"STEGO Malware Detection System"

Kakad Gauri Dilip[1], Junagade Sanika Bipinchandra[2], More Gauri Rajendra[3], Ahire Kunal Himmat[4], Asst. Prof. V. D. Mane[5]

[5]Guide

[1,2,3,4,5]AI&DS, Matoshri College Of Engineering And Research Centre, Nashik.

Abstract:
In the modern digital world, images are widely shared across online platforms, making them a potential medium for hidden cyber threats such as stegomalware. These threats embed malicious code within image files like GIF, PNG, and JPEG, often bypassing traditional security systems. This paper presents a stego malware detection system that uses a Convolutional Neural Network (CNN) to analyze images and identify hidden malware. The system includes image preprocessing and provides a web-based interface where users can upload images and receive real-time results. If a threat is detected, the system alerts the user and provides safety recommendations. The proposed solution ensures accurate detection, fast processing, and improved security against image-based cyberattacks.

Key Words: Detection, CNN, Image Malware, Cybersecurity, Deep Learning, Image Analysis, Web-Based System

INTRODUCTION

With the rapid growth of digital communication, images have become one of the most commonly shared forms of data across social media, websites, and messaging platforms. While images appear harmless, they can be used as a medium to hide malicious content through techniques such as steganography. This has led to the emergence of stegomalware, where harmful code is embedded within image files like GIF, PNG, and JPEG without altering their visible appearance. Such hidden threats can infect systems, steal sensitive data, or provide unauthorized access to attackers when the image is opened. Traditional antivirus systems mainly focus on executable files and often fail to detect malware concealed within images. This limitation creates a major security gap, especially as attackers increasingly use image-based techniques to bypass detection mechanisms. Additionally, existing tools are often complex and not user-friendly, making it difficult for general users to identify potential threats in images before accessing them.

To address this issue, this paper proposes an intelligent stego malware detection system using deep learning techniques. The system utilizes a Convolutional Neural Network (CNN) to analyze image patterns and detect hidden anomalies that may indicate malicious content. A web-based platform is developed to allow users to upload images and receive instant detection results. The primary aim of this system is to provide a simple, accurate, and efficient solution for identifying hidden malware in images, thereby enhancing cybersecurity and protecting users from image-based cyber threats.

LITERATURE SURVEY

The detection of malware hidden within digital images, commonly referred to as stegomalware, has gained significant attention in recent years due to the increasing use of steganography techniques in cyberattacks. Researchers have explored various approaches combining image processing, machine learning, and deep learning to improve detection accuracy and efficiency.

Alexis (2025) proposed a method for detecting stegomalware in PDF files using Kolmogorov Complexity. The study focused on identifying irregular patterns in file structures to improve detection accuracy and reduce false positives. While effective, the approach is limited to document-based files and does not directly address image-based malware detection.

Mohan (2024) presented a comprehensive survey on stegomalware in images, highlighting the use of machine learning models for pattern recognition and anomaly detection. The study emphasized the need for advanced

models capable of identifying hidden malicious content in images. However, it mainly focused on theoretical analysis rather than implementing a practical detection system.

Carrega (2020) introduced a programmable data gathering approach using Extended Berkeley Packet Filter (eBPF) for detecting stegomalware through system and network-level monitoring. This method improves real-time detection capabilities but does not focus specifically on analyzing image content directly.

Existing research shows that deep learning techniques, particularly Convolutional Neural Networks (CNNs), are highly effective for image analysis and pattern recognition. However, many existing systems either lack user-friendly interfaces, are limited to specific file types, or do not provide detailed threat interpretation. The proposed system addresses these gaps by implementing a CNN-based image analysis approach along with a web-based platform, enabling accurate, real-time, and user-friendly detection of hidden malware in images.

METHODOLOGY

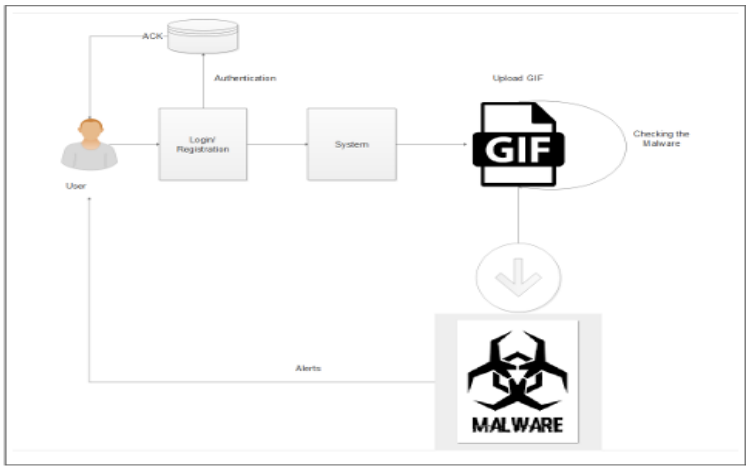
The proposed stego malware detection system follows a structured approach that integrates image processing, deep learning, and web-based deployment. The overall workflow consists of image acquisition, preprocessing, feature extraction, classification, and result generation. Initially, users upload image files such as GIF, PNG, or JPEG through a web-based interface. Since images may vary in size and quality, preprocessing is performed to standardize the input. This includes resizing the image, normalization, and noise reduction to enhance important visual features.

After preprocessing, feature extraction is carried out using a Convolutional Neural Network (CNN). The CNN automatically learns and extracts meaningful patterns from the image data, including hidden anomalies that may indicate the presence of malware. These features help in identifying subtle differences between safe and malicious images that are not visible to the human eye.

The extracted features are then passed through the classification stage, where the system determines whether the image is safe or contains hidden malware. Based on the prediction, the system generates the output and provides relevant information about the detected threat.

To make the system accessible, the trained model is integrated into a web-based platform. Users can upload images and receive real-time results along with alerts and safety recommendations if malware is detected. This methodology ensures accurate detection, efficient processing, and a user-friendly experience for identifying hidden threats in digital image.

BLOCK DIAGRAM



OBJECTIVE

1. To develop a system capable of detecting hidden malware in digital images such as GIF, PNG, and JPEG.
2. To implement a Convolutional Neural Network (CNN) for accurate image analysis and malware detection.
3. To provide real-time scanning results through a web-based platform.
4. To generate alerts and safety recommendations when malicious content is detected.
5. To create a user-friendly system accessible to both technical and non-technical users.

PROBLEM DEFINATIONS

Digital images can be used to hide malware through steganography, making them a serious cybersecurity threat. Existing security systems often fail to detect such hidden threats, especially in image files. Therefore, there is a need for an automated, accurate, and user-friendly system to detect malware embedded in images before they cause harm.

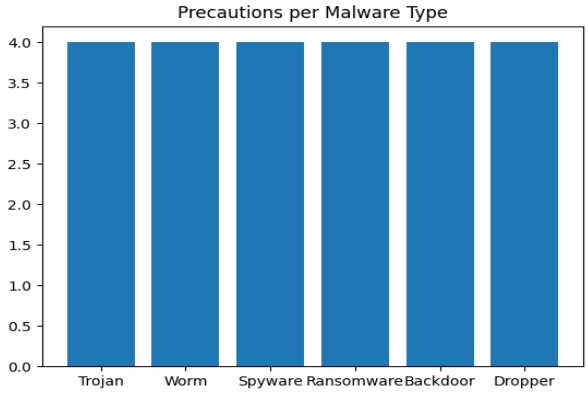
FUCTIONAL REQUIREMENTS

1. The system shall allow users to upload image files for scanning.
2. The system shall preprocess images before analysis.
3. The system shall detect hidden malware using a CNN model.
4. The system shall display results indicating safe or malicious images.
5. The system shall provide alerts and safety recommendations if malware is detected.

NON FUCTIONAL REQUIREMENTS

1. Performance: The system should provide fast and efficient detection results.
2. Accuracy: The model should achieve high detection accuracy with minimal errors.
3. Usability: The interface should be simple and user-friendly.
4. Security: User data and uploaded images must be securely handled.
5. Scalability: The system should support multiple users and large datasets.

RESULTS



The bar chart titled “Precautions per Malware Type” illustrates different categories of malware Trojan, Worm, Spyware, Ransomware, Backdoor, and Dropper and the number of precautions required to handle each type. The y-axis represents the number of precautions, while the x-axis lists the malware types.

All the bars have the same height, with a value of 4, indicating that each malware type requires four key precautionary measures. This uniformity shows that no malware category should be considered less dangerous or ignored.

From a system perspective, this means:

- Each malware type has comparable risk levels in terms of impact on security.
- The detection system should treat all malware types with equal importance during analysis.
- Users must follow multiple layers of protection, such as avoiding suspicious files, using secure platforms, keeping systems updated, and scanning files before opening.

Overall, the diagram highlights that effective cybersecurity is not dependent on a single precaution, but rather a combination of measures applied consistently across all types of malware threats.

IMPLEMENTAION

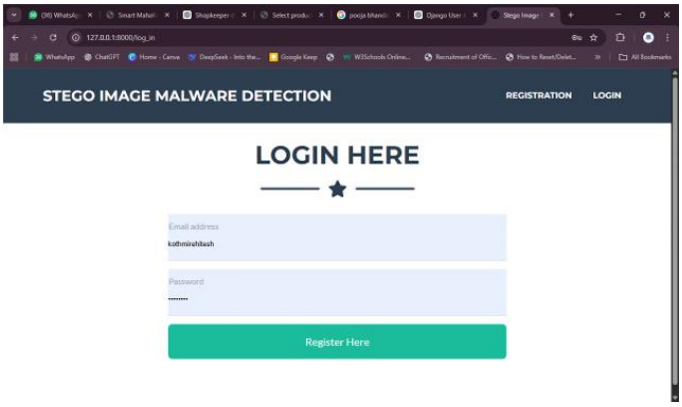


Fig: Home Page

Fig: Dashboard

CONCLUSION

The proposed system provides an effective solution for detecting hidden malware in digital images using a CNN-based approach. It ensures accurate detection, fast processing, and a user-friendly interface. The system enhances cybersecurity by allowing users to identify and avoid image-based threats, making it a reliable tool for safer digital communication.

REFERENCES:

[1] R. Chaganti, V. Ravi, M. Alazab, and T. D. Pham, "Stegomalware: A Systematic Survey of Malware Hiding and Detection in Images, Machine Learning Models and Research Challenges," *IEEE Access*, 2021.

[2] S. Freitas, R. Duggal, and D. H. Chau, "MalNet: A Large-Scale Image Database of Malicious Software," *IEEE*, 2021.

[3] A. Mihoub et al., "Malware Detection Using Deep Learning and CNN Models," in *Proc. IEEE Int. Conf. Cyberworlds (CW)*, 2023.

[4] Y. Song et al., "Application of Deep Learning in Malware Detection: A Review," *Journal of Big Data*, 2025.

[5] M. Masab et al., "Malware Image Classification Using Global Context Vision Transformer," *IEEE*, 2025.

[6] D. Gilkarov et al., "Steganography Detection and Malware Classification in Neural Networks," *IEEE Transactions*, 2025.

[7] D. M. Deepak et al., "A Hybrid Deep Learning Based Approach for Malware Detection and Classification," in *Proc. IEEE ICECCC*, 2025.

[8] M. S. K. P. et al., "HExNet: Enhancing Malware Classification through Explainable CNN Architecture," *IEEE Access*, 2025.

[9] R. Apau et al., "Image Steganography Techniques for Resisting Statistical Steganalysis Attacks," *IEEE Access*, 2024.

[10] L. Diana et al., "Overview on Intrusion Detection Systems for Cybersecurity," *IEEE Access*, 2025.