Instituto Tecnológico de Buenos Aires

StegoBMP

72.44 Criptografía y Seguridad - 2024Q1

Tomás Marengo - 61587

tmarengo@itba.edu.ar

Índice

1. Introducción

La esteganografía es la práctica de ocultar información dentro de otro objeto, de manera que su existencia no sea perceptible a simple vista. A lo largo de la historia, se han utilizado diversas técnicas esteganográficas para proteger la confidencialidad de la información. En el contexto digital, una de las técnicas más comunes consiste en ocultar datos en archivos de imagen modificando sus bits menos significativos (LSB, por sus siglas en inglés).

Este trabajo práctico tiene como objetivo implementar y probar un sistema de esteganografía digital utilizando diferentes métodos de inserción en los bits menos significativos de imágenes BMP. Además, se exploran técnicas de cifrado para proteger la información antes de ocultarla, garantizando así una capa adicional de seguridad. El objetivo es garantizar que la información sea indetectable y, en caso de ser descubierta, inaccesible sin la clave adecuada.

2. Diseño del sistema

El sistema está diseñado en una arquitectura modular que consta de las siguientes partes:

- **Operator:** Clase base que contiene los parámetros comunes a las operaciones de ocultamiento y extracción.
- **Embedder:** Clase derivada de Operator, responsable del ocultamiento de datos en una imagen BMP.
- **Extractor:** Clase derivada de Operator, responsable de la extracción de datos de una imagen BMP.
- **SteganographyUtil:** Contiene métodos estáticos para la encriptación y desencriptación de datos, así como constantes utilizadas en todo el sistema.
- **Steganography:** Punto de entrada del programa que parsea los argumentos de la línea de comandos y coordina las operaciones de ocultamiento y extracción.

3. Stegoanálisis de los archivos provistos

4. Cuestiones a Analizar

- *Discutir los siguientes aspectos relativos al documento.*
  - *a) Organización formal del documento:*
    - **Respuesta:**
  - *b) La descripción del algoritmo:*
    - **Respuesta:**
  - *c) La notación utilizada, ¿es clara? ¿hay algún error o contradicción?*
    - **Respuesta:**
- *Esteganografiar un mismo archivo en un .bmp con cada uno de los tres algoritmos, y comparar los resultados obtenidos. Hacer un cuadro comparativo de los tres algoritmos estableciendo ventajas y desventajas.*
  - **Respuesta:**
- *Explicar detalladamente el procedimiento realizado para descubrir qué se había ocultado en cada archivo y de qué modo. Indicar qué se encontró en cada archivo.*
  - **Respuesta:**
- *Algunos mensajes ocultos tenían, a su vez, otros mensajes ocultos. Indica cuál era ese mensaje y cómo se había ocultado.*
  - **Respuesta:**
- *Uno de los archivos ocultos era una porción de un video de una película, donde se ve ejemplificado una manera de ocultar información. ¿Qué se ocultaba y sobre qué portador?*
  - **Respuesta:**
- *¿De qué se trató el método de esteganografiado que no era LSB1 ni LSB4 ni LSBI? ¿Es un método eficaz? ¿Por qué?*
  - **Respuesta:**
- *¿Por qué la propuesta del documento de Majeed y Sulaiman es realmente una mejora respecto de LSB común?*
  - **Respuesta:**

- *En la implementación se optó por guardar los patrones invertidos al final del mensaje. ¿Es esta una opción más segura que guardarlos antes del mensaje? ¿Por qué?*
  - **Respuesta:**
- *¿De qué otra manera o en qué otro lugar podría guardarse el registro de los patrones invertidos?*
  - **Respuesta:**
- *¿Qué dificultades encontraron en la implementación del algoritmo del paper?*
  - **Respuesta:**
- *¿Qué mejoras o futuras extensiones harías al programa stegobmp?*
  - **Respuesta:**