WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

INFORMATION HIDING USING STEGANOGRAPHY

Jeeshan Siddiqui[1], Sayyed Hasan[2]

Computer Science and Engineering Department
Shri Shankaracharya Technical Campus, Bhilai, Chhattisgarh, India

ABSTRACT:

Steganography refers to the practice of hiding sensitive data within non-secret digital media to ensure secure communication. As public data sharing becomes increasingly prevalent, concealing information within digital formats—particularly images—has gained importance. This paper explores various steganographic techniques, with a primary focus on digital images, and examines their benefits, limitations, and application compatibility. A comparative analysis highlights the most effective approaches for specific use cases.

1. Introduction

The term *steganography* originates from two Greek words: *steganos* (meaning "covered") and *graphein* (meaning "writing"), together translating to "covered writing." It involves concealing data in a seemingly innocuous medium so that its presence remains unnoticed. In today's digital landscape, the exchange of sensitive data necessitates enhanced security mechanisms.

While both **cryptography** and **steganography** aim to protect information, their methodologies differ. Cryptography transforms information into an unreadable format using encryption, making it secure but still visible as protected content. In contrast, steganography hides the existence of the information itself, leveraging human perception limitations.

Steganographic techniques can be applied across a variety of media: text, audio, video, and images. This paper emphasizes image-based methods, given their popularity in online communications.

2. Common Steganographic Mediums

1. **Image Steganography**: Utilizes the pixel intensity values of images to embed data.
2. **Video Steganography**: Embeds information into video frames using techniques such as the Discrete Cosine Transform (DCT).
3. **Audio Steganography**: Hides data within audio files (e.g., WAVE, MP3), which is highly relevant with the rise of VOIP.
4. **Network Steganography**: Uses communication protocols (e.g., TCP, UDP) to conceal data.
5. **Text Steganography**: Encodes messages using spacing, font styles, or hidden characters.

3. Characteristics of an Effective Steganography System

- **Accuracy**: Extracted data should match the original hidden content.
- **Capacity**: The system should support a high volume of embedded data.
- **Robustness**: Data must survive standard processing like compression or scaling.
- **Privacy**: Unauthorized parties should not detect or extract the hidden message.

4. Steganographic Standards

- **Payload Capacity**: Indicates how much secret data can be embedded.
- **Imperceptibility**: The changes in the host media should be visually or audibly undetectable.
- **Security**: The stego content should resist steganalysis or detection.
- **Efficiency**: Fast embedding and extraction with minimal computational cost.
- **Quality Preservation**: Host media quality must remain unaffected.
- **Undetectability**: Human observers shouldn't perceive any difference in the media.

5. Terminology

- **Cover Image**: The original, unaltered image used for embedding.

- **Stego Image**: The image after data has been embedded.
- **Message**: The data to be hidden (e.g., text, another image).
- **Stego Key**: A password or key used to extract hidden data.
- **Embedding Algorithm**: Method used to insert the message.
- **Extraction Algorithm**: Process used to recover the hidden message.

6. Steganographic Techniques

A. Frequency Domain Methods

- **DCT (Discrete Cosine Transform)**: Converts spatial data into frequency components for embedding.
- **DWT (Discrete Wavelet Transform)**: Uses wavelets to embed information at different resolutions.
- **DFT (Discrete Fourier Transform)**: Represents the signal in frequency space for data embedding.

B. Spatial Domain Methods

- **Pixel Value Differencing (PVD)**: Determines pixel intensity differences to embed data.
- **Edge-Based Embedding**: Hides data in edge areas detected using algorithms like Canny.
- **Least Significant Bit (LSB)**: Modifies the LSB of pixel data to insert secret bits.
- **Random Pixel Embedding**: Distributes data randomly across image pixels.

LSB Pros:

- Minimal distortion of the cover image
- High embedding capacity

LSB Cons:

- Vulnerable to simple attacks or image processing
- Weak robustness under transformations

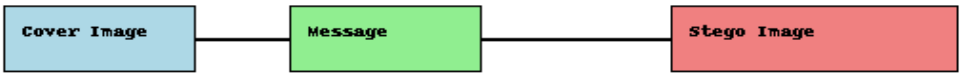
7. Bitmap-Based Image Steganography

Bitmap (BMP) images are preferred due to their uncompressed format and simplicity. A pixel in a BMP image is made up of three components (RGB), and data is embedded in the least significant bits of these components.

For example, using three pixels, one byte of data can be hidden:

```
yaml
CopyEdit
Pixel 1: 01110101 01010101 11101100
Pixel 2: 11010010 10010101 00010100
Pixel 3: 10110010 10011100 01101011
```

The application embeds data from the least significant bit plane upwards to maintain visual fidelity. The decryption process reverses this to recover the original file.



8. System Implementation

The proposed system allows users to:

- Load any image format
- Select a file to embed
- Encrypt it using a multi-layered LSB method
- Generate a stego image in BMP format

To extract data:

- The user selects the stego image
- Decryption algorithm retrieves both the hidden file and the original image

9. Result & User Interface

The interface includes:

- Tabs for encryption and decryption
- Fields for image and file selection
- Status panel showing image metadata (size, height, width)

Steps:

1. Choose encryption tab
2. Browse and select image
3. Select file to hide
4. Click Encrypt to generate BMP image
5. Choose decryption tab and select encrypted image
6. Set destination folder and decrypt

A success message confirms the hidden file retrieval.

10. Conclusion

This paper presents a comprehensive overview of steganography and its implementation using digital images. A multi-format image hiding approach is proposed that leverages LSB embedding and BMP output to ensure flexibility, efficiency, and security.

REFERENCES:

1. Mukesh Garg, Gurudev Jangra. *"An Overview of Different Types of Data Hiding Schemes in Image Using Steganographic Techniques"*, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 1, Jan 2014.
2. Namrata Singh. *"Survey Paper on Steganography"*, International Refereed Journal of Engineering and Science (IRJES), Vol. 6, Issue 1, Jan 2017.
3. Yunura Azura Yunus, Salwa Ab Rahman, Jamaludin Ibrahim. *"Steganography: A Review of Information Security Research and Development in Muslim World"*, American Journal of Engineering Research (AJER), Vol. 2, Issue 11.
4. Dr. Rajkumar L Biradar, Ambika Umashetty. *"A Survey Paper on Steganography Techniques"*, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 1, Jan 2016.
5. T. Morkel, J.H.P. Eloff, M.S. Olivier. *"An Overview of Image Steganography."*
6. Samer Atawneh, Ammar Almomani, Putra Sumari. *"Steganography in Digital Images: Common Approaches and Tools"*, IETE Technical Review, Vol. 30, Issue 4, Jul-Aug 2013.
7. Various Authors. *"Mastering C#", "SQL Server Bible", ".NET Black Book".*