Criptografía y Seguridad

Trabajo práctico de Implementación

Grupo: **Supergrupo**

Integrantes:

- Lata, Andrea
- Sal-Lari, Julieta
- Pierri, Alan
- Rey, Juan Pablo

Cuestiones a analizar

1. *Para la implementación del programa stegowav se pide que la ocultación comience en la primer muestra del archivo de audio. ¿Sería mejor empezar en otra ubicación? ¿Por qué?*

Empezar a ocultar en un lugar diferente al inicio del archivo sería mejor en cuanto al aspecto de "hiding", ya que sería más dificil poder determinar si un archivo tiene o no otro archivo embebido. Esto sería así siempre y cuando la posición donde se inicie el ocultamiento sea aleatoria, y a definir entre quien oculte y quienes deseen leer. En caso de ser un valor fijo conocido, sería equivalente a ocultar desde el inicio.

En cuanto a la protección de datos, es preferible encriptar los datos ocultados a tener de clave la posición de comienzo, ya que esto los volvería muy susceptibles a estegoanálisis.

La desventaja es que se necesita que tanto el emisor como el receptor sepan la posición del comienzo de la ocultación como un dato extra, al igual que la encripción.

2. *Esteganografiar un mismo archivo en un .wav con cada uno de los tres algoritmos, y comparar los resultados obtenidos. Hacer un cuadro comparativo de los tres algoritmos estableciendo ventajas y desventajas.*

Modo de ocultamiento	**Dim. mínima vector / Dim. datos**	**Grado de corrupción del audio**	**Facilidad de detección**
LSBE	Depende de los valores del vector (sólo se utilizan los bytes con valor 254 o 255)	Variable (depende la posición del byte dentro del muestreo)	Muy difícil (sólo se ven afectados levemente bytes con valores específicos)
LSB1	Alto (**x** *bytes payload * tamaño muestreo * 8)*	Mínimo	Moderada (se ven alteraciones leves cada intervalos fijos de bytes)
LSB4	Bajo (**x** *bytes payload* * tamaño muestreo * 2)	Perceptible	Fácil (se ven alteraciones grandes cada intervalos fijos de bytes)

3. *Para la implementación del programa stegowav se pide que la extensión del archivo se oculte después del contenido completo del archivo. ¿por qué no conviene ponerla al comienzo, después del tamaño de archivo?*

Creemos que es lo mismo, ya que la extensión termina en un '\0', por lo que no afectaría en principio el cambio. La única ventaja aparente de la posición de la extensión al final del archivo es que en archivos muy grandes es mucho más dificil stegoanalizar bajo métodos variables (estilo LSBE) los diferentes patrones ya que tiene que leer toda la cantidad de bytes para llegar a la extensión y dar cuenta de ella.

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

Para cada tipo de hiding se analiza:

- Se lee el presunto tamaño, y se analiza si alcanza el tamaño de bytes del archivo para lo leído.
- Se lee dicha cantidad de bytes para ver si efectivamente existen (para métodos de hiding variables como LSBE)
- Se lee el primer byte de la extensión, esperando un '.' o un '\0'.
- Se lee los sucesivos bytes, esperando letras **solamente** (o '\0') ya que ningún otro caracter puede formar parte de una extensión, a diferencia del nombre de archivo.
- Se genera un archivo temporal y se analiza el **header** y el **magic number** del archivo.

5. ¿Qué se encontró en cada archivo?

Se posee de un método de "stegoanálisis" en el programa, que analiza automáticamente los archivos por posibles patrones de LSB1, LSB4 y LSBE.

Ironic10.wav

No se encontro nada. Creemos que el archivo está limpio.

Ironic10a.wav

En principio no, ya que estaba encriptado. Luego de desencriptarlo, encontramos un video bajo el método LSB4, encriptado bajo aes256 en modo cbc con password "compartido".

Show10a.wav

Sí, se encontro un archivo bajo el método LSB1.

```
### File extension matches LSB1 format ###
Its extension is '.png'
Size: 42536
File type detection:
PNG image data, 413 x 302, 8-bit/color RGBA, non-interlaced
```

Show10b.wav

Sí, se encontró un archivo bajo el método LSB Enhanced.

```
### File extension matches LSB Enhanced format ###
Its extension is '.pdf'
```

```
bytes_written: 19589
File type detection:
PDF document, version 1.5
```

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

El archivo oculto en **show10a.wav** tenía una imagen de un buscaminas casi resuelto. Cada fila indicaba los últimos 6 bits de una letra, siendo **1** las posiciones que tenían una mina, **0** caso contrario. Así se descubrió el mensaje “Aes**cbc**” que indicaría que el contenido de **ironic10a.wav** estaba encriptado bajo algún método **aes** y en modo **cbc**.

7. Uno de los archivos ocultos era una porción de un video, donde se ve ejemplificado una manera de ocultar información ¿cuál fue el portador?

El portador sería la tela cuyo tejido posee un método de hiding.

8. ¿De qué se trató el método de estenografiado que no era LSB? ¿Es un método eficaz? ¿Por qué?

Es eficaz ya que es casi imperceptible, pero el problema es que la forma de codificar y decodificar datos es demasiado costosa.

9. ¿Qué mejoras o futuras extensiones harías al programa stegowav?

Sería muy bueno desarrollar un método en él que dado un vector y un archivo “payload” a ocultar, te determine LSB**n**, siendo **n** el número mínimo de bits por muestra a utilizar para que el payload quepa en el vector. De esta forma, se minimizaría el ruido que se genera al ocultar información.