (IoT data)	No (embedding only)
Mahjabin et al. [2]	DNA-based cryptography & steganography	DNA encoding + crypto survey	N/A (survey)	N/A	Not reported	No (survey only)
Jalal et al. [3]	Secure image steganography	LSB + AES encryption	Server	Not reported	Good (clean images)	Partial (no anomaly detection)
Rani et al. [4]	Secured stego for wireless	Hybrid optimization (SSII)	Wireless / Edge	Not reported	High (wireless env)	No (embedding only)
Wei et al. [5]	Universal image vaccine	Adversarial perturbation	GPU server	Not reported	Variable	No (vaccine only)
Smart StegoGuard (Proposed)	Detection, prevention, secure image transmission	DWT + Histogram + SSOA + XGBoost + DNA Encryption + Sandbox	Web App + Cloud / edge hybrid	Real-time (>90% accuracy)	>90% (test images)	Yes (full pipeline)

V. SYSTEM DESIGN AND ARCHITECTURE

A. Architectural Overview

The Smart StegoGuard system follows a modular layered architecture that integrates a web-based user interface, AIbased steganalysis engine, anomaly detection sandbox, DNA-based encryption module, PostgreSQL database, and automated threat response. This design ensures real-time performance, scalability, and smooth user interaction. The system consists of four main components:

1) The Web-based User Interface for image upload, scanning, and quarantine management
2) The Steganalysis Engine for feature extraction, selection, and AI-based classification
3) The Anomaly Detection and Sandbox Module for unknown threat identification
4) The Database and Encryption Service for secure storage and image transmission

B. User Interface Layer (Web Application) The frontend is developed as a web-based application using HTML, CSS, and JavaScript, which acts as the primary interface for users. It enables secure user authentication and allows users to upload images for real-time scanning. The application displays live detection results, confidence scores, DWT scores, histogram scores, and the final verdict for each image. Flagged images are presented in a quarantine dashboard where users can review and approve or reject them.

C. Steganalysis Engine

The steganalysis engine performs the core detection pipeline. Image preprocessing first cleans, resizes, and normalizes input images. The Discrete Wavelet Transform (DWT) then analyzes frequency components to identify hidden patterns not visible to the human eye. Histogrambased feature extraction studies pixel intensity distribution to detect data embedding. The Seagull Search Optimization Algorithm (SSOA) selects the most relevant

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

features, reducing noise and improving classification efficiency.

D. AI Classification Layer

The selected features are passed to the XGBoost classifier, which determines whether an image contains hidden data. XGBoost is chosen for its high accuracy, speed, and ability to handle complex patterns in data. The system generates a detailed transparency report for each image including DWT score, histogram score, overall confidence level, and a final verdict: Clean, Suspicious, or Stego. For unseen attack types, the sandbox module performs behavioral analysis to isolate and flag anomalous images.

E. Technology Stack

Table II summarises the complete technology stack of the Smart StegoGuard system across all architectural layers.

TABLE II
SMART STEGOGUARD TECHNOLOGY STACK

Layer	Technology	Version	Function
Presentation	Web UI (HTML/CSS/JS)	–	User interface for image upload, scanning, quarantine management
Authentication	User Login / Session Management	Custom	Secure user authentication and session control
Image Processing	Python + NumPy + OpenCV	Python 3.x	Image cleaning, resizing, normalization
Feature Extraction	DWT + Histogram Analysis	Custom	Frequency-domain and pixel-intensity feature extraction
Feature Selection	SSOA (Seagull Search Optimization)	Custom	Select most relevant features for classification
Classification	XGBoost	Latest stable	Detect presence of hidden steganographic data
Anomaly Detection	Unsupervised ML + Sandbox Analysis	Custom	Identify unknown / zero-day steganographic attacks
Encryption	DNA-based Encryption + RSA	RSA-2048	Secure image transmission and digital signature verification
Database	PostgreSQL	Latest stable	Store messages, images, detection results, metadata
Report Gen.	Custom Detection Report Engine	Python	Generate per-image detection reports with scores and verdicts

VI. CONCLUSION

This paper has presented a structured survey of the state of the art in image steganography detection and secure transmission, grounded in five closely related research works, and has identified the specific gaps that motivate the Smart StegoGuard system. The key findings are as follows.

Hybrid AI detection improves steganalysis reliability. Dhawan et al. [1] and Rani et al. [4] show that optimization-based approaches achieve high accuracy, directly supporting the effectiveness of Smart StegoGuard's DWT + SSOA + XGBoost detection pipeline.

DNA-based encryption enables secure transmission. Mahjabin et al. [2] demonstrate the robustness of DNA encoding for data protection, validating Smart StegoGuard's integration of DNA-based encryption into its secure image transmission module.

Automated threat response and detection are the critical missing capabilities. No surveyed system combines steganalysis detection, anomaly identification, automated blocking, quarantine handling, and encrypted secure transmission in a single end-to-end pipeline. Smart StegoGuard is specifically designed to close this gap [3], [4].

Privacy must be considered in cloud-dependent architectures. Systems relying on cloud APIs for image analysis raise data privacy concerns [5]. Smart StegoGuard acknowledges this limitation and identifies on-device processing as a priority for future work.

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

Robustness under real-world conditions remains an open problem. Prior studies highlight missing benchmarks for compressed, varied-format, and novel steganographic environments [2], [4]. Smart StegoGuard addresses this through DWT + histogram hybrid extraction, SSOA feature selection, and sandbox-based anomaly detection techniques.

In summary, Smart StegoGuard represents the next logical step in the evolution of intelligent image security systems—moving from isolated detection or encryption tools toward a unified, end-to-end platform capable of detecting, classifying, blocking, quarantining, encrypting, and securely transmitting images with minimal human intervention. Future enhancements, such as deep learning model integration (CNNs and transformers), audio and video steganography support, and direct integration with major communication platforms, will further expand the system's capabilities and real-world impact.

REFERENCES

[1] S. Dhawan, C. Chakraborty, J. Frnda, R. Gupta, A. K. Rana, and S. K. Pani, "SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT," IEEE Access, vol. 9, pp. 87563–87580, Jun. 2021.

[2] T. Mahjabin, A. Olteanu, Y. Xiao, W. Han, T. Li, and W. Sun, "A Survey on DNA-Based Cryptography and Steganography," IEEE Access, vol. 11, pp. 116423–116446, Oct. 2023.

[3] A. S. Jalal, M. A. Khan, and M. A. Khan, "A Secure Image Steganography Technique Based on LSB and AES Encryption," The Journal of Supercomputing, vol. 78, no. 12, pp. 18654–18675, Dec. 2022.

[4] R. Rani, G. Srivastava, M. L. Gavrilova, A. Nayyar, and V. Kumar, "SSII—Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT," Wireless Personal Communications, vol. 127, pp. 2359–2383, 2022.

[5] S. Wei, Z. Wang, and X. Zhang, "Universal Image Vaccine Against Steganography," Symmetry, 2025.

[6] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2009.

[7] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003.

[8] T. Pevýný, T. Filler, and P. Bas, "Using High-Dimensional Image Models to Perform Highly Undetectable Steganography," IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 215–224, 2010.

[9] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016.

[10] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in Proc. 22nd ACM SIGKDD Int. Conf. Knowledge Discovery Data Mining, 2016, pp. 785–794.