

Criptografía y Seguridad (72.44)

TRABAJO PRÁCTICO: ESTEGANOGRAFÍA

1. Objetivos

- Introducirlos en el campo de la esteganografía y sus aplicaciones.
- Experimentar con métodos de ocultamiento de información en archivos bmp, analizando ventajas y desventajas de cada uno.

2. Introducción

La **esteganografía** (del griego στεγανος *steganos*, *encubierto u oculto* y γραφος *graphos*, *escritura*) es la ciencia que se ocupa de la manera de **ocultar** un mensaje.

La existencia de un mensaje u objeto es ocultada dentro de otro, llamado **portador**. El objetivo es proteger información sensible, pero a diferencia de la criptografía que hace ininteligible dicha información, la esteganografía logra que la información pase completamente desapercibida al ocultar su existencia misma.

La criptografía y la esteganografía se complementan. Un mensaje cifrado mediante algoritmos criptográficos puede ser advertido por un intruso. Un mensaje cifrado que, además, ha sido ocultado mediante algún método de esteganografía, tiene un nivel de seguridad mucho mayor ya que los intrusos no pueden detectar su existencia. Y si por algún motivo un intruso detectara la existencia del mensaje, encontrarían la información cifrada.

La estenografía tiene un origen muy antiguo. Ya Heródoto en el año 440 aC narra la historia de un mensaje escrito en una tablilla que es cubierto con cera para pasar desapercibido ante el enemigo. El mensaje puede así llegar a su destino, siendo develado por sus receptores al quitar la cera.

En la era digital, el interés se renueva por sus múltiples aplicaciones, entre otras:

- Protección de derechos de autor (watermarking y fingerprinting)
- Técnicas de anonimato
- Voto electrónico

Los algoritmos de ocultamiento dependen del archivo portador, ya que la alteración del mismo de manera profunda puede despertar sospechas respecto de la existencia de un mensaje. En general se eligen como archivos portadores algún tipo de archivo multimedial: imagen, video o archivo de audio. Pero también existen otras posibilidades como archivos zip o archivos ejecutables.

El **estegoanálisis** se ocupa de estudiar métodos para detectar si un archivo ha sido ocultado en otro. Este campo de estudio está teniendo un desarrollo muy importante especialmente por agencias de investigación criminales debido a los alcances que la esteganografía con malos propósitos puede llegar a tener (por ejemplo, ataques terroristas, pedofilia, etc)

3. Consigna

- Realizar un programa **stegobmp** en lenguaje C o Java que efectúe las siguientes operaciones:
 - Oculte un archivo cualquiera en un archivo .bmp, mediante un método de esteganografiado elegido, con o sin password.
 - Descubra un archivo oculto en un archivo .bmp que haya sido previamente esteganografiado con uno de los métodos provistos.
- Estegoanalice un archivo .bmp para determinar si tiene un archivo incrustado, con qué algoritmo y lo extraiga correctamente.

4. Archivos .BMP

El formato BMP es un formato de archivos de imagen bastante simple. Consta de dos partes:

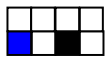
1. Encabezado → de 54 bytes
2. Cuerpo → de tamaño variable.

El encabezado contiene información acerca del archivo: tamaño de archivo, ancho de imagen, alto de imagen, bits por píxel, si está comprimido, etc

IMPORTANTE: Considerar la versión V3 de archivos BMP. Es la más común. No hace falta considerar otras versiones que puedan tener otro tamaño y datos de encabezados.

En el cuerpo del archivo bmp, están los bits que definen la imagen propiamente dicha. La imagen se lee de abajo hacia arriba y de izquierda a derecha. Si la imagen es de 24 bits por píxel, la distribución

es: 8 primeros bits para azul, 8 bits para verde, y 8 bits para rojo.



Ejemplo: La imagen de la izquierda representa un bmp de 4 pixeles por 2 pixeles.

El primer píxel leído es el azul, luego el blanco, luego el negro.

Si la imagen es de 24 bits por píxel, el píxel azul tiene la siguiente estructura:



En este trabajo práctico sólo interesa usar el cuerpo del archivo bmp como portador, para ocultar allí la información a esteganografiar. Por este motivo, sólo se utilizarán archivos .bmp que tengan las siguientes características:

- Imagen de 24 bits por píxel. Esto es, por cada píxel, se tienen 3 bytes donde ocultar información.
- Imagen bmp sin compresión. Para ello controlar el parámetro de compresión del encabezado.

5. Detalles del programa stegobmp

5.1. Ocultamiento de un archivo en un .bmp.

El programa debe recibir como parámetros:

➤ **-embed**

Indica que se va a ocultar información.

➤ **-in file**

Archivo que se va a ocultar.

➤ **-p bitmapfile**

Archivo bmp que será el portador.

➤ **-out bitmapfile**

Archivo bmp de salida, es decir, el archivo bitmapfile con la información de file incrustada.

➤ **-steg <LSB1 | LSB4 | LSBI>**

algoritmo de esteganografiado: LSB de 1bit, LSB de 4 bits, LSB Enhanced

Y los siguientes parámetros opcionales:

➤ **-a <aes128 | aes192 | aes256 | des>**

➤ **-m <ecb | cfb | ofb | cbc>**

➤ **-pass password** (password de encriptación)

Ejemplo 1:

Esteganografiar el archivo de texto "mensaje1.txt" en el archivo portador "imagen1.bmp" obteniendo un archivo "imagenmas1 .bmp" mediante el algoritmo LSB Improved, con encriptación DES en modo CBC con password "oculto"

```
$stegobmp -embed -in "mensaje1.txt" -p "imagen1.bmp" -out "imagenmas1.bmp" -steg LSBI -a des -m cbc -pass "oculto"
```

Ejemplo 2:

Esteganografiar el archivo de imagen "mensaje1.txt" en el archivo portador "imagen1 .bmp" obteniendo un archivo "imagenmas1.bmp" mediante el algoritmo LSB Improved, sin encriptación

```
$stegobmp -embed -in "mensaje1.txt" -p "imagen1.bmp" -out "imagenmas1.bmp" -steg LSBI
```

Importante:

No se puede encriptar/desencriptar sin **password**. Si este dato no está, sólo se esteganografía.

Son válidas en cambio las siguientes opciones:

- indicar **algoritmo** y **password** pero no modo: Se asume CBC por default.
- Indicar **modo** y **password** pero no algoritmo: Se asume aes128 por default.
- Indicar **sólo password**: Se asume algoritmo aes128 en modo CBC por default.

5.2.Extraer de un archivo .bmp un archivo oculto.

➤ **-extract**

Indica que se va a extraer información.

➤ **-p bitmapfile**

Archivo bmp portador

➤ **-out file**

Archivo de salida obtenido

➤ **-steg <LSB1 | LSB4 | LSBI>**

algoritmo de esteganografiado: LSB de 1bit, LSB de 4 bits, LSB Improved

Y los siguientes parámetros opcionales:

➤ **-a <aes128 | aes192 | aes256 | des>**

➤ **-m <ecb | cfb | ofb | cbc>**

➤ **-pass password (password de encripcion)**

Ejemplo:

Extraer el archivo de texto "mensaje1.txt" del archivo portador "imagenmas1.bmp" oculto mediante el algoritmo LSB Improved, con encripción DES en modo CBC con password "oculto"

```
$stegobmp -extract -p "imagenmas1.bmp" -out "mensaje1" -steg LSBI -a des -m cbc -pass "oculto"
```

5.3.Algoritmos de Esteganografiado.

Ocultamiento sin encripción:

Antes de ocultar el archivo propiamente dicho, con cualquiera de los algoritmos, ocultar su tamaño.

Después de ocultar el tamaño y el archivo propiamente dicho, con cualquiera de los algoritmos, ocultar su extensión (".png", ".jpg", ".txt", ".html", etc)

La extensión debe comenzar con '.' Y terminar con '\0'.

Es decir, se esteganografía:

Tamaño real || datos archivo || extensión

Y el total de datos a esteganografiar es:

4 (del tamaño) + longitud archivo + e (extensión)

Siempre se sabe que los primeros 4 bytes (DWORD size) corresponden al tamaño de archivo.

Siempre se sabe que después de los n bytes del archivo viene un punto y los n ascii de la extensión, terminando en '\0'.

Ocultamiento con encripción:

Si se eligió encriptar antes, se procede de la siguiente manera:

- Se obtiene la secuencia de bytes correspondiente a **Tamaño real || datos archivo || extensión**.
- Dicha secuencia se encripta con el algoritmo , modo y password.
- Se esteganografía el tamaño del cifrado y a continuación la secuencia cifrada.

Es decir, se esteganografía:

Tamaño cifrado || encripcion(tamaño real || datos archivo || extensión)

Y el total de datos a esteganografiar es:

4 (del tamaño del cifrado) + tamaño del cifrado

Para extraer, siempre se sabe que los primeros 4 bytes (DWORD size) corresponden al tamaño de cifrado. Con dicho tamaño, y algoritmo modo y password que se envían por argumento al programa se descifra. Una vez hecha la descifra se obtiene el tamaño real del archivo, se lee esa cantidad de bytes y se toma la extensión (hasta el '\0').

Ejemplo:

Si el tamaño real de "saco.txt" es 414 bytes, y se eligió encriptación en Des Cbc.

Entonces se encripta:

414 || datos archivo || ".txt\0"

Que da un total de $4 + 414 + 5 = 423$ bytes.

No es múltiplo de bloque así que requiere padding. Por lo tanto se encripta 423 + padding.

Luego, se esteganografía:

(423+padding) || encriptacion(414 || datos archivo || ".txt\0")

Es decir, se ocultan 4 (del tamaño del cifrado) + (423 + padding) bytes.

1. LSB1

Inserción en el bit menos significativo (Least Significant Bit Insertion - LSB)

Es el método más simple y consiste en insertar información sustituyendo el bit menos significativo de cada byte del archivo portador por un bit del mensaje.

En el caso de archivos de imagen ".bmp" consideraremos que cada bit del mensaje se inserta en el bit menos significativo de la **componente** (cada pixel tiene un componente rojo, un componente verde y un componente azul, cada uno de 8bits).

Como se observa, el primer bit del mensaje a ocultar se inserta en el bit menos significativo de la primer componente del primer pixel, el segundo bit del mensaje a ocultar se inserta en el bit menos significativo de la segunda componente del primer pixel, el siguiente, en la tercer componente del primer pixel. Entonces para guardar un byte, se requieren 2 pixeles completos y 2 componentes del siguiente pixel.

Importante: Si el archivo bmp no puede albergar el archivo a ocultar completo, deberá mostrarse un mensaje de error, en el que se indique cuál es la capacidad máxima del archivo bmp portador.

2. LSB4

Inserción en los cuatro bits menos significativos

Es una variante del anterior, donde 4 bits del mensaje se ocultan en los 4 bits menos significativos de la componente del pixel que corresponda.

Importante: Si el archivo bmp no puede albergar el archivo a ocultar completo, deberá mostrarse un mensaje de error, en el que se indique cuál es la capacidad máxima del archivo bmp portador.

3. LSB Improved

Es una variante de los anteriores propuesta por Juneja y Sandhu en el documento "An improved LSB based Steganography with enhanced Security and Embedding/Extraction".

Dicho documento se encuentra en:

<https://pdfs.semanticscholar.org/f797/fb90205d872df50e4660ce31a1467ca6a1bc.pdf>

En el documento, el mensaje a esteganografiar se cifra previamente con RC4. Este algoritmo debe usar una clave de 40 bits a 128 bits. En esta implementación, usaremos como clave los 6 primeros bytes (48 bits) de la imagen portadora. Es decir, los dos primeros pixeles (6 bytes) de la portadora serán la clave RC4.

Lo obtenido luego se oculta en la portadora en los bits menos significativos de los bytes que estén en la secuencia elegida. La secuencia depende de la elección de un "salto" (hop). Si bien podría ser elegido por argumento de programa, en esta implementación, usaremos el primer bit más significativo del primer byte de la portadora. Así si el primer byte de la portadora es 1000 0000, entonces el salto será 128. Si, en cambio, el primer byte de la portadora fuera 0111 0100, entonces el salto será 64. Si todos los bits del primer byte fueran 0, entonces el salto será 256.

Por lo tanto, en este método los pasos generales serían:

- Con los datos del archivo que se quiere ocultar, hacer:
msj = **Tamaño real || datos archivo || extensión**

o bien, si es cifrado:

msg = **Tamaño cifrado** || **encriptacion**(tamaño real || datos archivo || extensión)

- Aplicar RC4 a ese mensaje: $RC4_k(msg)$
- Ocultar $RC4_k(msg)$ en los LSB de los bytes elegidos por el “salto”.

Importante: Como los primeros 6 bytes de la portadora se utilizarán como clave para RC4, esos bytes no se usarán para LSB.

Importante: Si el archivo bmp no puede albergar el archivo a ocultar completo, deberá mostrarse un mensaje de error, en el que se indique cuál es la capacidad máxima del archivo bmp portador.

5.4. Otras consideraciones.

- **Respecto de cómo guardar el tamaño del bloque.**

Suponiendo que el tamaño del bloque a ocultar es 17,118.

Ese número ocupa 4 bytes.

Puede guardarse en Little Endian:

DE	42	00	00
----	----	----	----

O puede guardarse en Big Endian:

00	00	42	DE
----	----	----	----

Los archivos que les entregaremos tendrán el tamaño guardado en forma Big Endian.

- Si el archivo a ocultar requiriera padding usar el padding por defecto de openssl que es PKCS5.
- El archivo que se encripta es el que se quiere ocultar. Se encripta completo. Es decir, aún si fuera un bmp, se encripta desde el byte 0 hasta el último, cabecera incluida.
- Para la generación de clave a partir de una password, asumir que la función de hash usada es sha256, y que no se usa SALT.
- Los bmps utilizados deben ser de **24 bits** (8bits para rojo, 8bits para verde y 8bits para azul).
- Los bmps utilizados **no deben** tener compresión.
- En algunos archivos bmp, se completa con "padding" para lograr el tamaño de múltiplo de 4 bytes en las filas de píxeles. Para el esteganografiado usen todo el bloque completo de los píxeles + bytes de padding.
- Para modos de feedback considerar una cantidad de 8 bits si es CFB y 128 si es OFB.

Equivalencias OpenSSL / JCE para modos de Feedback:

	OpenSSL	JCE
CFB	EVP_aes_128_cfb(),	"AES/CFB/NoPadding" (corresponde a 128 bits de feedback)
	EVP_aes_128_cfb1()	NO tiene
	EVP_aes_128_cfb8()	"AES/CFB8/NoPadding" (corresponde a 8 bits de feedback)
OFB	EVP_aes_128_ofb()	"AES/OFB/NoPadding" (corresponde a 128 bits de feedback)
	NO tiene para 1 bit	NO tiene para 1 bit
	NO tiene	"AES/OFB8/NoPadding" (corresponde a 8 bits de feedback)

6. Estegoanálisis

La cátedra proveerá de 4 archivos con información oculta. De ellos, uno de los archivos contendrá un archivo ocultado mediante LSB1, otro mediante LSB4 y otro mediante LSBI. Un cuarto archivo ocultará información de otra forma que habrá que descubrir.

En los que están esteganografiados con los métodos LSB1, LSB4, LSBI, se sigue el formato especificado previamente:

tamaño + archivo + extensión

Habrá que obtener los archivos ocultos (estegoanálisis) descubriendo de qué manera fueron ocultos.

En general, el análisis que se puede hacer es:

- por conocimiento de archivo portador
- por repetición de archivo portador
- estadístico
- de tamaño de los archivos
- etc.

IMPORTANTE:

Se recomienda, para este análisis, usar algún editor de archivos binarios (hex editor neo o similar) que permita hacer comparaciones de los archivos.

7. Cuestiones a analizar

Serán publicadas en la semana del 20/4.

8. Organización de los grupos

El trabajo será realizado en grupos de máximo 3 integrantes.

9. Entrega

La fecha de entrega es el día **25 de junio**

Cada grupo entregará el ejecutable y el código en C o Java, junto con los archivos para obtener el ejecutable y la documentación correspondiente al uso del programa a mroig@itba.edu.ar y a rramele@itba.edu.ar

Además presentarán un informe **impreso** con la solución correspondiente al estegoanálisis de los archivos que se le entregarán oportunamente al grupo y con el análisis de las cuestiones planteadas en el punto 7.

10. Material de consulta recomendado

Hay mucho material en internet sobre el tema.

Es obligatorio leer:

Sobre el método que para este TP denominamos LSBI:

El documento “An improved LSB based Steganography with enhanced Security and Embedding/Extraction” de autores Mamta Juneja y Parvinder S. Sandhu disponible en:

<https://pdfs.semanticscholar.org/f797/fb90205d872df50e4660ce31a1467ca6a1bc.pdf>

Sobre algoritmo RC4:

El apunte “El cifrado RC4” de Alicia Boya García, disponible en : http://rufian.eu/Cifrado_RC4/

Sobre archivos bmp:

[http://msdn.microsoft.com/en-us/library/windows/desktop/dd183374\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/dd183374(v=vs.85).aspx)

Otros documentos que son útiles para la comprensión del tema o para contestar las preguntas:

- Cummings, Jonathan y otros: **Steganography and Digital Watermarking**. Disponible en: <http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.pdf>
- Gómez Cárdenas, Roberto: **Esteganografía**. Disponible en: <http://www.cryptomex.org/SlidesCripto/Estegano.pdf>
- Johnson, Neil F. y Jajodia, Sushil : **Exploring Steganography. Seeing the Unseen**. Disponible en: <http://www.creangel.com/papers/steganografia.pdf>