International Conference on Science, Engineering & Management Trends

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Least Significant Bit (LSB)-Based Image and Audio Steganography for Covert Communication

Praveen [1], Nandika M [2], Jaraline Kirubavathy K [3]

[1,2] Department of Electronics and Communication Engineering, KCG College of Technology,India

[3] Assistant Professor, KCG College of Technology,India

Abstract- The word "steganography" is derived from the Greek words steganos (covered) and graphein (to write), and it refers to the art of concealing the very existence of a secret message within another, seemingly innocuous message or object. Unlike cryptography, which scrambles data so its meaning is obscured, steganography secures data by obscuring its existence. Media files such as images and audio are ideal for steganographic transmission due to their often large size and inherent redundancy, which allows for subtle, imperceptible modifications. This report focuses on digital image steganography and audio steganography, detailing the core principle of using the Least Significant Bit (LSB) method to embed secret data, a technique widely used for its simplicity. The objective is to provide an overview of these techniques, their working principles, and their significance in covert communication. The report also acknowledges that steganography, while having legitimate uses, can also be employed for malicious purposes, necessitating continuous research in steganalysis.

Index Terms — Audio steganography, covert communication, image steganography, least significant bit.

I. INTRODUCTION

This section introduces the concept of steganography—the practice of hiding information within another message or object such that the presence of the concealed information is not evident. Digital steganography most commonly employs multimedia files like documents, images, audio, or video as cover media (or carrier) to conceal a secret message, resulting in a stego-file.

The change made to the cover file is designed to be so subtle that it is unlikely to be noticed by an unsuspecting person.

I. Image Steganography

Image steganography involves hiding a secret message within a digital image. The main motive is to hide important information byte by byte within the image pixels. The size of the cover image must typically be larger than the size of the input message.

i. Least Significant Bit (LSB) Substitution

The LSB method is one of the simplest and most common techniques for image steganography.

- This technique uses pixel intensity to hide information.
- It works by replacing the least significant bit (the rightmost bit) of the cover image's pixel colour values (e.g., in an RGB image) with the bits of the secret message.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

- Changing the LSB of a color component is generally unnoticeable to the human eye, as it only results in a very slight, perceptually transparent change in color.
- The resulting image, known as the stego-image, is visually nearly identical to the original cover image but contains the hidden data.

II. Audio Steganography

Audio steganography uses an audio file as the carrier to conceal information. Digital audio formats like WAVE, MIDI, MPEG, and AVI can be used for this purpose.

i. Techniques for Audio Steganography

There are several methods used for embedding data in audio, including:

- Low Bit Encoding: Similar to the LSB method in images, this involves altering the least significant bits of the audio samples. While simple, this can create a predictable distortion that is easily detectable by steganalysis methods.
- Phase Coding: This technique embeds the secret message by modifying the phase of the audio signal's frequency components.
- Spread Spectrum: This involves embedding the message by spreading it over a wider range of the audio frequency spectrum.
- Transform Domain Methods: Techniques like modifying the Discrete Cosine Transformation (DCT) values of the audio signal's frequency components are also employed.

II. PROJECT OVERVIEW AND OBJECTIVE

I. Name and Objective

- Project Name: StegoVault

- Objective: To create a secure, user-friendly, and accessible web application that performs Least Significant Bit (LSB) steganography on digital media. The application allows registered users to hide secret text messages within cover files (Images and Audio) and later extract the messages, facilitating covert communication.

II. Core Features Implemented

- User Authentication: Secure registration and login using a JSON-based database for persistence.
- Image Steganography: Hiding and revealing text messages in lossless image formats (PNG and BMP) using the stegano library.
- Audio Steganography: Hiding and revealing text messages in lossless audio formats (WAV) using a custom, robust LSB implementation based on numpy and scipy.io.wavfile.
- File Management: User-specific file naming and retrieval to prevent unauthorized access.
- Web Deployment: Successful deployment as a production-ready web service.

III. TECHNOLOGY STACK AND DEPENDANCIES

I. Core Framework

Technology	Function
Flask	The lightweight web framework providing routing, sessions, and template rendering[2].

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Technology	Function
Flask-Session	Manages server-side sessions to maintain user login state[3].
Jinja2	Template engine used to render the dynamic HTML pages[4].
Gunicorn	Production-grade WSGI HTTP Server used for reliable hosting on Render[5].

II. Libraries Used For Steganography And Data Handling

- stegano: Primary tool for Image Steganography on PNG and BMP files2. It uses
- Image LSB (Least Significant Bit) in the spatial domain3.
- Pillow (PIL): Used by the stegano library and for mandatory image mode conversion (e.g., to RGB) to ensure reliable LSB hiding4.
- numpy: Essential for fast array manipulation, specifically flattening and reshaping audio data arrays5.
- scipy.io.wavfile: Used for reading (wavfile.read) and writing (wavfile.write) uncompressed WAV audio files6.
- json: Used for reading and writing the local user database (users.json)7.

III. METHODOLOGY AND CORE EXPLANATION

I. Least Significant Bit (LSB) Steganography

LSB is the simplest and most common steganography technique.

- Principle: Every digital file (image or audio) is composed of bytes, and each byte has 8 bits. The
- Least Significant Bit (LSB) is the rightmost bit of a byte.
- Effect: Changing the LSB results in the smallest possible alteration to the cover medium's perceived quality.
- In Images: Secret messages are hidden by replacing the LSB of one or more color channels (Red, Green, Blue) of each pixel with a bit from the secret message.
- In Audio (WAV): Messages are hidden by replacing the LSB of the digitized audio sample values.

II. Audio Steganography implementation

A custom solution was developed for audio LSB because standard libraries often lack robust, platform-independent support.

1. Message Conversion: The secret string is converted into a long binary string. A specific delimiter (
2. ### which is '0010001100100011001000011' in binary) is appended to mark the end of the message. This allows the extraction function to stop precisely when the message ends.
3. Audio Processing: The WAV file is read using scipy.io.wavfile. The resulting audio data array (1D for mono, 2D for stereo) is immediately flattened using
4. numpy to create a continuous stream of sample values for embedding.
5. Embedding (LSB Manipulation): The message bits are embedded by manipulating the LSB of each audio sample in the flattened array:

- audio_array[i] = audio_array[i] & 254: This clears the current LSB (sets it to 0) using a bitwise AND operation with the binary value 11111110.
- If the message bit is '1', then audio_array[i] = audio_array[i] | 1 sets the LSB to 1 using a bitwise OR operation with 00000001.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

4. Extraction: The process iterates through the audio samples, extracts the LSB of each sample using (sample & 1), and concatenates them to form a binary string. The loop terminates when the delimiter pattern is found.

III. The challenge of Lossy Compression

A critical limitation of LSB was identified relating to data loss:

- Problem: When an embedded file (like a PNG) is shared through services like WhatsApp, the service often applies lossy compression (e.g., converting PNG to JPG).
- Result: This compression alters the LSBs, which corrupts the hidden message and makes it unrecoverable.
- Mitigation: The only solution is to instruct users to share embedded files as a document or file attachment to preserve the original, unaltered LSB data.

IV. DEVELOPMENT AND DEPLOYMENT SUMMARY

I. Development:

The StegoVault application was developed using Python 3.x and employed a local flat file (users.json) for its database.

II. Deployment Statergy:

The application was deployed to a production environment using a Platform as a Service (PaaS) model.

- Repository Setup: The project files (including app.py, templates/, and requirements.txt) were committed to a GitHub repository named StegoVault-website.
- Configuration: The project was configured for production via:
  requirements.txt: This file lists all dependencies, including the production server Gunicorn.
  Procfile: This specifies the command to start the web service: web: gunicorn app:app.
- Hosting Platform: The application was successfully deployed on Render as a Web Service.
- Security: A secure, generated SECRET_KEY was set as an environment variable in Render to secure the Flask application's session cookies.

III. Final Result

The StegoVault web application is live and publicly accessible, providing users with a functional, secure platform for LSB-based steganography

V. GLOBAL CASES

I. A recent report by *India Today* revealed that Pakistani hackers have launched a sophisticated cyber espionage campaign targeting India's "Make in India" defence programs. The operation, conducted by a Pakistan-based hacking group, specifically aimed at Indian defence officials and state-run defence contractors, potentially compromising highly sensitive data. This attack underscores the growing threat of cyber warfare and the vulnerability of critical national projects to foreign adversaries, highlighting the urgent need for enhanced cybersecurity measures in India's defence sector.

II. According to a report by *The New York Times*, Chinese hackers have repeatedly infiltrated Russian systems since 2022 in an effort to obtain sensitive military secrets. The sustained cyberattacks highlight the complex and often covert nature of global cyber-espionage, where even strategic partners engage in intelligence gathering against each other. This development underscores the increasing role of cyber

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

warfare in international relations and raises concerns over the security of critical military data in the digital age.

III. A report by *The Print* revealed that hackers accessed and put up for sale on the dark web around 20TB of highly sensitive data belonging to the Defence Ministry. The compromised information allegedly included a 'secret' document linked to a strategic defence project, raising serious concerns over national security. This breach not only exposes glaring lapses in cybersecurity infrastructure but also emphasizes the urgent need for stronger protective measures to safeguard critical military information from exploitation by hostile entities.

IV. According to a *Reuters* report, the United States and its allies have accused North Korean hackers of stealing sensitive military secrets through cyber intrusions. These operations, attributed to state-backed groups, highlight Pyongyang's growing reliance on cyber-espionage as a tool to strengthen its strategic and military capabilities. The allegations underscore the persistent threat posed by North Korea's cyber activities to global security, raising concerns over the vulnerability of critical defence information worldwide.

V. A report highlighted by *Politico* revealed that a Russian spy leak has exposed significant risks to Germany's military communications, raising alarms about broader cybersecurity weaknesses within the Bundeswehr. The incident, currently under investigation by German authorities, has prompted cybersecurity experts to call for accountability and stronger safeguards. This breach underscores the growing vulnerability of military systems to espionage and the urgent need for comprehensive measures to protect sensitive defence communications.