**Project 1: LSB Image Steganography**

**Abstract Summary**

Steganography is the technique of hiding secret information within other non-suspicious files—most commonly digital images. Unlike cryptography, which makes data unreadable, steganography conceals the very existence of the data. This project implements a simple image-based steganography method using the Least Significant Bit (LSB) technique on BMP files to embed and extract hidden text.

**Project Requirements**

* Accepts a .bmp image and a .txt secret file
* Verifies that the image has enough capacity to embed the message
* Embeds a **magic string** for stego image verification
* Supports **decode mode** to extract the hidden message
* Operates via **command-line arguments only**

**Pre-Requisites**

* Understanding of:
  + File I/O
  + Pointers and Structures in C
  + Basic encryption/decryption logic

**Project Complexity**

* Level: **Medium**
* Focus: Bitwise operations, BMP file format understanding, CLI design

**🔗 References**

* [Wikipedia – Steganography](https://en.wikipedia.org/wiki/Steganography)
* [Wikipedia – BMP File Format](https://en.wikipedia.org/wiki/BMP)

**Sample Usage**

For Encoding ./a.out -e beautiful.bmp secret.txt [stegno.bmp]

For Decoding ./a.out -d stegno.bmp [data.txt]

[stego.bmp] [data.txt] optional not necessary if not provided default name will be assigned

Command line argument for use:

./a.out -e beautiful.bmp secret.txt

./a.out -d stegno.bmp