Criptografía y Seguridad
Trabajo Práctico
2022

Integrantes

- Alejandro Marcelo Rolandelli 56644
- Luca La Mattina 57093

1. Discutir los siguientes aspectos relativos al documento. a. Organización formal del documento. b. La descripción del algoritmo. c. La notación utilizada, ¿es clara? ¿hay algún error o contradicción?

El documento está bien organizado pero le faltaria una seccion exclusiva donde se describa en detalle los pasos para realizar el algoritmo. La ausencia de la misma hace que la descripción del algoritmo no sea clara ya que solo usa un ejemplo muy simple para describir el proceso. Esto causa que uno tenga que inferir cómo funcionan partes del algoritmo, por ejemplo en qué lugar de la imagen y con qué formato se esconde la información sobre qué bits invertir. Además se utilizan notaciones que no se aclaran correctamente *“Keywords- bit inversion; least significant bit; steganography; quality; PSNR (key words)” .* Cuando menciona el segundo esquema se confunde al compararlo con el primer esquema y menciona el segundo denuevo *“The total pixel benefit in this [second] scheme is more than (or equal to) pixel benefit in second scheme”.*

2. 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.

Algoritmo	Ventajas	Desventajas
LSB1	Imágen con mensaje similar a la imagen portadora a simple vista	Requiere de una imagen portadora de tamaño más de 8 veces más grande que el mensaje
LSB4	Reduce mucho el tamaño de la imagen portadora necesaria	Modificó mucho la imagen portadora, a simple vista puede ser

	para esconder un mensaje en particular	posible diferenciar cual es la imagen que tiene un mensaje escondido de la original
LSBI	Mayor similitud de imagen con mensaje y la imagen portadora a simple vista que LSB1	Hay que ocupar 4 bytes más que en LSB1

3. 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.

Primero probamos de extraer un msj con todos los algoritmos, para cada archivo. Logramos extraer con LSB4 el mensaje en Paris, que era una imagen de un juego de buscaminas. Ademas al tratar de extraer el archivo sherlock.bmp se obtuvo un error advirtiendo que el tamaño especificado en el header no coincide con el tamaño real del archivo, debido a esto se abrió el archivo sherlock en un hex editor y se encontró la frase “la password es eleccion”. Y por último tras extraer el archivo montevideo.bmp con LSBI, obtuvimos un pdf que decía de modificar el png a zip y descomprimir, al hacerlo se obtuvo el archivo sol13.txt. Siguiendo las instrucciones en el archivo sol13 analizamos el tablero del buscaminas para encontrar el algoritmo y modo de encriptación (aes128 y ofb). Probando se logró extraer del archivo madrid.bmp con LSB1 -pass eleccion -a aes128 -m ofb y se obtuvo un archivo .wmv, una parte de la película Wanted (2008)

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

El archivo madrid.bmp tenía oculta una porción de la pelicula Wanted (2008), se la obtuvo haciendo un extract con LSB1 -pass eleccion -a aes128 -m ofb

5. Uno de los archivos ocultos era una porción de un video, donde se ve ejemplificado una manera de ocultar información ¿qué se ocultaba según el video y sobre qué portador?

El video muestra un método de esteganografia en el que un tejido de tela funciona como portador y se extrae el mensaje siguiendo el hilo vertical del tejido, cuando el mismo pasa por arriba de un hilo horizontal se anota un 1 caso contrario un 0.

6. ¿De qué se trató el método de estenografiado que no era LSB1 ni LSB4 ni LSBI? ¿Es un método eficaz? ¿Por qué?

El método consiste en embeber el mensaje al final del archivo portador. Este método no es eficaz ya que con cualquier herramienta de visualización de entropía muy probablemente se pueda detectar la existencia de un posible mensaje y resulta fácil de extraer.

7. ¿por qué la propuesta del documento de Akhtar, Khan y Johri es realmente una mejora respecto de LSB común?

Es una mejora ya que utilizando solo 4 bytes mas de espacio en la imagen portadora se puede potencialmente reducir mucho el ruido que se genera por embeber el mensaje en la misma. También se le dificulta a un posible atacante poder recuperar el mensaje de la imagen ya que es probable que algunos bits esten invertidos.

8. ¿de qué otra manera o en qué otro lugar podría guardarse el registro de los patrones invertidos?

Se podrían guardar al final del mensaje o en alguna posición de la imagen que no sea adyacente al mensaje y guardarse esa posición antes del mensaje para poder recuperarla

9. Leer el Segundo esquema y analizar (sin implementar) cuáles serían las ventajas que pueden verse.

La principal ventaja es que la imagen con el mensaje embebido seria todavia mas mas parecida a la imagen portadora ya que se sería más minucioso el criterio con el que un bit se invierte y le agrega un obstáculo más a un posible atacante ya que debería poseer la imagen portadora original para poder revelar el mensaje.

10. Leer el Segundo esquema e indicar qué desventajas o inconvenientes podría tener su implementación.

El receptor debería tener acceso a la imagen portadora original, lo que dificulta la logística de como enviarle toda la información necesaria al receptor para poder extraer el mensaje

11. ¿Qué dificultades encontraron en la implementación del algoritmo del paper?

Se nos dificulto debuggear el código una vez finalizada la implementación. Si bien los archivos de prueba que habilitó la cátedra sirvieron muchísimo para poder testear el código, la naturaleza de su propósito dificulta encontrar los errores. También fue difícil al principio entender bien el algoritmo de LSBI, son pasos con varias cosas a tener en cuenta para esconder tanto como para extraer la información.

12. ¿Qué mejoras o futuras extensiones harías al programa stegobmp?

Se podría agregar soporte para otras extensiones de archivo además de .bmp para usar como portadores. También se podrían agregar otros algoritmos de LSB como LSB2, LSB3, etc.