textOsFtextTOsFliningLFliningTLFtextosflininglftabulartabproportionalpropsuperiorSup superiorSup

fontspechyperref

TITLE

Author1

University

IMPLEMENTACIÓN DEL ALGORITMO ESTEGANOGRÁFICO LSB (LEAST SIGNIFICANT BIT) ESTÁNDAR EN ARCHIVOS DE AUDIO MP3

Gabriel Segura Bernal 1, Alan Díaz Andrade 2
IPN, CIDETEC,Depto. de Posgrado 1,2

Resumen

Esteganografía: disciplina que estudia las técnicas y algoritmos de ocultamiento de información, teniendo como principal objetivo transferir un mensaje oculto a través de medios no usuales llamados portadores. Se apoya en dos principios básicos:

1. Selección del medio: refiriéndose a que el archivo a ocultar a pesar de que pierde calidad no sea perceptible.
2. Toma en cuenta las limitaciones del hombre si de percepción se habla, la gama de colores que aunque varíen un poco el ojo humano no alcanza a decodificar

En este trabajo, se presenta una aproximación del algoritmo de Bit menos significativo (LSB) en archivos de audio utilizando lenguaje C para su implementación.

Palabras Clave: Esteganografía en audio, codificación LSB, ocultamiento de información codificación LSB, ocultamiento de información

1. Introducción

La criptografía y la esteganografía son dos campos que se complementan basados en la seguridad informática: el primero oculta el significado del mensaje y el segundo oculta la existencia del propio mensaje. Cada una por separado no asegura el secreto, pero si se aplican ambas técnicas para cifrar y ocultar un mensaje, aumentando el nivel de seguridad y con ello las posibilidades de éxito.

Esteganografía: disciplina que estudia el conjunto de técnicas que tiene como objetivo común la ocultación de información sensible, mensajes u objetos, dentro de otros llamados ficheros contenedores, comúnmente multimedia: imágenes digitales, videos o archivos de audio, con el objetivo de que la información pueda pasar inadvertida a terceros y solo pueda ser recuperada por un usuario legitimo [4].

Aunque existen múltiples formas de ocultar una información, comúnmente se basan en dos principios:

1. Aprovechar estegomedios con información redundante, no útil, que puede ser modificada sin levantar sospechas, por ejemplo mediante la técnica LSB, explicara más adelante.
2. Aprovechar el reordenamiento de los elementos que definen un estegomedio, por ejemplo, reordenar los píxeles de la paleta de colores en un fichero GIF.

Figura 1. Monalisa una de las imágenes más usada para ejemplificar la esteganografía en imágenes

Clasificada en dos tipos:

- Protección contra borrado
- Protección contra detección

Emplea como base de estudio el algoritmo de LSB; que a continuación se explica cómo interviene en la fase de la esteganografía

1. Esteganografía de protección contra detección.: Se basa en esconder datos binarios en la maraña de bits que supone un archivo. Los bits que componen el mensaje a ocultar se introducen (bien sea añadiéndolos, o realizando operaciones aritméticas con los originales) en el fichero ya existente, procurando que el archivo resultante después de realizar los cambios parezca el original, es decir; sin cambio alguno. Por ejemplo se puede encontrar este tipo de esteganografía en imagen, sonido, y ejecutables.

2. Esteganografía de protección contra borrado: dentro de esta división se encuentran dos ramas:

- Marcas de agua. Se oculta información relacionada con un objeto dentro del mismo de tal forma que pueda ser extraída y validada posteriormente por una computadora.
- Adiciona datos de derechos de autor a contenido, y huella dactilar esta además de contener datos del propietario del copyright del objeto, contiene datos del comprador original o del que adquiere los derechos de uso [4]

2. Trabajo relacionado

En la actualidad existen diversos métodos y algoritmos utilizados para ocultar la información dentro de archivos multimedia: [5]

1. Enmascaramiento y Filtrado: la información se oculta dentro de una imagen digital empleando marcas de agua que incluyen información, como el derecho de autor.
2. Algoritmos y transformaciones: método que oculta el mensaje en los bits de datos menos importantes.
3. Inserción en el bit menos significativo (LSB Inserción): consiste en hacer uso del bit menos significativo de los pixeles de una imagen y alterarlo. Los mejores resultados se obtienen en imágenes con formato de color RGB (tres bytes, componentes de color, por píxel). La misma técnica puede aplicarse a vídeo y audio.
4. Técnica cetel: El uso de esteganografía en los documentos puede funcionar sólo con añadir un espacio en blanco y las fichas a los extremos de las líneas de un documento.
5. Técnica en archivos de audio: la técnica más utilizada en el ocultamiento de archivos de audio es el low bit encoding (baja bit de codificación), [5] similar a la LSB que suele emplearse en las imágenes [5]. El problema que se presenta con el low bit encoding es que es apreciable para el oído humano, así que es un método arriesgado para que alguien lo use; si están tratando de ocultar información dentro de un archivo de audio.
6. Spread Spectrum: Funciona mediante la adición de ruidos al azar a la señal de que la información se oculta dentro de una compañía aérea y la propagación en todo el espectro de frecuencias. [5].

7. Hecho data hiding: usa los ecos en archivos de sonido con el objetivo de ocultar información. Consigue mejorar realmente el sonido del audio dentro de un archivo de audio.
8. Técnica en videos: Es común utilizar el método DCT (Discrete Cosine Transform).

DCT: funciona cambiando ligeramente cada una de las imágenes en el vídeo, la información es ocultada en cada fotograma de vídeo, de manera que no sea perceptible por el ojo humano

3. Nuestra contribución

El oído humano es extremadamente sensible a cambio en los patrones de audio, pero no tanto como para percibir cambios dentro de una misma frecuencia. A la hora de ocultar un mensaje en audio, es importante saber el medio por el que se va a transmitir el mensaje, no es lo mismo entre medios digital-digital (entre ordenadores) o entre aire-digital (micrófono). Por eso se desarrolla un algoritmo de LBS.

3.1 Metodología

Función de la esteganografía:

[]@l@

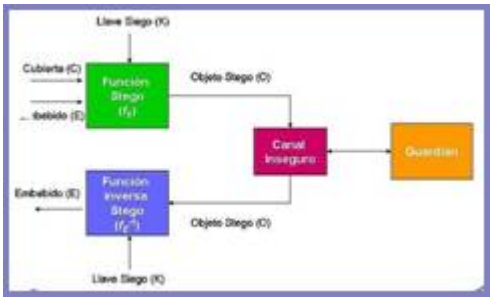


Figura2. Esquema general de Esteganografia

Este es uno de los algoritmos más utilizados en esteganografía ya que es muy fácil de aplicarse a una imagen y audio. Una gran cantidad de información puedes ser escondida con poco de tiempo o en una imagen muy pequeña.

El proceso de LBS consiste en elegir un subconjunto {j1,.., jm} de elementos de la tapa y realización de la operación de substitución Cji<->mi dentro de la información ya que cambia el LBS de Cji por algún bit 0 o 1, podría también imaginar una operación de substitución que cambia más de un trozo de la tapa, por ejemplo almacenando dos trozos de mensaje en los dos trozos menos significativos de un elemento de la tapa. En el proceso de extracción, el LSB de los elementos de la tapa seleccionados son extraídos y rayados hasta reconstruyen el mensaje secreto [1].

A continuación se muestra los algoritmos Proceso de fijación y de proceso de extracción.

Algoritmo 1: Proceso de fijación: la substitución de trozo menos significativa
Para i = 1,...,lc hasta
si ← ci

Fin para

Para i = 1 ...,lm hasta

Cálculo del índice ji donde almacenar i el mensaje del bit
sji ← cji mi

Fin para

Algoritmo 2: Proceso de extracción: la substitución de trozo menos significativa
Para i = 1,...,lM hasta

Calculo de índice ji cuando el i del mensaje almacena el bit más significativo
mi ←LSBCij

Fin para

Algoritmo 3: Proceso de fijación: método de intervalo arbitrario
Para i = 1...,lc hasta
si ← ci

Fin para

Generar secuencia aleatoria ki utilización de la semilla k
n ← k1
Para i = 1,...,lm hasta
sn ← cn mi
n ← n + ki

Fin para

Algoritmo 4: Proceso de extracción: método de intervalo arbitrario

Generar secuencia aleatoria ki utilización de la semilla k

n ← k1
para i = 1,...,lm
mi ← LSBcn
n ← n + ki

Fin para

4. Desarrollo

El proceso de LBS consiste en elegir un subconjunto {j1,.., jm} de elementos de la tapa y realización de la operación de substitución Cji<->mi dentro de la información, cambia el LBS de Cji por algún bit 0 o 1, se podría también imaginar una operación de substitución que cambia más de un trozo de la tapa, por ejemplo almacenando dos trozos de mensaje en los dos trozos menos significativos de un elemento de la tapa.

En el proceso de extracción, el LSB de los elementos de la tapa seleccionados son extraídos y rayados hasta reconstruyen el mensaje secreto [1].

5. Resultados experimentales

Producto del desarrollo que se describe en la parte superior.

El programa se encarga de comprimir las bandas sonoras del formato MPEG III, ofrece una calidad de compresión de 11 a 1 (128 kilobits por segundo), esto da una oportunidad muy buena del ocultamiento de información. Aunque WMA tenga la mejor calidad en general, yo no tenía el acceso al código y sólo una realización para MP3.

La aplicación esconderá la información en archivos MP3 durante el proceso de compresión. Los datos son comprimidos primero, codificados y luego escondidos en el flujo de bit MP3. Aunque MP3Stego haya sido escrito con aplicaciones esteganografía en mente él podría ser usado como un sistema de marca de agua para los archivos MP3.

El proceso de ocultamiento ocurre en el corazón de la Capa III proceso de codificación a saber en el ciclo de codificación. El proceso interior cuantifica los datos de entrada y aumenta el tamaño hasta que los datos cuantificados puedan ser cifrados con el número disponible de fila gramas. A continuación se muestra una interfaz de cómo debe de hacerse la esteganografía.

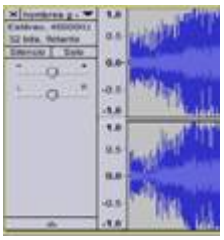
[]@l@

Figura 3. Salida de filagramas cifrados

Para presentar estos resultados se empleó software llamado audacity el cual sirve para analizar los archivos de audio.

Lo primero que se realizo fue cargar en el programa los dos archivos de audio el original y el archivo con esteganografía y a simple vista no se ve diferencia alguna al momento de reproducir no se altera nada el sonido y el tiempo de reproducción es el mismo. La tabla 1 muestra la comparación de las ondas de ambos archivos, en la parte derecha está el archivo original y en la izquierda el archivo compuesto así se nombrara por comodidad durante la explicación al archivo que se le aplico la esteganografía.

[]@ll@



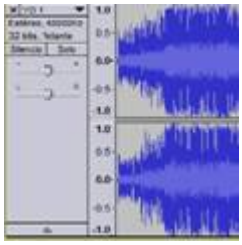


Figura 4. Audio original **Figura 5.** Audio con LBS

5.1 Análisis de decibeles

Como se puede apreciar en las imágenes anteriores no se muestra los cambios significativos y en base a esto se realiza una comparación en decibeles y frecuencias que se manejan, en la tabla se muestran los resultados

[]@l@

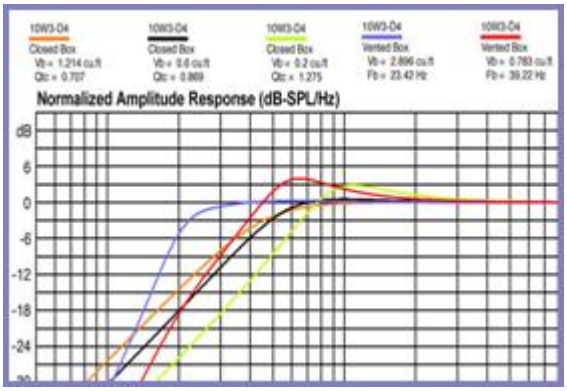


Figura 6. Análisis de decibeles

6. Concluciones

Dadas las características especiales de este trabajo, se han estudiado las propiedades fundaméntales del Sistema Auditivo Humano, para encontrar “huecos” para desarrollar un estego-sistema sobre el códec de audio MP3. El estudio realizado permite obtener una visión amplia y con un nivel de profundidad medio del panorama actual, y compone una base sólida a partir de la cual se puede seguir profundizando en métodos más especializados. Este estudio, además, ha permitido establecer guías a partir de las cuales crear y diseñar un nuevo estego-sistema.

El estudio de las técnicas estegoanalíticas básicas, permite conocer, mejor las debilidades de los propios algoritmos esteganográficos, conocimiento fundamental para desarrollar algoritmos efectivos y con la cualidad deseada.

Del estego-sistema creado e implementado, en ningún se pretendió crear un sistema “irrompible”, sino más bien un punto de partida para crear un sistema competente. Así, aunque el hecho de que, como se comenta a continuación, se pueda considerar estegoanalizado estadísticamente, algo que no es sencillo de obtener incluso para estego-sistemas básicos, esto no debe considerarse únicamente como un defecto, si no como el reconocimiento de la debilidad del algoritmo en dichos aspectos y el camino que marca los próximos pasos a seguir para alcanzar un sistema seguro.

Bibliografía

[1] Mazen Abu Zaher, “Modified Least Significant Bit (MLSB)”, Computer and Information Science pp 60 -70 2011

[2] ARTZ, Donovan. Digital Steganography: Hiding Data within Data. p. 77 ss. Junio 2001. Los Alamos National Laboratory. Spotlight. pp 13

[3]SIMMONS, G. J. “The prisioners’ Problem and the subliminal channel”, in Advanced in Criptology, Proceedings of CRYPTO 83, Plenum Press, 1984. pp 8

[4] Roberto Gómez Cárdenas, “La esteganografía”. Artículo publicado en la revista Bsecure de marzo del 2004.

[5] Greg Kipper, “Investigator’s Guide to Steganography”, Intellectual Property Protection Systems, Auerbach Publications 2004. pp 58.

Referencias

[1] http://www.robotis.com/xe/darwin˙en

[2] Brushless DC (BLDC) Motor Fundamentals, Padmaraja Yedamale Microchip Technology Inc.

[3] Técnicas de control para motores Brushless Comparativa entre conmutación Trapezoidal, conmutación Sinusoidal y Control Vectorial, Roger Juanpere Tolrà.

Referencias

[1] Albert Einstein, Isaac Newton, Marie Curie, Galileo Galilei, Charles Darwin ***(mayo - junio, 2025)*** *La teoría de la evolución biológica. Boletín UPIITA. año 19, (108) 2025* liga del artículo