Report on Steganography Tool for Image/File Hiding

Objective

The objective of this project is to design and implement a steganography tool that can hide text or files inside image files. The method used is Least Significant Bit (LSB) substitution, which changes the lowest bit of each pixel value to store hidden data without altering the visible appearance of the image. This makes the approach suitable for concealing information in plain sight.

Tools Used

- Python – programming language used to build the tool
- PIL (Pillow) – library for image processing
- stepic – lightweight library for simple LSB steganography (can be replaced or combined with custom LSB logic)
- Tkinter – for building the graphical user interface (GUI)

Mini Guide to Implementation

- **Convert message to binary and embed in image LSB:**

Input text or file data is first converted into a binary bitstream. Each bit is then stored in the least significant bit of image pixels, ensuring minimal visual changes.

- **Allow uploading image + hidden message:**

Users can select a cover image (PNG or BMP) through the GUI. They can either type text directly or upload a file to be hidden inside the image.

- **Extract and decrypt (optional) from modified image:**

The tool reads the LSBs from the modified image to reconstruct the hidden data. If the payload was encrypted, the tool provides an option to enter a password for decryption.

- **Add drag-and-drop GUI:**

A simple Tkinter GUI allows file browsing. Optional drag-and-drop support makes adding images and payloads more convenient.

- **Support image formats like PNG, BMP:**

Only lossless formats are supported to preserve hidden data. PNG and BMP are ideal, while JPEG is avoided due to its lossy compression.

Deliverables

- Working GUI-based steganography application.
- Ability to hide text or files inside PNG/BMP images.
- Option to extract and decrypt hidden data.
- Simple and user-friendly interface with drag-and-drop.
- Demonstrates practical application of LSB steganography.

Conclusion

This project demonstrates the practical use of steganography for information hiding. It combines fundamental concepts of binary data manipulation with a graphical interface to make the process accessible. By supporting both text and file embedding, optional decryption, and common image formats, the tool serves as both a learning project in cybersecurity and a useful utility for concealing information.