CRIPTOGRAFÍA Y SEGURIDAD

TRABAJO PRÁCTICO DE IMPLEMENTACIÓN: ESTEGANOGRAFÍA

Diego Vazquez - 54377
Franco Prudhomme - 54263
Ignacio Gutiérrez - 54293
Pablo Pauli - 51185

Introducción

El objetivo del siguiente trabajo práctico fue el de introducirnos en el campo de la esteganografía y sus diversas aplicaciones., además de experimentar con métodos de ocultamiento en archivos *.wav*, analizando las distintas ventajas y desventajas de cada uno.

Estegoanálisis de los archivos

Cuestiones a analizar

A continuación se resolverán las nueve cuestiones a analizar del punto 7 del trabajo práctico.

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?

Creemos que lo mejor es empezar desde el comienzo, ya que de esta forma se puede llegar a almacenar más información en el archivo portador, pero, en caso de que se quiera obtener un mayor nivel de complejidad en cuanto a su decodificación, se podría comenzar en una posición aleatoria que solo aquel que en codifique la sepa.

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.

	LSB1	LBS4	LSBE
Capacidad máxima	838699 bytes	3354798 bytes	31471 bytes
Tiempo de estenografiado	393 ms	346 ms	324 ms
Ventajas	cantidad de ruido moderado	cantidad ligeramente superior de ruido con respecto a LSB1	cantidad de ruido despreciable

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?

Porque la longitud de la extensión del archivo a esconder es variable y de hacerlo así habría que almacenar al comienzo también la longitud de la extensión escondida. Otra alternativa sería almacenar la extensión al comienzo como string null terminated, de esta forma la única desventaja es que no se sabe con exactitud el punto en donde comienza el archivo hasta que se termina de leer la extensión.

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

Teniendo los cuatro archivos, lo que se hizo fue probar cada por separado con los tres métodos de LSB, obteniendo como resultado que los archivos *desdecuando7a.wav* y *desdecuando7b.wav* ocultaban información con los métodos LSB1 y LSBE respectivamente, dándonos cuenta de esto debido a que la extensión obtenida como salida de dichas funciones era válida, mientras que la de los otros archivos no lo era. Cabe aclarar que para el archivo *clock7a.wav* (probando LSB4), si bien la extensión no era válida, el tamaño del archivo ocultado era relativamente pequeño con respecto a los demás, dándonos el indicio de que dicho archivo tenía la información encriptada, llegando a la conclusión de que el que tenía información estenografiada con otro método que no era LSB tenía que ser el archivo *clock7.wav*.

Con estos dos archivos que obtuvimos (un *.png* con un buscaminas y un *.pdf* el cual indicaba modificar el *.png* y tratarlo como *.zip*), y luego de realizar todos los pasos indicados, se obtuvo que el algoritmo y modo de desencripción para el archivo restante eran *des* y *ofb* respectivamente.

Pasamos algún tiempo buscando formas de sacar la información del archivo *clock7.wav*, pensando que se había codificado con algún LSB distinto, o que la información estaría en los headers del wav, pero no logramos obtener información útil de dicho portador, hasta que terminamos pidiendo ayuda a la cátedra, la cual nos recomendó leer el archivo con algún editor de texto, y ahí fue donde encontramos que la información se encontraba en texto plano al final del mismo, siendo dicha información la contraseña a utilizar para descifrar el archivo encriptado.

De esta forma, obtuvimos toda la información necesaria para poder desencriptar el archivo oculto en *clock7a.wav*, siendo el mismo un archivo *.wmv*.

5. ¿Qué se encontró en cada archivo?

- ➔ ***clocks7.wav:*** al abrirlo con un editor de texto hexadecimal se encontró al final del mismo la frase *"la password es descubrilo"*.
- ➔ ***clocks7a.wav:*** con este archivo pudimos encontrar un archivo *.wmv*.

- ➔ ***desdecuando7a.wav:*** con este archivo pudimos encontrar un archivo *.png*.
- ➔ ***desdecuando7b.wav:*** con este archivo pudimos encontrar un archivo *.pdf*.

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

El archivo .png tenía, además de la imagen (que en sí tenía un mensaje asociado), tiene oculto un archivo de texto al cual se puede acceder si se considera al .png como un archivo .zip y se le descomprime.

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?

Nota:
Se asume que la pregunta refiere a cual ese archivo portador dentro del video.

Dado que el video menciona un email y luego habla sobre un archivo que pesa mas de lo que debería, es muy probable que el portador sea un archivo adjunto en el email.

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

El método constó en concatenar texto plano al final del archivo de audio. Creemos que no es un método eficaz debido a que en caso de ocultar mucha información quedaría en evidencia el tamaño del archivo, siendo el mismo más grande de lo que debería (en este caso un archivo de audio, que llegaría a tener un mayor tamaño de lo que corresponde con la duración del sonido). Esto es una posible explicación a lo que mostraba el video que desencriptamos.

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

- Permitir que el archivo se oculte a partir de un sample arbitrario
- Permitir esconder múltiples archivos