ESTUDIO Y APLICACIÓN DE LA ESTEGANOGRAFÍA CON ARCHIVOS .WAV [1]

Quintero R., Javier E[1]. y León T. Jauri[2]
Universidad Autónoma de Bucaramanga
[1]Jquintero382@unab.edu.co, [2]jleontellez@gmail.com

Resumen **En el presente artículo se da a conocer la importancia de la esteganografía y su impacto en la seguridad de la información, y su modo de operación en archivos .WAV. De igual manera se presenta, algunas de las posibles arquitecturas de un sistema que permita enviar un mensaje oculto dentro del dominio del tiempo, desarrollado en la plataforma MatLab por su versatilidad y comprensión al usuario.**

Abstract **This article discloses the importance of steganography and its impact on information security, and its mode of operation in WAV files. Similarly it shows some of the possible systems architecture of a system that can send a hidden message in the time domain, developed in the MatLab platform for its versatility and understanding of the user.**

Palabras Claves*—Esteganografía, Telemática, Información, Señal de Audio, Criptografía, Matlab.*

Keywords— Steganography, Telematics, hide information, Audio Signal, Cryptography, Matlab.

1.- INTRODUCCIÓN

A nivel mundial las empresas y organizaciones de distintos sectores gubernamentales, sociales, académicos y económicos han incrementado su interés y atención en la protección de lo que hoy en día es un activo de vital importancia la "INFORMACIÓN", todo esto consecuencia de que los avances tecnológicos han derivado en nuevas amenazas, y los problemas que afectan a la seguridad informática avanzan a la par que la tecnología.

Un entorno seguro implica realizar varios estudios y el establecimiento de un esquema que soporte a los servicios de seguridad que se quieren proteger. Así surge la esteganografía [1] [2], que es el arte de enviar información oculta a través de un medio, sin que ningún tercero dude de la existencia del mensaje. Dicho de otra forma, consiste en el desarrollo de técnicas que proporcionen la creación de medios de comunicación encubiertos que pasen totalmente desapercibidos.

La esteganografía es aplicable a diferentes tipos de archivos, especialmente en textos, en imágenes, en sonidos, entre otros.

Los archivos en sonido, que es de interés en esta propuesta, con características especiales, cuentan no sólo con un buen tamaño disponible para los mensajes que se quieran incluir sino además con la limitación que tiene el hombre de escuchar tan sólo algunas frecuencias de sonido. El formato más usado y recomendado para el almacenamiento de sonido en una computadora es WAVE comúnmente conocido como .WAV.

Se debe resaltar la rapidez de un software como Matlab [3], en la ejecución de cálculos complejos con resultados precisos, esto hace posible llevar a cabo la graficación de señales y la comparación de las mismas, facilitando al usuario la compresión de lo que ocurre en el proceso.

El método tratado es uno de los métodos más usados en esteganografía digital. Nuestro interés es mostrar de manera sencilla el funcionamiento de éste tipo de sistemas para poder introducir al lector en el área de la esteganografía.

2.- MARCO CONCEPTUAL Y SU APLICABILIDAD

El formato .WAV Posee dos partes: el encabezado y el sector de datos. El encabezado contiene la información de cómo se encuentra digitalizado el archivo de sonido. Cantidad de canales, frecuencia de muestreo y tamaño de muestra. En el sector de datos se encuentran en forma de bits secuenciales las muestras, es decir el sonido. Esto deja implícito, que es en el sector de datos dónde sucede todo el proceso de

ocultamiento del mensaje

A. Ocultación de señales de audio

La esteganografía puede basarse en dos métodos, el que usa el dominito del tiempo y el que usa el domino de la frecuencia [4], como en el caso de la transformada del coseno, los de este tipo ofrecen mayor robustez por eso tienen algoritmos más complejos. El método de ocultación tratado en este documento está basado en el dominio del tiempo.

B. Ocultación de audio en el dominio del tiempo

La ventaja de esta técnica esta principalmente en que en comparación con las demás, es relativamente sencilla y tiene menos costo de procesamiento a nivel computacional lo que la hace más eficiente. [5]

El sonido se muestrea y se escala en Matlab como enteros de 8 bits, la longitud total del archivo es almacenada en un vector, donde también se crea una cabecera inicial en la que se incorpora la longitud del archivo en 10 bits y aparte el nombre en 150 bits, ambas longitudes son de tamaño fijo y también manejan el formato entero de 8 bits; con la información anterior se recrea un nuevo vector con los valores tanto de la longitud original como del nombre y con la información del archivo de audio, en el que se distribuyen 4 bits para el canal izquierdo y 4 bits para el derecho de la portadora WAV estéreo.

La novedad de este método es que al implementar la cabecera para el nombre de archivo, los archivos recuperados conservarán su nombre original y se podrá conocer de manera eficaz el espacio disponible para la ocultación de archivos, pues el código fue diseñado con el fin de proporcionar esta información al usuario de manera aproximada para que pueda hacer un mejor uso del método.

La razón por la que se usan 4 bits LSB (bit menos significativo) es la de mantener la fidelidad del archivo y la menor distorsión posible.

La figura 1 ilustra el proceso ejecutado en el emisor, que es donde se oculta la información en la portadora WAV y se genera el estego-objeto.

En el primer bloque se lee el archivo el cual se va a utilizar para ocultar la información en un formato WAV, se recomienda que este archivo tenga como mínimo una frecuencia de muestreo de 44.1 KHz y una profundidad 16 bits para que el sistema opere sin errores.

En el segundo bloque se leen los archivos que se quieren ocultar en formato MP3, en el código diseñado se recomienda cargar los archivos de forma secuencial para evitar errores.

En el tercer bloque se convierten los MP3 a ocultar en vectores de enteros de 8 bits sin que se pierda la calidad del audio a insertar.

En el cuarto bloque se crea la cabecera de cada uno de los MP3 con la información del nombre y las longitudes de cada MP3 para que estas puedan ser recuperadas posteriormente sin necesidad de una instrucción externa.

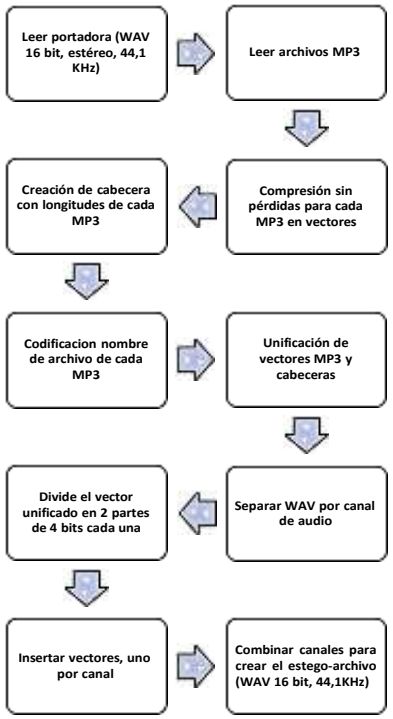

Figura 1. Diagrama de bloques emisor

En el quinto bloque se codifica la información del nombre de cada MP3 en enteros de 8 bits para que puedan ser trabajadas junto con la información del MP3.

En el sexto bloque se concatenan la información del nombre y longitud del MP3 seguido de su información de audio para cada uno de los archivos MP3 seleccionados.

En el séptimo bloque se separan los canales de audio a procesar posteriormente. En la octava etapa se toma el vector unificado que contiene la información en 8 bits de nombres, cabeceras y datos para dividirlo en dos vectores de 4 bits cada uno.

En la novena etapa se inserta un vector de 4 bits en el canal izquierdo y el otro en el derecho.

En la etapa final se unifica el archivo de audio WAV para crear el estego-archivo.

En el receptor ocurre un proceso similar pero de forma inversa en el cual se toma el estego-archivo, y a partir de ahí, se comienza a reconstruir el vector con información de los archivos incrustados por el emisor para luego extraer cada uno en una carpeta generada por el programa; este proceso puede verse en el diagrama de bloques de la figura 2.

En el bloque uno se muestrea el estego-archivo. En el bloque dos se separan el canal izquierdo del derecho para prepararlo para la extracción. En el bloque tres se extraen los vectores de 4 bits y se recrea el vector unificado con la información de nombres, cabeceras y datos.

En el bloque cuatro se recuperan el vector unificado original de 8 bits, uniendo las partes de 4 bits contenidas en cada canal.

En el bloque cinco se generan los vectores con la información de los nombres y cabeceras en formato de enteros de 8 bits.

En el bloque seis se obtienen los nombres y las cabeceras de convertir la información en forma de enteros de 8 bits contenida en el vector unificado recuperado a Unicode.

En el bloque siete se recuperan los fragmentos delimitados por las cabeceras desde el vector unificado creando una variable con la información de cada MP3.

En la etapa final se exporta la información de cada MP3 y se asigna su nombre correspondiente, es por esta razón se reescribirán los archivos homónimos por el que se haya procesado más recientemente.

En comparación con otros métodos más robustos, el presente es bastante frágil. Lo que quiere decir que el estego-archivo generado es susceptible a cualquier tipo de modificación, y ninguno de sus parámetros puede ser modificado o estar envuelto en un proceso que implique degradación de datos.

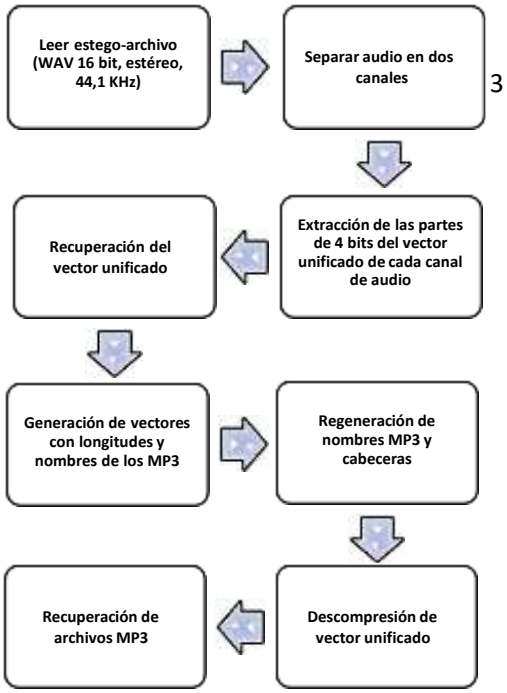

Figura 2. Diagrama de bloques receptor

3.-RESULTADOS

Como se mencionó al comienzo de este artículo, la gráfica de la señal resultante depende de las propiedades de la señal estéreo WAV utilizada en la etapa inicial del proceso.

A. Comparación de WAV original y el generado.

Con la finalidad de hacer visible el objetivo del método propuesto a través del espectro, se ha utilizado una onda mp3 convertida a WAV por medio de un proceso de escalado en un editor de audio; el algoritmo mp3 principalmente elimina las frecuencias del espectro por encima del espectro audible, estas son las que están sobre los 20 KHz, por esta razón al convertirla a WAV las frecuencias mayores son solo un espacio vacío.

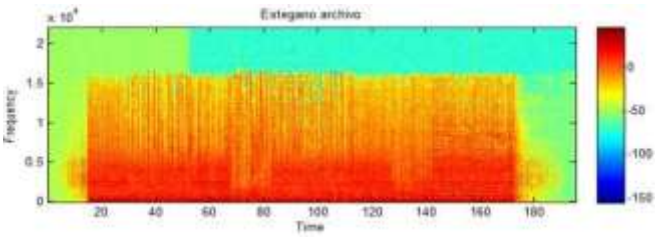

Figura 3. Espectrograma del estego-archivo de un mp3 escalado (Autor)

Comparando la gráfica con el espectro del archivo original, se puede ver que hay una coloración en el espectro del estego-archivo, la coloración se da porque hay información oculta incrustada en portadora, el resto que se ve en celeste es el espacio disponible que puede utilizarse para ocultar más información.

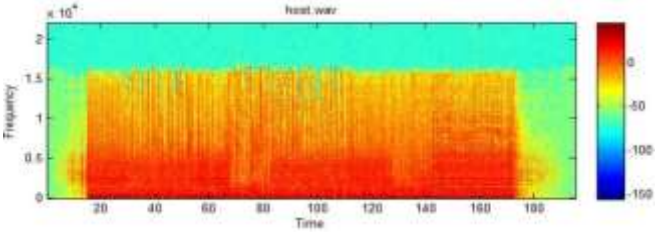

Figura 4. Espectrograma del archivo mp3 escalado original (Autor)

En la comparación anterior se ha usado un archivo MP3 escalado como archivo WAV con la finalidad de que se pueda apreciar el proceso, es por eso que se visualiza un espacio vacío después de los 16 KHz y se observa cómo se va llenando el esteganoarchivo con la información secreta.

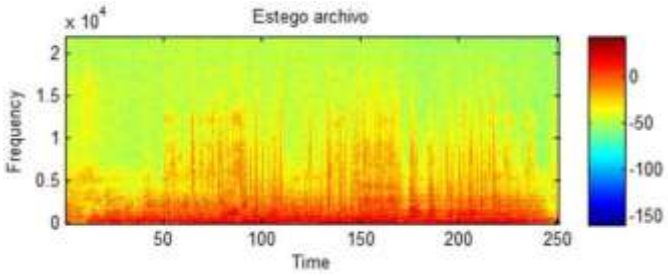

Figura 5. Espectrograma del estego-archivo (Autor)

En la figura 5 se ilustra la gráfica generada por Matlab para el análisis del espectro del estegoarchivo generado a partir de un WAV de onda completa que contiene información oculta y se compara con el de la figura 6, que ilustra la gráfica del WAV original no procesado.

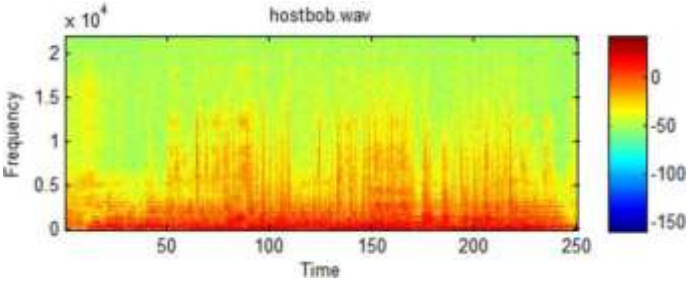

Figura 6. Espectrograma del archivo WAV original (Autor)

A simple vista parecen el mismo, cumpliendo con el objeto planteado en este proyecto el cual es ocultar la información importante a terceros.

4.- OBSERVACIONES Y CONCLUSIONES

Tras las pruebas realizadas se observa que el algoritmo utilizado es vulnerable a cambios en las propiedades principales del archivo, como la amplitud, frecuencia o fase, haciendo el que archivo final sea un archivo del que no se podrá recuperar la información.

Una de las ventajas del método aplicado, es que no solo permite el envío de archivos de audio, sino que también permite por enmascarar otro tipo de archivos con la extensión de un archivo de audio, esto permite que el programa sea versátil e igual de efectivo al ocultar un archivo.

El número de archivos a ocultar y el tamaño de cada uno de ellos depende directamente del tamaño de la portadora a utilizar, en este estudio se definieron 5 archivos mp3 como estego-archivos pero el código puede ser modificado para admitir una mayor cantidad, siempre y cuando se distribuya y no se exceda el espacio de almacenamiento disponible en la portadora.

Aunque la encriptación no fue el tema abordado en este proyecto, es posible agregar en el código del programa algún tipo de encriptación o clave de seguridad al archivo para hacerlo aún más robusto antes de recuperar la información en el receptor.

REFERENCIAS

[1] E. B. C. GAMEZ, *TECNICA DE INSERSION DE INFORMACION EN VIDEO APROVECHANDO EL MISMO ANCHO DE BANDA,* México, D.F.: Instituto Politecnico Nacional, 2008, p. 150.

[2] I. S. A. ORBEGOZO, *TECNICAS DE AUTO ESCALADO DE CLOUD COMPUTING APLICADAS AL ESTEGANOANALISIS.,* Madrid: UCM, 2011.

[3] S. J. Chapman, MATLAB Programming for Engineers, Boston, MA: Cengage Learning, 2015.

[4] INTECO, «nstituto Nacional de Ciberseguridad de España, S.A. (INCIBE),» 17 Febrero 2010. [En línea]. Available: https://www.incibe.es/file/cMACs_tFRyI_Q1i88xyWtA. [Último acceso: 15 04 2015].

[5] G. M. Galcerán, *SISTEMA DE WATERMARKING BASADO EN ALTERACIONES DE COLOR,* Barcelona: UPC, 2013.