CAPSTONE PROJECT

Secure Data Hiding in Image Using Steganography

Presented By
Student Name : Tushar Raha
College Name & Department : Vidya Vihar Institute of Technology &
B.Tech Computer Science

edunet
foundation

OUTLINE

- **Problem Statement**
- **Technology used**
- **Wow factor**
- **End users**
- **Result**
- **Conclusion**
- **Git-hub Link**
- **Future scope**

Problem Statement

The problem involves securely hiding sensitive data within an image using steganography to ensure confidentiality and prevent unauthorized access. Traditional encryption methods make hidden data noticeable, whereas steganography conceals it within image pixels without altering the visual appearance. The challenge is to develop an efficient algorithm that embeds and extracts data while maintaining image quality and security.

Technology used

Libraries Used:
    Standard Libraries: stdio.h, stdlib.h, string.h
    Custom Header: "steganography.h"

Platforms:
    Operating System: Ubuntu 20.04
    Compiler: GCC
    File Format: BMP (Bitmap Image)

Additional Points:
    Steganography Method: Least Significant Bit (LSB) Encoding
    Data Handling: Embeds and extracts text data from images

Wow factors

1 **LSB-Based Steganography – Hides data in the Least Significant Bit, ensuring security without visible image changes.**

2 **Lossless BMP Processing – Works with uncompressed BMP images to maintain data integrity.**

3 **Lightweight & Fast – Written in C for high efficiency, outperforming Python/Java-based tools.**

**4** **Simple CLI Interface – Easy command-line usage for embedding and extracting data, ideal for automation.**

End users

1 **Cybersecurity Professionals** – Use steganography for secure data transmission and covert communication.

2 **Forensic Experts** – Extract hidden information from images for digital investigations.

3 **Government & Defense Agencies** – Securely embed sensitive data in images for intelligence and confidential operations.

4 **Researchers & Academics** – Study and improve steganographic techniques for data security and cryptography.

5 **Privacy-Conscious Users** – Individuals who want to protect personal or confidential information from unauthorized access.

Results
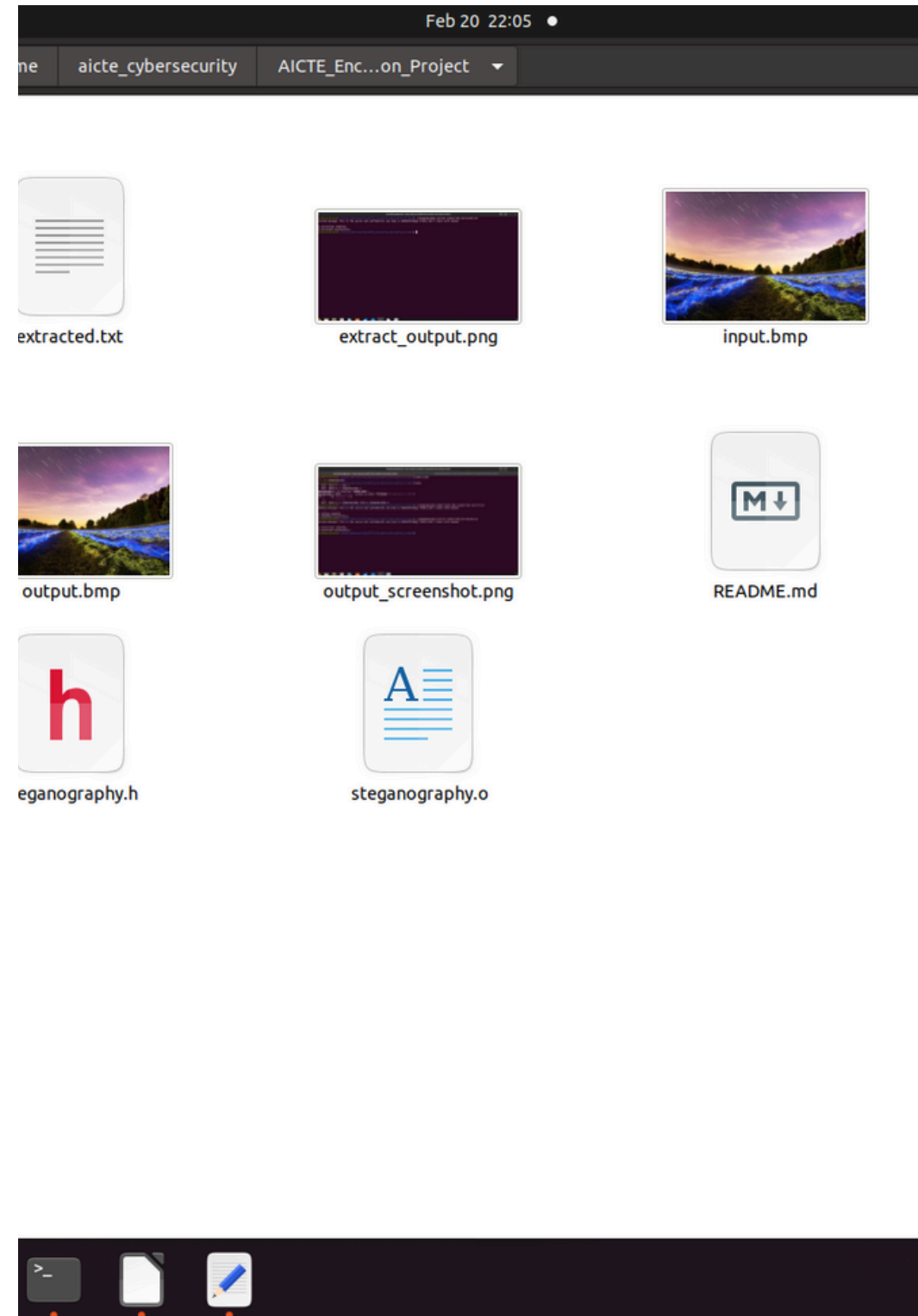
Conclusion

This project successfully addresses the challenge of securely hiding data within an image using LSB-based steganography. By modifying the Least Significant Bit (LSB) of pixel values in BMP images, it ensures that sensitive information remains hidden without noticeable visual changes. The approach maintains data integrity, works efficiently with minimal dependencies, and provides a simple CLI interface for embedding and extracting data.

While the current implementation supports BMP files, it can be extended to support other formats like PNG or use DCT-based methods for JPEG. This project provides a lightweight, fast, and secure solution for data confidentiality, making it useful for cybersecurity, forensics, and private communication.

GitHub Link

- https://github.com/Tushar552/AICTE-IBM-Cybersecurity-Internship-
- Description:
- This project implements Least Significant Bit (LSB) steganography to hide and extract secret messages within BMP images.

- Repository Contents:
- 📂 Source Code – C programs for embedding and extracting hidden messages.
- 📂 Sample Images – BMP images used for testing steganography.
- 📂 Documentation – Project report, explanations, and implementation details.
- 📂 Presentation – PPT slides summarizing the project.

Future scope(optional)

- 🖥️ Graphical User Interface (GUI) – Develop a user-friendly GUI to make embedding and extracting messages easier.
- 📂 Drag and Drop Support – Allow users to select images and messages through a simple drag-and-drop interface.
- 🛠️ Customization Options – Provide settings for users to adjust the encoding method and choose different bit depths.
- 📊 Real-time Preview – Show a preview of the image before and after steganography is applied.

THANK YOU

edunet
foundation