INSTITUTO TECNOLÓGICO DE BUENOS AIRES

Ingeniería Informática

Trabajo Práctico de Implementación

Esteganografía en Imágenes BMP

Criptografía y Seguridad (72.04)

Grupo 2

Santiago Mesa Rubio, 63162
Manuel José Santamarina Balbín, 63622
Matias Sapino, 61067

2025

Índice

1. Introducción **3**

2. Estegoanálisis y cuestiones a analizar **3**

1. Introducción

La esteganografía es la disciplina que estudia técnicas para ocultar información dentro de objetos aparentemente inocuos, de modo tal que no sólo se proteja el contenido del mensaje, sino también su existencia. A diferencia de la criptografía clásica, que se centra en volver ininteligible el mensaje, la esteganografía apunta a que el mensaje pase desapercibido para un observador no autorizado.

En este trabajo práctico se implementó el programa `stegobmp`, que permite ocultar y extraer archivos arbitrarios dentro de imágenes BMP de 24 bits sin compresión, utilizando distintos algoritmos basados en la modificación de los bits menos significativos (LSB). Además, se incorporó la posibilidad de combinar esteganografía con criptografía simétrica (AES y 3DES en distintos modos de operación), reforzando la confidencialidad de la información.

2. Estegoanálisis y cuestiones a analizar

I. **Discutir los siguientes aspectos relativos al documento.**

a) **Organización formal del documento.**
El paper sigue la estructura típica de un artículo científico: *Abstract*, *Introducción*, explicación de LSB tradicional, descripción del método propuesto (técnica de inversión de bits y luego el algoritmo), sección de resultados y conclusiones.

b) **Descripción del algoritmo.**
El algoritmo propuesto primero aplica LSB estándar en los planos verde y azul, ocultando los bits del mensaje en el LSB de cada píxel. Luego clasifica los píxeles según el patrón formado por su 2.º y 3.er bit (00, 01, 10, 11) y compara, para cada patrón, cuántos píxeles cambiaron tras el embedding y cuántos no. Si en un patrón hay más píxeles modificados que sin modificar, invierte el LSB de todos los píxeles de ese patrón, reduciendo así el número total de cambios. Finalmente, guarda un mapa de qué patrones fueron invertidos para poder revertir la operación durante la extracción.

c) **Notación utilizada (claridad, errores, contradicciones).**
La notación es en general clara, aunque con algunos typos y pequeñas inconsistencias entre "secret message" y "secret image". Nada de eso impide reconstruir el algoritmo.

II. **Esteganografiar un mismo archivo en un .bmp con cada uno de los tres algoritmos y comparar los resultados obtenidos.**

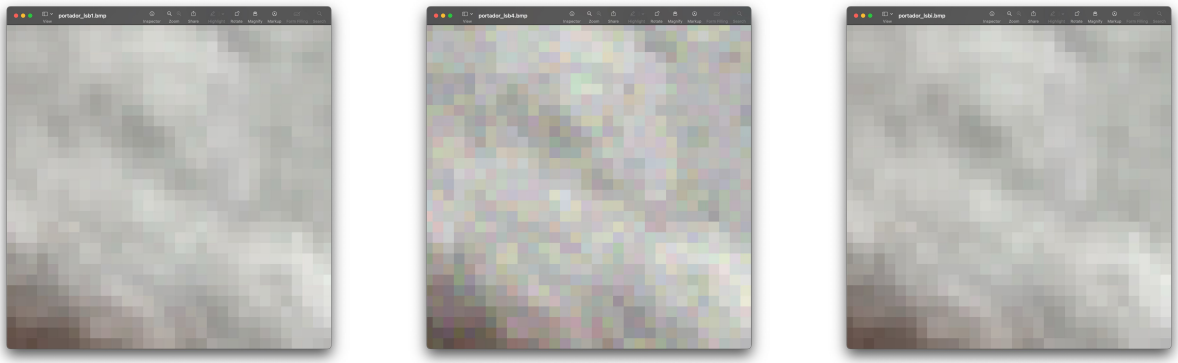


Figura 1: Imágenes encriptadas con LSB1, LSB4 y LSBI (zoom al máximo).

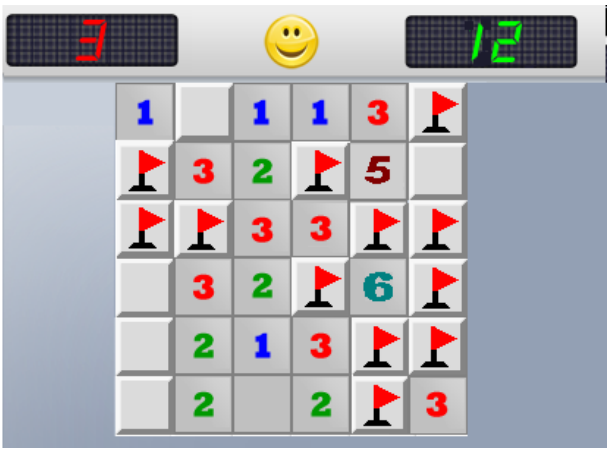
Algoritmo	Cómo funciona	Ventajas
LSB1	Modifica solo el bit menos significativo de cada componente del píxel.	Alteración mínima del píxel; fácil de implementar; baja detectabilidad.
LSB4	Modifica los 4 bits menos significativos de cada componente.	Alta capacidad; inserción rápida.
LSBI	Inserción adaptada según correlación entre píxeles.	Difícil de detectar; mejor relación imperceptibilidad/capacidad.

Cuadro 1: Comparación entre LSB1, LSB4 y LSBI

III. **Explicar detalladamente el procedimiento realizado para descubrir qué se había ocultado en cada archivo y de qué modo.**

A continuación se presenta un resumen del análisis realizado sobre cada archivo BMP entregado por la cátedra. Para cada uno se indica el método de esteganografiado detectado, el contenido recuperado y cualquier observación relevante.

– `Kings1.bmp`
En primer lugar, se obtuvo el archivo oculto en `Kings1.bmp` utilizando LSB4. De ahí se obtuvo la siguiente imagen:



– `madrid.bmp`
Luego, del archivo `madrid.bmp` se obtuvo un PDF con el siguiente texto: "al .png cambiarle la extensión por .zip y descomprimir" utilizando LSBI.
Se hizo lo indicado y se obtuvo un texto indicando el método de encripción de otro archivo oculto. Este era AES-ECB con clave de 128 bits.

– `Kings.bmp`
Se analizó este archivo usando un editor hexadecimal. Al final del archivo se encontró un mensaje en texto plano que indica que la password para desencriptar el video es "campeon".

– `silenceG2.bmp`
De este archivo se extrajo un secreto encriptado con el método y la password encontra-

dos anteriormente. A partir de eso se obtuvo el video secreto.

IV. **Algunos mensajes ocultos tenían, a su vez, otros mensajes ocultos. Indica cuál era ese mensaje y cómo se había ocultado.**

V. **Uno de los archivos ocultos era una porción de un video. ¿Qué se ocultaba y sobre qué portador?**

VI. **¿De qué se trató el método de esteganografiado que no era LSB1 ni LSB4 ni LSBI? ¿Es un método eficaz?**
En este caso, el mensaje se encontraba incrustado directamente dentro de la sección de datos del BMP, visible en texto plano al inspeccionar el archivo con un editor hexadecimal. Se trató de una técnica rudimentaria basada en sobrescribir bytes completos de los píxeles con los bytes del mensaje, sin manipulación de bits menos significativos ni codificación adicional. El método es poco eficaz porque genera modificaciones notorias y su detección es trivial.

VII. **¿Por qué la propuesta del documento de Majeed y Sulaiman es una mejora respecto de LSB común?**
La técnica reduce la cantidad de píxeles efectivamente modificados al decidir por patrones cuándo conviene invertir el LSB. Esto disminuye la distorsión visual y estadística, haciendo la imagen esteganografiada más difícil de detectar.

VIII. **¿De qué otra manera podría guardarse el registro de patrones invertidos?**
Podría almacenarse al final del mensaje oculto, en una región fija de la imagen destinada a metadata o derivarse de una clave mediante un generador pseudoaleatorio.

IX. **¿Qué dificultades encontraron en la implementación del algoritmo del paper?**
Como grupo tuvimos dificultades para implementar correctamente la lógica de patrones e inversión de bits del algoritmo del paper, especialmente para asegurar que la forma en que decidíamos qué bits invertir durante el ocultamiento coincidiera exactamente con la forma correcta de invertirlos durante la extracción.

X. **¿Qué mejoras o futuras extensiones harías al programa `stegobmp`?**
Una posible mejora sería extender `stegobmp` para que soporte más algoritmos de esteganografía y poder comparar su desempeño con LSB1, LSB4 y LSBI usando la misma herramienta.

Bibliografía

Referencias

[1] Mohammed Abdul Majeed y Rossilawati Sulaiman, "An Improved LSB Image Steganography Technique using bit-inverse in 24 bit colour image", *Journal of Theoretical and Applied Information Technology*, Vol. 80, No. 2, 2015.