IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

Steganography Detection Using Kali Linux

Aditya Masawle[1], Kirtiraj Bansode[2], Sunil Dhere[3], Samarth Thorat[4], Prof. G. Solanke 5
Students, Department of AI & ML[1234]
Guide, Department of AI & ML[5]
Rasiklal M. Dhariwal Institute of Technology, Pune, Maharashtra

Abstract: *Steganography is a technique used to embed secret information in a digital medium like an image, audio, or video. Although it is used for secure communication, it is also used for spreading harmful information and illegal content. Thus, the detection of secret information is an important area in the field of cybersecurity.*
The objective of this project is to detect steganography using available tools in Kali Linux. Kali Linux is a Linux distribution that includes a variety of forensic and steganography detection tools, such as Steghide, Stegseek, Binwalk, and Zsteg, which can be used for detecting hidden data within a file.
The proposed system is designed to analyze suspicious files, detecting hidden messages using various steganalytical techniques. This enables investigators to determine whether secret messages have been embedded within digital files...

Keywords: Steganography, Kali Linux, Cybersecurity, Steganalysis, Digital Forensics.

I. INTRODUCTION

With the advent of digital communication, the practice of hiding information in multimedia messages has become common. Steganography is a technique for hiding messages in images, videos, and other multimedia messages.
While cryptography is used for hiding the contents of a message, steganography is used for hiding the message itself.
However, this method may also be misused for illegal communication, malware transmission, and cybercrime activities. Detection of such hidden information becomes necessary for security experts.
Kali Linux contains powerful tools that can be used for detection and analysis of Steganography. These tools help investigators detect and extract secret information from a file.

II. LITERATURE SURVEY

Several researchers have worked on steganography and steganalysis techniques.
Some have focused on Least Significant Bit (LSB) detection techniques, which involve identifying differences in the pixel values of an image where the hidden information is embedded.
Others have used statistical analysis techniques to identify abnormalities in digital media files that indicate hidden data.
Researchers have also used machine learning algorithms to identify patterns in hidden data in multimedia files.
Kali Linux is a widely used operating system for digital forensic analysis due to the availability of tools for steganography detection.

III. PROBLEM STATEMENT

Steganography is a method through which secret information is embedded inside digital media files such as images, audio, or videos. Even though steganography is helpful in secure communication, it is sometimes misused for illegal activities such as hiding malware, secret information, or messages.
Traditional methods of detecting steganography may not always prove helpful in detecting secret information. Therefore, a system is required that can help detect and analyze secret information.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, April 2026 Impact Factor: 8.2

Objective of the Project:
The main purpose of this project is to use tools available in Kali Linux to detect steganography in digital media files..

EXISTING SYSTEM
Some steganography tools provide users with the option to hide data in files.
Some examples include:
• Steghide
• OpenStego
• SilentEye
However, it is hard to detect such information in a file by using normal methods because the modifications made in a file are extremely minute and cannot be noticed by a human eye.

LIMITATIONS
However, the existing system also has some disadvantages:
• Hidden data is not easy to detect without specific tools
• Some steganography techniques are extremely sophisticated
• Detection using this method is time-consuming
• Some tools support only certain formats

MODULES
The system is composed of the following modules:
1. File Input Module
This module enables users to input suspicious files such as images or audio files for analysis.
2. Steganography Detection Module
In this module, the file is scanned using tools found in the Kali Linux operating system to detect any steganographycontent.
3. Data Extraction Module
In case the steganography content is detected, the module will attempt to extract the data.
4. Analysis Module
This module analyzes the extracted data and provides results to the user.

IV. PROPOSED SYSTEM

The tools used in this proposed system for detecting hidden information in multimedia files are Kali Linux tools.
The tools used for scanning suspicious files are as follows:
• Steghide
• Stegseek
• Binwalk
• Zsteg
• Exiftool
These tools are used for analyzing the structure of the suspicious files.
The system will generate a report stating whether hidden information is present in the suspicious files or not.

WORKING OF THE SYSTEM
1. User chooses a suspicious file.
2. The system uses Kali Linux tools to scan the file.
3. The tools scan the file's metadata and pixel patterns.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, April 2026 Impact Factor: 8.2

4. If found, the system extracts the hidden data.
5. The results are then shown to the user.
This process enables investigators to detect steganography in digital media files

SYSTEM ARCHITECTURE

The system architecture is composed of three levels:
Presentation Layer
This is where the user uploads files for analysis.
Processing Layer
This layer executes Kali Linux steganography detection tools.
Data Layer
This is where files and their results are stored.

HARDWARE REQUIREMENTS

- RAM: 8 GB
- Processor: Intel i5 or higher
- Hard Disk: 40 GB
- System: Laptop or Desktop

SOFTWARE REQUIREMENTS

- Operating System: Kali Linux
- Tools Used:
  - o Steghide
  - o Stegseek
  - o Binwalk
  - o Zsteg
  - o Exiftool
- Programming Language (optional): Python
- IDE: VS Code / Terminal

V. FUTURE SCOPE

The system can be improved by:

- Integrating machine learning for automatic steganography detection
- Supporting more file formats like video and audio
- Creating a graphical interface for easier analysis
- Developing real-time detection tools for cybersecurity monitoring

VI. CONCLUSION

The detection of steganography is crucial for cybersecurity and digital forensic purposes. The use of hidden information in multimedia files can be for legal or illegal purposes.
The project aims to show the use of Kali Linux tools in detecting hidden information from digital files.
The use of Kali Linux tools can help in the investigation of digital files and improve cybersecurity.

REFERENCES

[1]. N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography", IEEE Security & Privacy.
[2]. Johnson, N. F., "Steganography: Seeing the Unseen", Computer Journal.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

[3]. Kali Linux Official Documentation.
[4]. Jessica Fridrich, "Steganography in Digital Media".
[5]. Kali Linux Tools Documentation