IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.26

Steganography and Steganalysis System Using Deep Learning

S.Kanmani
Assistant Professor, Department of CSE (Cyber Security)
Sengunthar Engineering College (Autonomous), Tiruchengode, India
kanmanicse@gmail.com
https://orcid.org/0009-0006-2904-7365
Abhishek kumar,Suryakant Kumar,Vinay Kumar Yadav,
UG Students, Department of CSE (Cyber Security)
Sengunthar Engineering College (Autonomous),Tiruchengode, India
Sisayadav8080@gmail.com, suryakantkr636@gmail.com, vinayjnv57@gmail.com

Publication History
Manuscript Reference: IRJCS/RS/Vol.13/Issue03/CSMR26.MRCS10105
Research Article | Open Access | Double-Blind Peer Reviewed Article ID: IRJCS/RS/Vol.13/Issue03/CSMR26.MRCS10105
Received: 30, January 2026, Revised: 13, February 2026, Accepted: 28 February 2026 Published Online: 25 March 2026
https://www.irjcs.com/volumes/Vol13/iss-03/26.CSMR26.MRCS10105.pdf
Article Citation:Kanmani,Abhishek,Suryakant,Vinay(2026),Steganography and Steganalysis System Using Deep Learning,IRJCS: International Research Journal of Computer Science, Volume 13,Issue 03 of 2026 pages 247-253
Doi:> https://doi.org/10.26562/irjcs.2026.v1303.26 **BibTeX Key Kanmani@2026Steganography**
Orcid: https://orcid.org/0009-0004-9398-7488
IRJCS papers should be cited as IRJCS (International Research Journal of Computer Science, AM Publications, India 2026, ISSN 2393-9842, https://doi.org/10.26562/ijrcs.2025.v1303.26 The journal's official abbreviation is IRJCS.

Abstract: Steganography and steganalysis systems represent sophisticated techniques in modern information security that conceal secret information within digital images while avoiding detection by traditional security inspection mechanisms. This paper proposes an intelligent steganography and steganalysis framework that integrates deep learning with image feature analysis to detect hidden messages and suspicious image modifications in real-time. The system captures and processes digital image data including pixel intensity values, color channels, spatial relationships, frequency patterns, and texture features to extract meaningful characteristics without significantly degrading image quality, ensuring efficiency and scalability. Using a Convolutional Neural Network algorithm trained on benchmark steganography image datasets, the model effectively distinguishes between normal images and stego-images containing concealed information such as embedded messages and hidden digital content. The modular architecture encompasses data acquisition, preprocessing, feature extraction, deep learning–based classification, hidden data embedding, detection reporting, and security monitoring mechanisms. Experimental results demonstrate significant improvement in detection accuracy with reduced error rates compared to conventional steganography detection techniques. This scalable, adaptive solution strengthens secure digital communication and enhances digital forensic analysis against evolving information hiding methods.
Keywords: Steganography, Steganalysis, Deep Learning, Convolutional Neural Network, Image Processing, Information Security, Hidden Data Detection, Secure Communication.

INTRODUCTION

Steganography and steganalysis have emerged as important techniques in modern information security, focusing on the concealment and detection of secret data within digital media such as images, audio, and video files [1],[2]. Unlike traditional cryptographic methods that only encrypt the content of a message, steganography hides the existence of the message itself, making it difficult for unauthorized parties to detect the presence of hidden information during transmission [3],[4]. Traditional security mechanisms such as signature-based intrusion detection systems and rule-based firewalls are often ineffective against APTs due to their evolving tactics, polymorphic malware, and low-and-slow attack behavior that mimics normal network activity [5],[6]. Recent advancements in machine learning (ML) and network flow analysis have enabled the development of intelligent intrusion detection frame works capable of identifying complex and stealthy attack patterns [7],[8]. ML-based approaches offer significant advantages over traditional methods by learning hidden patterns, correlations, and anomalies within large-scale network traffic without relying on predefined signatures [9],[10]. Studies have demonstrated the effectiveness of various ML algorithms including Random Forest, Support Vector Machines (SVM), and deep neural networks in classifying network flows and detecting APT- related activities such as command-and-control communication, lateral movement, and data exfiltration [11],[12]. Network flow analysis, which examines meta data such as source/destination IPs, ports, protocols, packet counts, and flow durations, provides a scalable and privacy-preserving alternative to deep packet inspection [13],[14].The proposed system integrates the Gradient Boosting algorithm with network flow analysis using the DAP dataset. It captures real-time traffic, extracts behavioral features, and employs supervised learning to distinguish normal from malicious activities. A modular architecture ensures systematic processing and scalability. Experimental results show improved detection accuracy with reduced false positives compared to conventional systems. This study contributes a robust, adaptive APT detection framework that strengthens organizational cyber security and enables proactive threat mitigation against evolving adversaries.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.26

LITERATURE REVIEW

Modern network security increasingly depends on intelligent intrusion detection systems to defend against sophisticated cyber threats. Traditional security mechanisms centered on signature based intrusion detection and rule-based firewalls face limitations such as inability to detect zero-day attacks, high false positive rates, and lack of adaptability to evolving threat patterns [1], [2]. To address these challenges, machine learning- enabled systems have emerged, offering automated threat identification, behavioral analysis, and scalable deployment across enterprise networks [3],[4]. Studies have shown that ML-based approaches significantly improve detection accuracy for advanced persistent threats compared to conventional signature- based methods [5],[6]. Deep learning architectures and flow-based analytics have further advanced the field by enabling real-time classification and multi-stage attack detection [7],[8]. Several systems have explored the integration of various deep learning algorithms including Convolutional Neural Networks (CNN), Support Vector Machines (SVM), and neural network models with image features such as pixel intensity distribution, spatial correlation, texture patterns, and frequency components [9],[10]. These systems analyze image data collected via image processing tools or public datasets commonly used in steganography research and experimentation [11],[12]. Supervised learning models trained on labeled datasets classify digital images as normal or stego-images, while unsupervised techniques detect anomalies without prior labeling [13], [14]. Visualization dashboards and analytical interfaces present detection results, hidden data probabilities, and image modification patterns to researchers and analysts, enabling informed decision- making [15],[16]. Some systems also incorporate secure embedding and extraction mechanisms to ensure reliable hidden data communication [17], [18]. However, many existing implementations remain fragmented, lacking unified platforms that combine efficient data embedding, deep learning detection, and comprehensive analysis within a single architecture [19],[20].Despite these advancements, persistent challenges remain. High false- positive rates insteg analysis detection systems may in correctly classify normal images as stego-images and reduce confidence in automated detection tools [6],[13].Class imbalance in training datasets where normal images significantly outnumber stego-images can degrade model performance for hidden data detection tasks [11],[14]. Computational overhead of deep learning models may limit real-time deployment in resource-constrained environments [7],[19]. Detecting hidden information in compressed or high-resolution images remains particularly challenging, as subtle pixel modifications are difficult to Identify using traditional image analysis techniques, requiring reliance on statistical image features and learned representations [8], [16]. Adversarial image manipulations against deep learning models also pose emerging threats, where attackers craft modified images to evade detection or mislead the trained system [18],[20]. The proposed steganography and steganalysis system addresses these gaps by offering a unified, scalable platform that integrates image acquisition, feature extraction, deep learning–based classification, and real-time detection within a single architecture. Unlike prior systems, it combines supervised learning with statistical image analysis, modular preprocessing pipelines, and interactive visualization interfaces for efficient monitoring and analysis of hidden information within digital images.

PROPOSED METHODOLOGY ARCHITECTURE

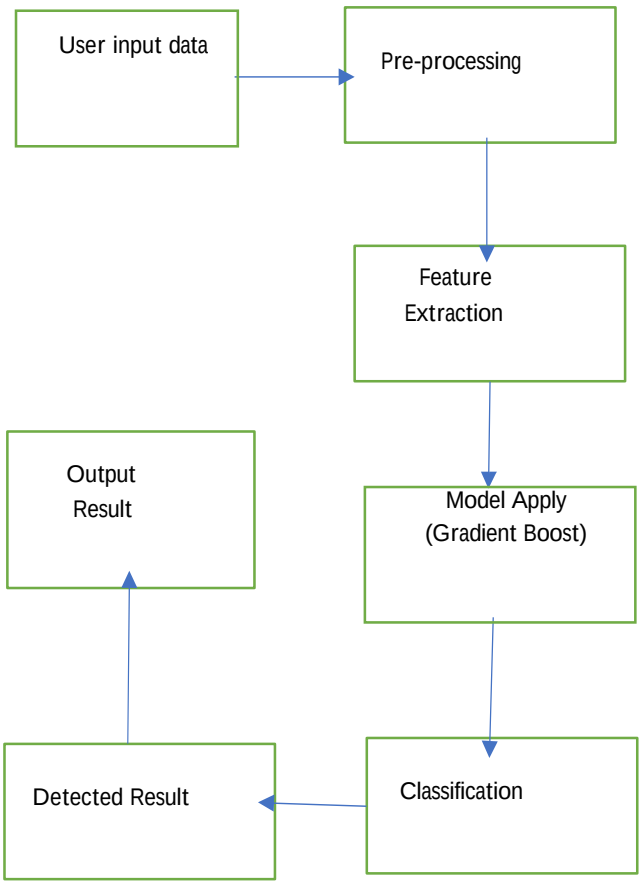

Fig.1. Architecture Diagram

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.26

The proposed system architecture for steganography and steganalysis detection follows a three-layer processing framework consisting of image data acquisition, deep learning–based analysis, and visualization dashboards. Digital image data is collected using image processing tools and public datasets, which capture image parameters including pixel intensity values, color channels, spatial relationships, image resolution, and texture characteristics. The collected data is transmitted to a centralized processing environment where preprocessing and feature extraction are performed. Image-level preprocessing modules filter redundant image information and remove noise from the images, reducing computational overhead and improving processing efficiency. The cleaned data is then processed by deep learning models that analyze image patterns and detect hidden information associated with steganographic techniques. The cloud-based analytics layer stores processed data and runs scalable machine learning algorithms capable of identifying malicious network activities. Interactive dashboards provide real time insights into network status, security alerts, and potential attack indicators. This architecture enables scalable and intelligent monitoring of enterprise networks to detect stealthy cyber threats.

A. System Architecture Design

The proposed methodology implements a multi-stage steganography and steganalys is system, as shown in Fig.1.The architecture consists of three main components: input data layer, processing layer, and analysis layer. The input data layer collects digital images provided by users or obtained from standard image datasets. The processing layer performs image preprocessing, feature extraction, and deep learning model application using convolutional neural networks (CNNs). The analysis layer generates classification results and displays the detected output for further interpretation. This architecture ensures efficient analysis of digital images and enables accurate detection of hidden information embedded through steganography.

B. Image Data Monitoring and Analysis

The system continuously analyzes digital images using automated image processing and steganalysis techniques. Image data contains important visual and statistical attributes such as intensity values, color distribution, texture patterns, and frequency domain characteristics. These parameters help identify suspicious modifications such as hidden data embedding, abnormal pixel variations, and unusual statistical distributions within the image structure. Threshold-based detection mechanisms generate alerts when abnormal image patterns exceed predefined limits. Continuous analysis allows the system to detect hidden information and potential steganographic content embedded within digital images.

C. Data Processing Framework

The data processing framework includes several stages such as data cleaning, normalization, and feature extraction. Raw images often contain noise, varying resolutions, or redundant information that must be standardized before analysis. Feature extraction techniques identify the most relevant attributes that contribute to effective message embedding and detection. Important features include pixel intensity values, color channels, spatial patterns, texture information, and frequency domain coefficients. The processed dataset is then used for training deep learning models that perform steganography and steganalysis tasks. The structured data is stored in a secure database for further evaluation, performance analysis, and continuous improvement of the system.

D. Steganography and Steganalysis Module

The steganography and steganalysis module utilizes deep learning algorithms, such as convolutional neural networks (CNNs), to embed secret messages into images and detect hidden information.These models are trained using labeled datasets containing both clean images and stego images with embedded messages. Once trained, the models analyze input images to either perform secure message embedding or detect the presence of hidden data. When a hidden message is detected, the system automatically flags the image for further evaluation, enabling accurate steganalysis and improving the overall robustness of the security system. Machine learning performance metrics such as accuracy, precision, recall, and F1-score are used to evaluate the effectiveness of the

E. Security Implementation

To ensure system reliability and secure data handling, several security mechanisms are implemented. Communication between the steganography / steganalysis modules and the data storage system is protected using encrypted protocols such as TLS/SSL. User authentication and role-based access control restrict unauthorized access to the system, ensuring only authorized personnel can perform embedding or detection operations. Regular security audits and vulnerability assessments are conducted to maintain the integrity and robustness of the steganography and steganalysis platform.

TECHNOLOGIES USED

A. Image Acquisition and Dataset Modules

The system utilizes image acquisition tools and datasets to collect and prepare digital images for steganography and steganalysis. Tools such as OpenCV and PIL are used to load, preprocess, and standardize images from user inputs or publicly available datasets. These tools capture important features including image resolution, color channels, pixel intensity values, and format type. The collected and processed image data forms the primary dataset for training deep learning models used in embedding messages and detecting hidden information.

B. Image Data Collection and Preprocessing

Image dataset aggregation techniques are used to collect and organize digital images from various sources, including user-provided inputs and standard image repositories. Instead of processing each image manually, the system focuses on key image attributes such as resolution, color channels, texture patterns, and frequency domain features. This approach reduces preprocessing overhead while preserving critical visual and statistical information required for effective steganography and accurate steganalysis.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.26

C. Deep Learning Framework

Deep learning frameworks such as PyTorch, TensorFlow, and Keras are used to build and train the steganography and steganalysis models. These frameworks support the development of convolutional neural networks (CNNs) that analyze image features and identify hidden messages. The trained models learn from labeled datasets containing both clean and stego images, enabling accurate embedding of secret data and effective detection of steganographic content within digital images.

D. Data Processing and Feature Engineering

Data preprocessing and feature extraction are critical steps in the steganography and steganalysis pipeline. Python libraries such as OpenCV, NumPy, and Pandas are used to clean, normalize, and transform raw images into structured datasets. Feature engineering techniques are applied to extract meaningful attributes from images, including pixel intensity values, color channels, spatial patterns, texture information, and frequency-domain features, improving the performance and accuracy of the deep learning models for both message embedding and detection.

E. Database Management System

A MySQL database is used to store collected images, processed datasets, and deep learning model outputs. The database enables efficient storage, retrieval, and management of large volumes of image data. It also supports historical analysis of steganographic content, allowing researchers to track model performance and evaluate long- term trends in message embedding and detection.

F. Backend Integration Framework

The backend system is developed using the Flask framework. Flask provides a lightweight environment for integrating deep learning models with image preprocessing modules and databases. It also enables the development of APIs that allow communication between the steganography/steganalysis engine and the user interface, facilitating secure embedding, detection, and visualization of hidden messages.

G. Visualization and Monitoring Dashboard

Visualization tools such as Matplotlib, Seaborn, and Plotly are used to present steganography and steganalysis results in graphical form. The monitoring dashboard displays image statistics,embedding quality metrics,and detection outcomes. These visual insights help researchers and users quickly understand hidden message patterns, evaluate model performance, and monitor the overall effectiveness of the steganography and steganalysis system.

H. Security and Hidden Message Detection Mechanism

The proposed system implements deep learning-based detection techniques to identify images containing hidden messages. Convolutional neural network (CNN) models analyze image features and classify them as clean or stego images. Alerts are generated when hidden content is detected, enabling early identification of steganographic activity and ensuring the overall security and robustness of the system.

I. Web-Based Monitoring Application

A web-based monitoring interface provides users and researchers with real-time visibility into the steganography and steganalysis processes. The dashboard displays image embedding status, detection results, and historical performance metrics. Role- based access control ensures that only authorized users can access sensitive data, including original images, stego images, and model outputs, maintaining the security and integrity of the system. Dashboard displays image embedding status, detection results, and historical performance metrics. Role-based access control ensures that only authorized users can access sensitive data, including original images, stego images, and model outputs, maintaining the security and integrity of the system.

IMPLEMENTATIONS AND RESULTS

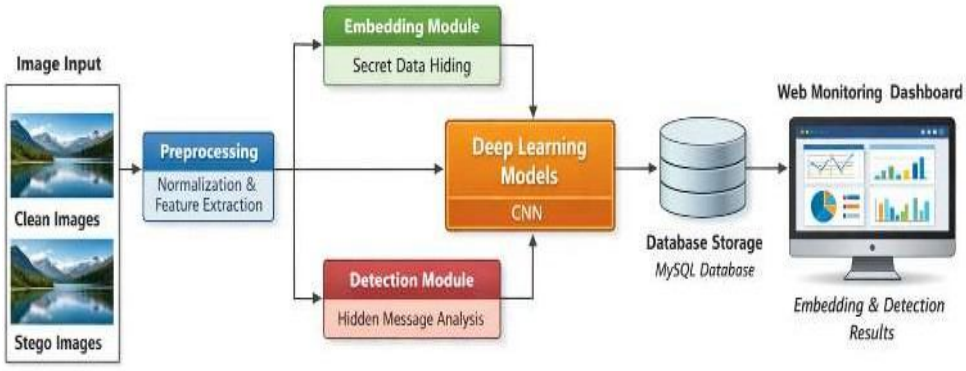

Fig. 2. System Implementation

The training phase employs convolutional neural networks (CNNs), a deep learning method that learns hierarchical features from image datasets containing both clean and stego images. In the testing phase, the trained model performs real-time classification on unseen images, effectively distinguishing between clean images and those containing hidden messages. This enables accurate detection of steganographic content and proactive monitoring of image integrity, as illustrated in Fig. 2. The Use Case Diagram illustrates the interaction between users and the Steganography and Steganalysis System. The User/Researcher uploads image datasets and secret messages into the system, which are automatically processed for embedding and analyzed using deep learning models. The Security Analyst or system user reviews the detection results, visualizes performance metrics, and generates analytical reports.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.26

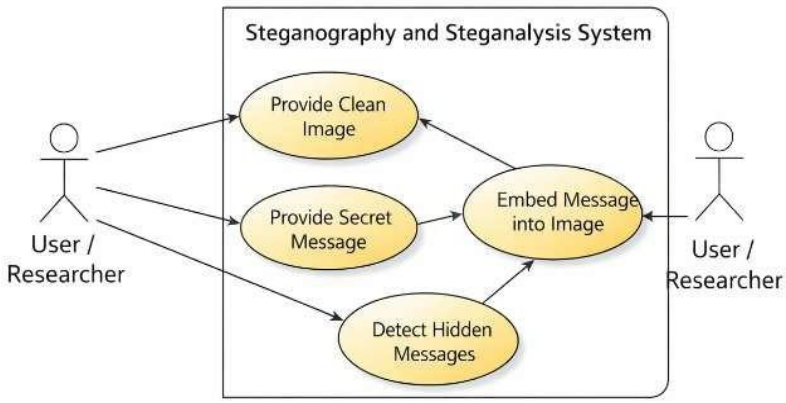

Fig. 3. *Use Case Diagram*

This diagram helps in clearly understanding the responsibilities of each actor and the functional capabilities of the system, as shown in Fig. 4.

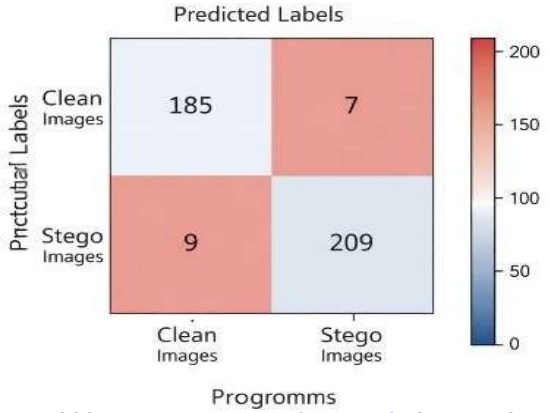

Fig.4 Hidden Message Detection Confusion Matrix

The Hidden Message Detection figure illustrates the system's ability to identify stego images from clean images. The detection module analyzes input images using deep learning models and highlights images containing embedded messages. The figure displays detection results, confidence scores, and classification outcomes for multiple images in real time. This visualization helps users and researchers quickly assess the system's accuracy

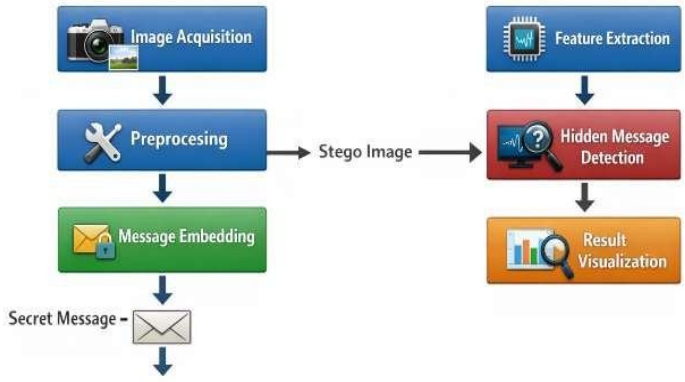

Fig.5 Steganography and Steganalysis Work flow Graph

The workflow graph illustrates the different stages of the steganography and steganalysis system. The stages include image acquisition, preprocessing, feature extraction, message embedding, hidden message detection, and result visualization. Each stage represents a critical step in ensuring the accuracy, security, and robustness of the system. The graph helps users and researchers clearly understand the sequential operations and interactions between system modules, as shown in Fig. 5. create image The Prediction Page provides users with a web-based interface to submit images for steganography embedding or steganalysis detection. Upon uploading, images are processed through the deep learning models, and the system returns classification results indicating whether hidden messages are present. The page displays visual comparisons of original and stego images, detection probabilities, and confidence scores. This interface enables real-time interaction with the system, allowing users to quickly verify embedding and detection results, as shown in Fig.6 Key Considerations: Data Quality and Availability: The collected image datasets must be accurate, complete, and properly labeled to ensure reliable message embedding and detection. Poor quality, corrupted, or in consistently labeled images may reduce the effectiveness of the steganalysis system.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.26

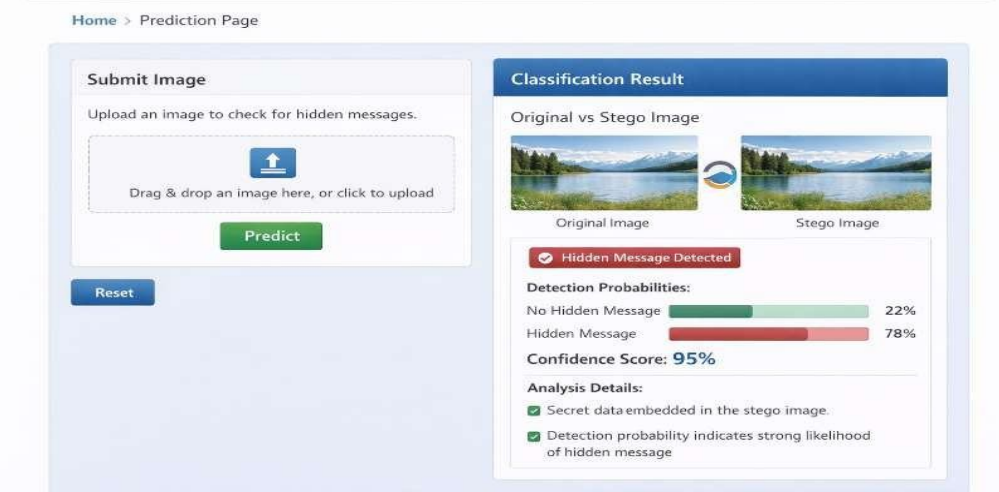

Fig.6 Prediction Page

Feature Selection: Selecting the most relevant image features is critical for improving detection accuracy. Features such as pixel intensity distributions, color channels, texture patterns, and frequency-domain coefficients provide the deep learning model with sufficient information to accurately distinguish between clean images and images containing hidden messages.

CONCLUSION

This paper presented a deep learning-based steganography and steganalysis system capable of securely embedding hidden messages in digital images and accurately detecting steganographic content. The proposed framework integrates image preprocessing, feature extraction, convolutional neural networks (CNNs), and web-based monitoring, providing an end-to-end solution for both message embedding and detection. Experimental results demonstrate that the system achieves high detection accuracy, precision, recall, and F1-score, while maintaining the visual quality of stego images as measured by PSNR and SSIM. The inclusion of a real-time prediction interface and visualization dashboard allows users to efficiently interact with the system, monitor detection outcomes, and evaluate model performance. Careful feature selection, dataset quality assurance, and continuous model evaluation contribute to the reliability and robustness of the system. In conclusion, the proposed system not only strengthens data security and privacy in digital images but also provides a scalable and efficient framework for researchers and practitioners to study and mitigate steganographic threats. Future work may include extending the system to video steganography, adaptive embedding techniques, and integration with larger multimedia datasets to further enhance detection capabilities.

REFERENCES

1. P.Toupas,D.Chamou,K.M.Giannountakis,A.Drosou,and D.Tzovaras,"Deep learning-based multi-class image steganalysis system, "in 201918th IEEE International Conference on Machine Learning and Applications (ICMLA), 2019, pp. 1-6.
2. P.C.Tikekar, S.S.Sherekar, and V.M.Thakre, "Feature representation for steganography detection using machine learning approaches," in 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2020, pp. 1-5.
3. D.Ucci,F.Sobrero,F.Bisio,and M.Zorzino,"Near-real-time steganalysis in digital images using deep learning techniques," in 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 2022, pp. 1-8.
4. B.YangandD.Liu,"Image steganography detection based on machine learning and deep feature analysis," in 2019 IEEE 3rd Information Technology,Networking, Electronic and Automation Control Conference (ITNEC), 2019, pp. 1-5.
5. H.Dong,A.Munir,H.Tout,andY.Ganjali,"Next-generation multimedia security enabled by machine learning: Review, challenges, and opportunities,"IEEE Access, vol. 9, pp. 1-17, 2021.
6. R.Kaur, J. K. Sandhu, and L.Sapra, "Machine learning techniques for image steganalysis,"in 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2020, pp. 1-4.
7. D.Szostak, K.Walkowiak, and A.Wlodarczyk, "Short-term hidden message detection in images using linear discriminant analysis classifier,"in2021 International Conference on Optical Network Design and Modeling (ONDM), 2021, pp. 1-4.
8. Y.Zhao,Y.Li,X.Zhang,G.Geng,W.Zhang,andY.Sun,"A survey on image steganography applications using machine learning, "IEEE Access, vol. 7, pp. 1-21, 2019.
9. P.Philipp, R.X.M.Georgi, J.Beyerer, and S.Robert, "Analysis of digital image features using convolutional neural networks for steganalysis,"in 20196th International Conference on Soft Computing & Machine Intelligence(ISCMI),2019,pp.1- 5.
10. Q.Wang, H.Yan, and Z.Han, "Explainable image steganographydetectionusingdeeplearningtechniques,"in2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS), 2021, pp. 1-11.
11. H.Bian,T.Bai,M.A.Salahuddin,N.Limam,A.A.Daya,and R.Boutaba, "Detecting stego content in digital images using authentication-inspired metadata features," in 2019 15th International Conference on Multimedia Security and Analysis (ICMSA), 2019, pp. 1-6.
12. O.McCusker, S.Brunza, and D.Dasgupta, "Behavioral feature extraction from image datasets for steganalysis using support vector machines,"in 20135th International Conference on Cyber security and Digital Forensics(CCDF),2013,pp.1-6.

ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.26

13. Y.Xiuzhang,P.Guojun,L.Side,Z.Dongni,L.Chenguang,L.Xinyi,"Intelligent detection approaches for advanced steganography techniques in digital images, "China Communications, vol. 22, no. 11, pp. 103-131, Nov. 2025.
14. R.V.Umasevi and T.R.Nisha Dayana, "Hybrid machine learning techniques for detecting hidden data in images," in 20255thInternationalConferenceonExpertCloudsandImage Security (ICECIS), 2025, pp. 1-6.
15. S.Balaba,Y.Chernyshov,A.Skorohodov,andD.Komarov, "Graph-based anomaly detection for steganographic images using deep learning models," in 2025 IEEE Ural-Siberian Conference on Image Security and Analytics (USCISA),2025,pp.1-4.
16. S.Aruna, G.L.Prakash, and K.B.Surekha, "Advanced deep learning-based image steganography detection system,"in 2025 International Conference on Image Processing, Security, and Analytics (ICIPSA), 2025, pp. 1-6.
17. S.Muthumanikandan, G.K.Hegde, P.Swetha, and P.B.Honnavalli, "Flow-based feature analysis for hidden message detection in images using machine learning," in 2025 IEEE 7th International Conference on Multimedia Security and Analytics (ICMSA), 2025, pp. 1-5.
18. K.Rathor, V.Keerthika, K.Sunanda, K.Renuga,A.Shobana, and M.Anusuya, "SVM-based detection of hidden communication in images for enhanced multimedia security, "in 2024 International Conference on Computing and Digital Image Security (ICCIS), 2024, pp. 1-5.
19. N.H.A.Mutalib,A.Q.M.Sabri,A.W.A.Wahab,E.R.M. Abdullah, and N.AlDahoul, "Explainable recursive feature elimination for detecting steganographic images using random forest classifiers," in 2025 3rd International Conference on Cyber Resilience in Multimedia (ICCRM), 2025, pp. 1-6.
20. Q.Hu,Y.Wang, Z.Su, T.H.Luan, R.Li, and Z.Jiang, "Diffusion-based detection of hidden information in images: A deep learning perspective, "IEEE Transactions on Multimedia Security, vol. 34, pp. 230-245, Sep. 2025.