Revista de Gestión Empresarial y Sustentabilidad

http://rges.umich.mx

El Arte de Esconder Información: Aplicación Práctica del Método LSB Secuencial

Pedro Chavéz Lugo[1]
Rigoberto López Escalera[2]

[1]Universidad Michoacana de San Nicolás de Hidalgo, pedro.chavez@umich.mx
[2]Universidad Michoacana de San Nicolás de Hidalgo, rigoberto.lopez@umich.mx

Revista de Gestión Empresarial y Sustentabilidad, Vol. 10, Núm. 1, Enero – Diciembre 2024, ISSN: 2448-6043, pp. 37 – 50, Fecha de Recepción 25 de Noviembre de 2024, Fecha de Aceptación 23 de Diciembre de 2024

El Arte de Esconder Información: Aplicación Práctica del Método LSB Secuencial

Resumen

Este trabajo presenta una implementación aplicada de esteganografía digital basada en la técnica del bit menos significativo (LSB), utilizando como estegomedios imágenes en formato BMP y archivos de audio en formato WAV. Los formatos BMP y WAV son utilizados debido a que no emplean compresión con pérdida, lo que garantiza que la información oculta no sea alterada o destruida durante el almacenamiento. En el caso de las imágenes BMP, se modifican los bits menos significativos de los valores RGB de cada píxel. En los archivos WAV, se alteran los bits menos significativos de las muestras PCM del audio. En síntesis, el trabajo demuestra cómo la técnica LSB aplicada a archivos BMP y WAV constituye una solución práctica y didáctica para ocultar información digital sin afectar perceptiblemente la calidad del medio portador.

Palabras clave: Esteganografía digital, método LSB secuencial, ocultamiento de información, seguridad de la información, bit menos significativo MSB.

Abstract

This work presents an applied implementation of digital steganography based on the Least Significant Bit (LSB) technique, using BMP image files and WAV audio files as steganographic media. The BMP and WAV formats are used because they do not employ lossy compression, which ensures that the hidden information is not altered or destroyed during storage. In the case of BMP images, the least significant bits of the RGB values of each pixel are modified. In WAV files, the least significant bits of the audio's PCM samples are altered. In summary, this work demonstrates how the LSB technique applied to BMP and WAV files constitutes a practical and instructional solution for hiding digital information without perceptibly affecting the quality of the carrier medium.

Keywords: Digital steganography, sequential LSB method, information hiding, information security, least significant bit MSB.

Introducción

Los avances tecnológicos han generado cambios en la gestión de la seguridad con el fin de preservar la confidencialidad e integridad de la información. Con el uso de Internet como medio de comunicación, la información viaja por diferentes redes que pueden implicar su captura. Existen diferentes alternativas para proteger cualquier tipo de información, independiente de su naturaleza o fines. Una de estas alternativas es la criptografía (Stinson, D. R. (2005)) (Paar, C., & Pelzl, J. (2010)), la cual se basa en la transformación de la información original, de esta manera en primera instancia no se puede conocer el contenido de la información, lo cual implica para conocerla la aplicación del criptoanálisis (Swenson, C. (2008)). Existe otra alternativa que tiene como objetivo ocultar la existencia de la información, tal es el caso de la esteganografía. La cual trata sobre el estudio de las técnicas que permiten ocultar información, basándose en la selección de un portador que contendrá la información en un archivo multimedia (imagen, audio, video). La información cifrada refleja que él emisor y el receptor intentan obtener confidencialidad en la comunicación. La criptografía puede ser combinada con la esteganografía ocultando la información cifrada en algún objeto que revele su presencia. La criptografía y la esteganografía son herramientas de seguridad defensiva que pueden ser combinadas para obtener confidencialidad. Otra opción más corresponde a la criptografía visual que combina imágenes para la transformación de la información (Naor, M., & Shamir, A. (1994, May)) (Stinson, D. R. (1997)).

Concepto de Esteganografía

La esteganografía se relaciona con el campo de la criptología pero no se encuentran relacionadas directamente. La esteganografía consiste en ocultar la existencia de la información (Swenson, C. (2008)), actualmente se utilizan objetos multimedia como contenedores. Los primeros antecedentes que describen el uso de técnicas esteganográficas fueron en la antigua Grecia en el siglo quinto A.C. En algunos casos rapaban al mensajero para tatuarle el mensaje y una vez que su pelo crecía transportaba el mensaje. En el ámbito

actual se utilizan como portadores objetos multimedia (imagen, audio, video) para incrustar la información, cuidando que dicha incrustación no sea perceptible para los sistemas visual y auditivo de las personas que accedan al objeto portador.

Estegomedio

Un estegomedio es un archivo con formato multimedia audio, imagen o video. El cual es utilizado para insertar o incrustar información. Dicha inserción debe no ser perceptible para las capacidades auditivas y visuales de las personas. Para la elaboración de este trabajo se utilizaron imágenes en formato BMP y audios en formato WAV.

Formato BMP

El formato BMP (Bitmap - mapa de bits) (Microsoft Docs.) (DGonzalez, R. C., & Woods, R. E. (2018)) se seleccionó como estegomedio porque no utiliza compresión con pérdida, los bits menos significativos pueden modificarse sin que la imagen sufra distorsión adicional y cada píxel se almacena explícitamente. Al no comprimirse tienen mayor capacidad de almacenamiento.

Formato WAV

El formato WAV (Waveform Audio File Format - archivo de audio de forma de onda) (Microsoft & IBM. (1991)) (Pohlmann, K. C. (2010)) se seleccionó como estegomedio porque no utiliza compresión con pérdida, los bits menos significativos pueden modificarse sin distorsionar la calidad sonora.

Método LSB (Least Significant Bit) Secuencial

El método LSB consiste en la modificación del bit menos significativo (Least Significant Bit) para incrustar la información (Muñoz, A. M. (2016)). La Figura 1, muestra 8 bytes del objeto contenedor y 1 byte de la información que se pretende incrustar. El bit más significativo (MSB) del byte a incrustar se incrusta en el bit menos significativo del primer byte del objeto contenedor. Este proceso se continua realizando con el resto de los bits del

dato a insertar, finalizando con la incrustación del bit menos significativo del byte a incrustar en el bit menos significativo del octavo byte.

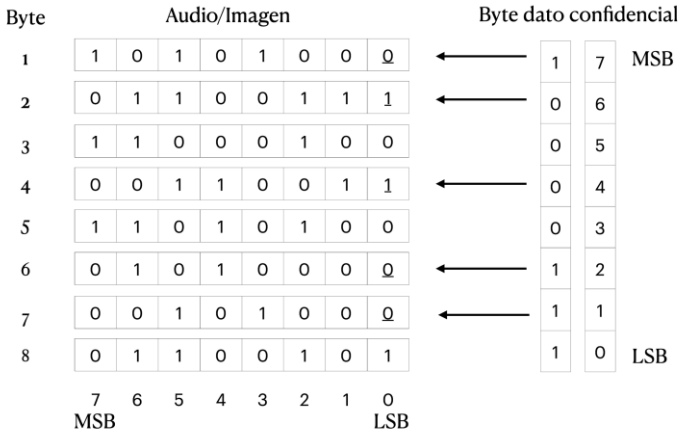


Figura 1. Proceso de inserción.

La Figura 2, muestra el resultado de la incrustación en el cual se puede observar que los bit menos significativos de los bytes 1, 2, 4, 6 y 7 cambiaron.

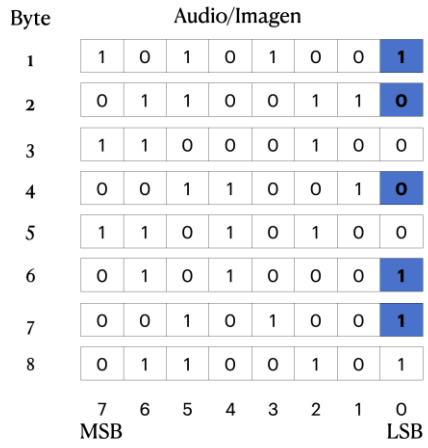


Figura 2. Inserción completa.

El método secuencial LSB ofrece la ventaja de no generar cambio de tamaño en los objetos contenedores, buscando también que las modificaciones no sean perceptibles a los sistemas visual y auditivo de las personas.

La Figura 3, muestra el proceso de incrustación en un píxel RGB (Red-Green-Blue). El dato a ocular es el carácter A que corresponde al valor 65 en decimal. Cada uno de los bits se incrustan en los bytes RGB del píxel. Como se puede observar el cambio producido por la incrustación implica la variación de una sola unidad, es decir, para el byte de R de 189 cambió a 188, mientras que el byte G cambió de 138 a 139 y el byte B se mantuvo en 82.

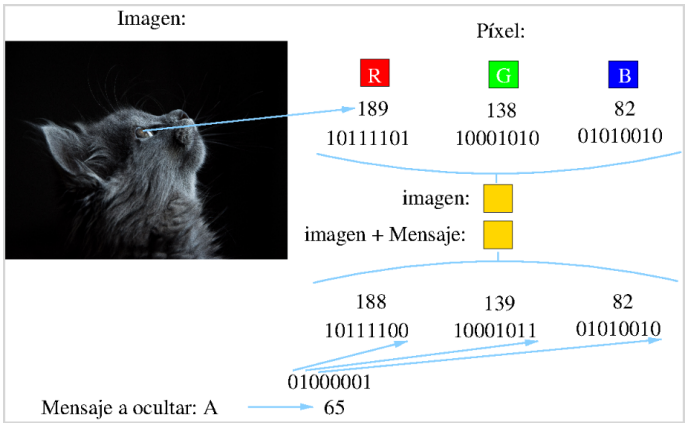


Figura 3. Incrustación en píxel.

Algoritmo LSB Secuencial

La aplicación del método LSB secuencial para incrustar objetos digitales puede implicar la incrustación opcional de las características del objeto o la incrustación sólo de los datos del objeto o de ambos. En el caso particular de este trabajo se decidió insertar el nombre, extensión del objeto digital y su contenido. La Figura 4, muestra la idea central de la incrustación de cualquier contenido digital en un objeto digital correspondiente a un archivo audio - WAV o imagen - BMP.

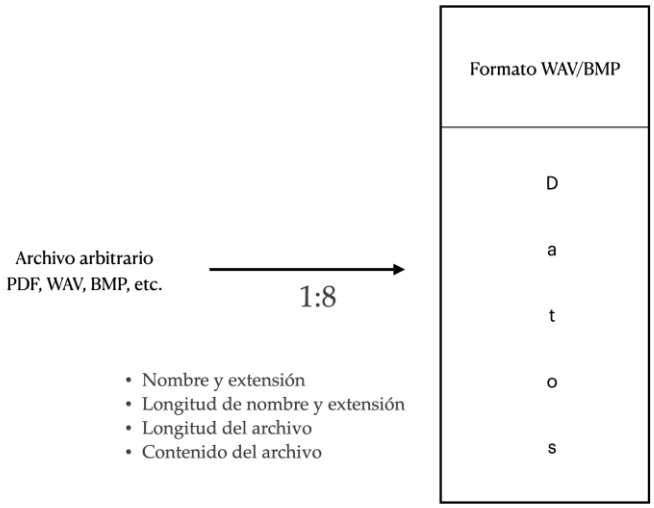


Figura 4. Inserción del objeto digital.

La incrustación requiere cumplir con una relación de 1 a 8, es decir cada byte del objeto a incrustar requiere 8 bytes del objeto contenedor. El objeto contenedor contendrá el nombre, extensión, longitud del nombre, longitud de la extensión, longitud del contenido y contenido del objeto incrustado.

La Figura 5, muestra la incrustación final del objeto digital. Como se puede observar la sección de encabezado se mantiene sin cambios, la incrustación se realiza en la sección de datos del objeto contenedor.

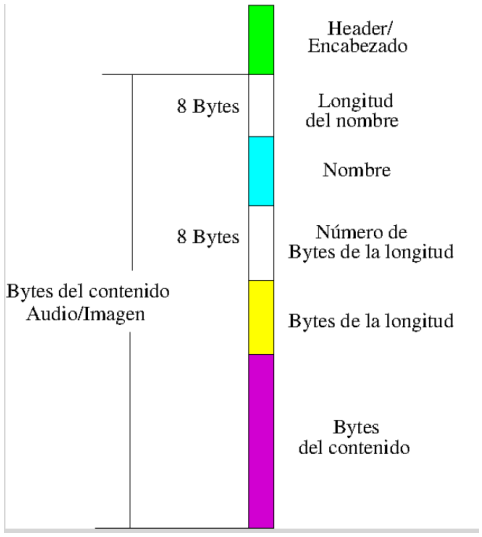


Figura 5. Inserción final del objeto digital.

La longitud del nombre y extensión del objeto a insertar se incrusta en los primeros 8 bytes del objeto contenedor, continuando con el nombre y extensión. Los siguientes 8 bytes se utilizan para especificar la longitud del objeto incrustado seguido de los datos del objeto incrustado.

La Figura 6, muestra el diagrama de flujo para la inserción y extracción. Se manejan tres principales opciones: insertar, extraer y su uso. La opción de incrustar requiere de una validación de la relación 1 a 8. Si el objeto contenedor tiene la capacidad para la incrustación se procede a insertar al objeto, de lo contrario se informa que no tiene la capacidad de incrustación siendo necesario un objeto contenedor con mayor capacidad. La opción de extraer realiza la extracción de los datos incrustados generando un objeto con el nombre, extensión y contenido del objeto incrustado. La opción uso muestra la sintaxis que se requiere para realizar las operaciones de insertar y extraer.

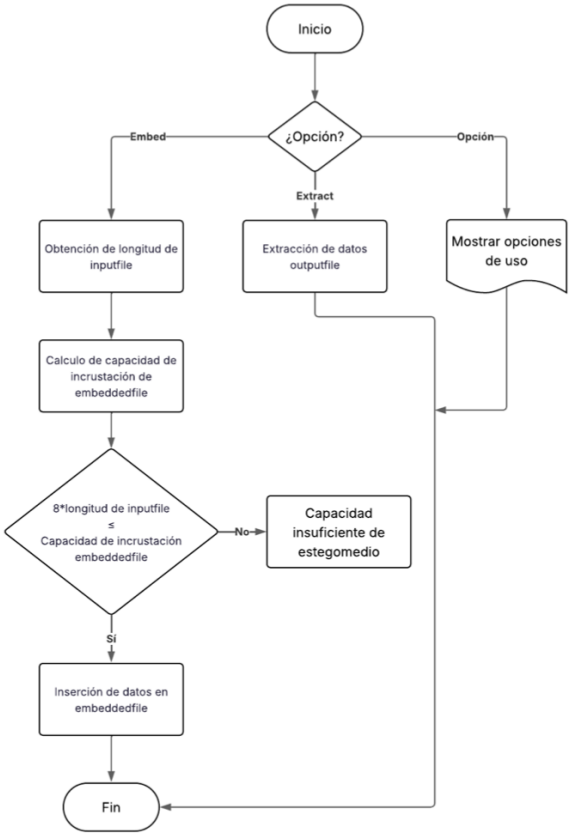


Figura 6. Diagrama de flujo para inserción y extracción.

Análisis de Resultados

Para analizar los resultados de la inserción de información se utilizó una imagen con formato BMP y un audio con formato WAV.

Inserción de información en imagen con formato BMP

La Figura 7, muestra la inserción de un archivo en formato PDF insertado en una imagen con formato BMP. El archivo en formato PDF se encuentra en la parte izquierda, seguido de la imagen contenedora que se encuentra al centro y la imagen resultante que se encuentra en la parte derecha. A la vista no se observan diferencias en la imagen resultante y la imagen original.

Figura 7. Inserción de información en imagen con formato BMP.

La Figura 8, muestra los histogramas de la imagen original y de la imagen resultante con archivo insertado/incrustado. El histograma resultante no revela cambio significativo sobre la distribución de los datos originales.

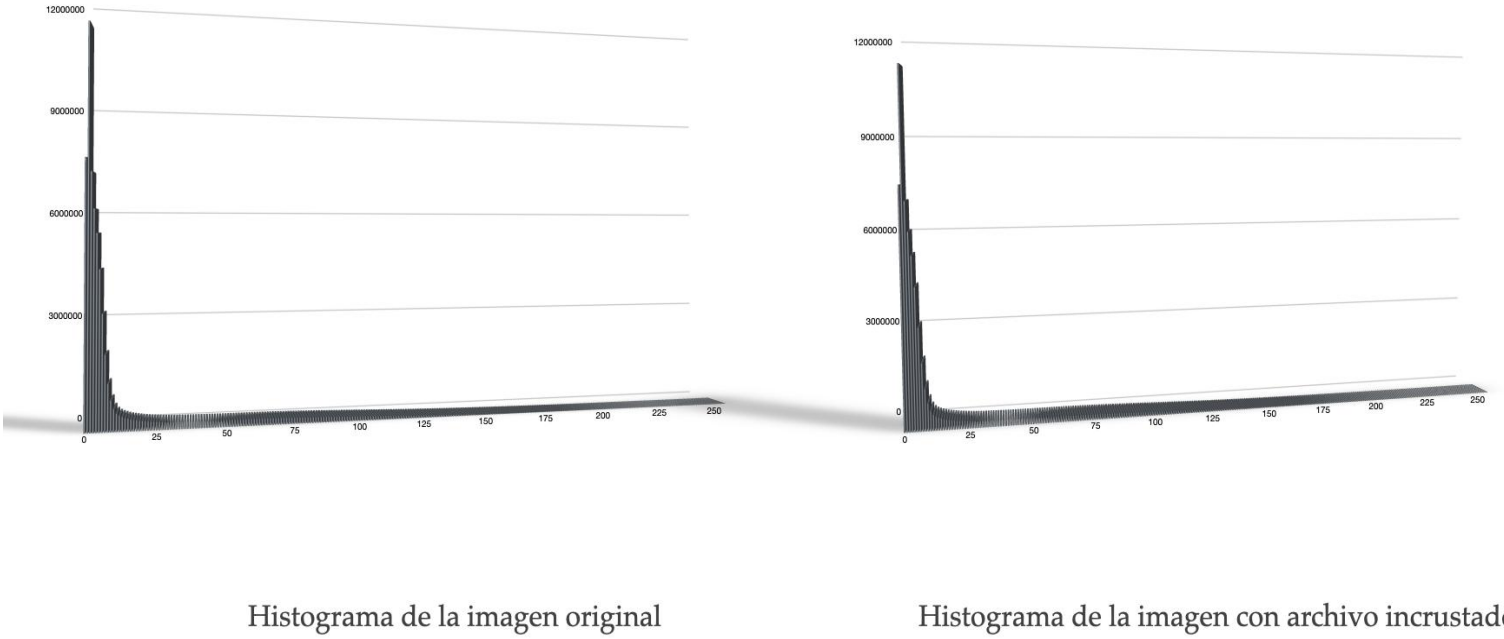


Figura 8. Histogramas de las imágenes contenedora y resultante.

La Figura 9, muestra la información del tamaño de la imagen contenedora, la cual tiene un tamaño de 72000122 Bytes. Al insertar la información fue necesario cambiar 851058 bits menos significativos, algunos cambiaron de 0 a 1 y otros de 1 a 0. Por otra parte 853110 bits menos significativos se mantuvieron con su valor de 0 o 1, es decir, sin cambio. Dados estos cambios el 99.85% de los bytes de la imagen se mantuvieron sin cambios.

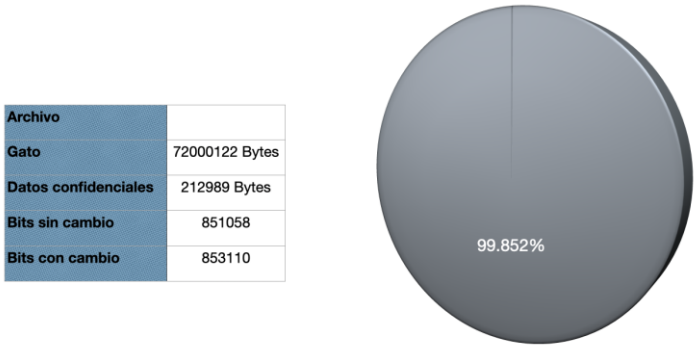


Figura 9. Información de la inserción en archivo BMP.

Inserción de información en audio con formato WAV

La Figura 10, muestra la inserción de un archivo en formato PDF insertado en un audio con formato WAV. El archivo en formato PDF se encuentra en la parte izquierda, seguido del audio contenedor que se encuentra al centro y el audio resultante que se encuentra en la parte derecha. En los diagramas de tiempo y amplitud de ambos audios se observan cambios. En la reproducción de ambos audios no hay percepción auditiva de posibles cambios.

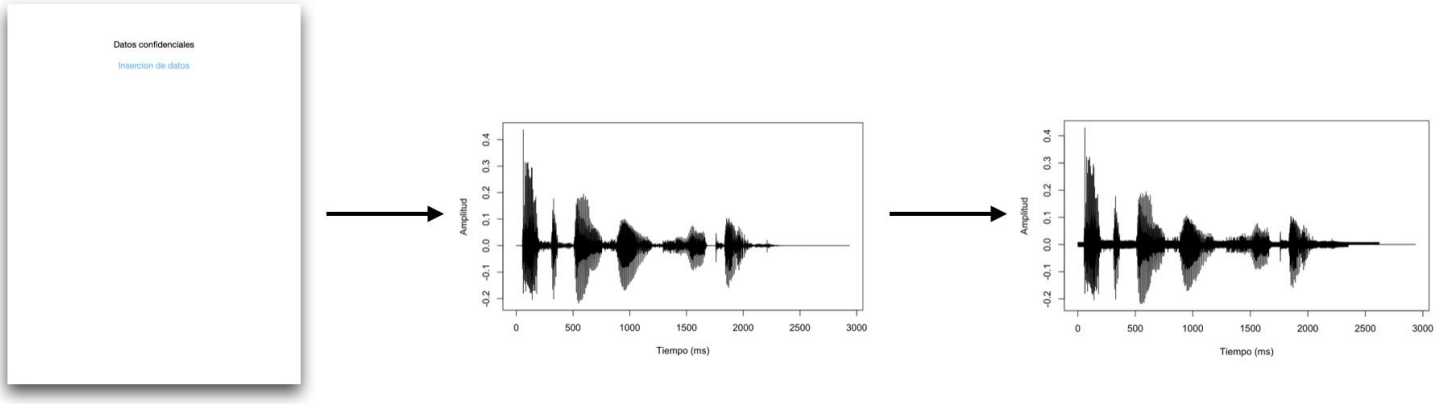


Figura 10. Inserción de información en audio con formato WAV.

La Figura 11, muestra los histogramas del audio original y del audio resultante con archivo insertado/incrustado. El histograma resultante revela cambios sobre la distribución de los datos originales.

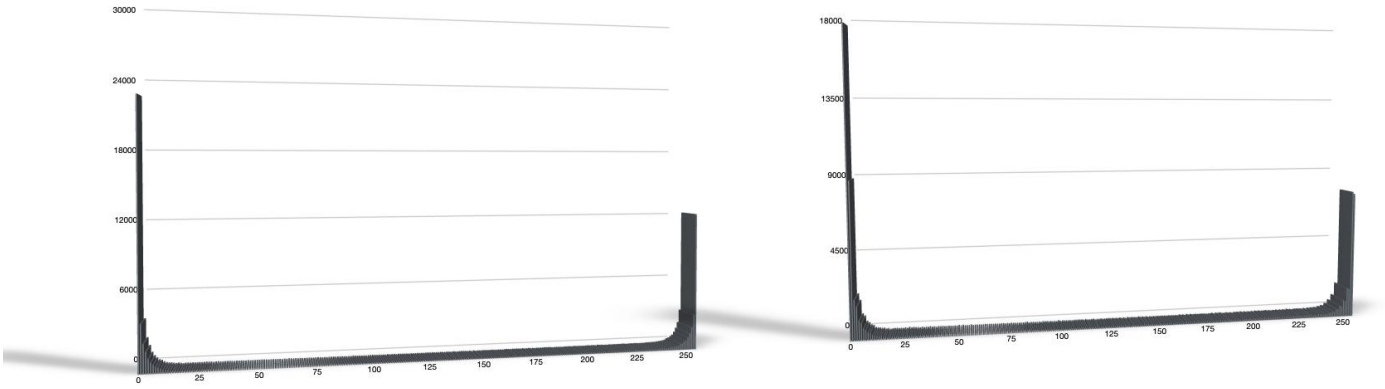
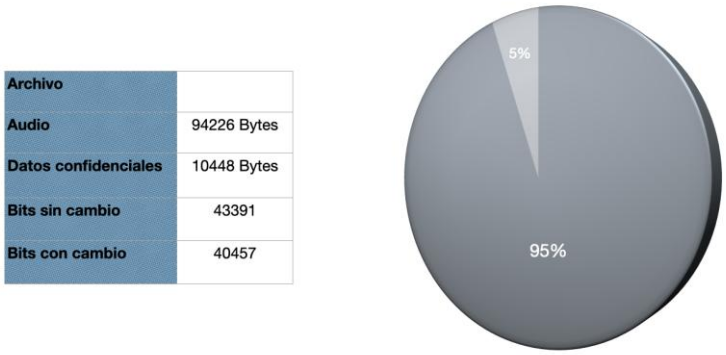


Figura 11. Histogramas de audio contenedor y resultante.

La Figura 12, muestra la información del tamaño del audio contenedor, la cual tiene un tamaño de 94226 Bytes. Al insertar la información fue necesario cambiar 43391 bits menos significativos, algunos cambiaron de 0 a 1 y otros de 1 a 0. Por otra parte 40457 bits menos significativos se mantuvieron con su valor de 0 o 1, es decir, sin cambio. Dados estos cambios el 95% de los bytes del audio se mantuvieron sin modificaciones y un 5% de los bytes fueron modificados.



Archivo	
Audio	94226 Bytes
Datos confidenciales	10448 Bytes
Bits sin cambio	43391
Bits con cambio	40457

Figura 12. Información de la inserción en archivo WAV.

Conclusiones

En este trabajo se presentó la aplicación de la esteganografía mediante el método LSB secuencial en documentos digitales con formato BMP y WA. demuestra que la técnica del bit menos significativo (LSB) secuencial constituye una estrategia eficaz y accesible para la implementación de esteganografía digital en medios multimedia.

En primer lugar, se comprobó que la utilización de imágenes en formato BMP y archivos de audio en formato WAV resulta adecuada debido a la ausencia de compresión con pérdida, lo que garantiza la integridad del mensaje oculto durante el almacenamiento y la transmisión.

Asimismo, los resultados obtenidos evidencian que la modificación de los bits menos significativos en píxeles (RGB) y muestras PCM permite insertar información sin generar alteraciones perceptibles para el sistema visual y auditivo humano. Esto confirma el principio de imperceptibilidad como uno de los pilares fundamentales de la esteganografía.

Desde el punto de vista técnico, el método LSB secuencial destaca por su simplicidad de implementación, bajo costo computacional y facilidad de comprensión, lo que lo convierte en una herramienta idónea para fines académicos y demostrativos.

No obstante, también se reconoce que, aunque eficiente, el método presenta limitaciones en términos de robustez y resistencia frente a técnicas avanzadas de estegoanálisis, lo que abre la posibilidad de futuras mejoras mediante esquemas más complejos o combinaciones con técnicas criptográficas.

En conclusión, el trabajo valida que la aplicación práctica del método LSB secuencial en archivos BMP y WAV representa una solución didáctica, funcional y efectiva para el ocultamiento de información digital, manteniendo un equilibrio adecuado entre capacidad, imperceptibilidad y simplicidad.

Referencias Bibliográficas

Swenson, C. (2008). Modern cryptanalysis: techniques for advanced code breaking. John Wiley & Sons.

Muñoz, A. M. (2016). Privacidad y Ocultación de Información Digital Esteganografía: Protegiendo y Atacando Redes Informáticas. Ra-Ma Editorial.

Microsoft Docs. (s.f.). Bitmap Storage. Windows

DGonzalez, R. C., & Woods, R. E. (2018). Digital Image Processing (4th ed.). Pearson.ev Center Documentation.

Microsoft & IBM. (1991). Multimedia Programming Interface and Data Specifications 1.0.

Pohlmann, K. C. (2010). Principles of Digital Audio (6th ed.). McGraw-Hill.

Stinson, D. R. (2005). Cryptography: theory and practice. Chapman and Hall/CRC.

Naor, M., & Shamir, A. (1994, May). Visual cryptography. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 1-12). Berlin, Heidelberg: Springer Berlin Heidelberg.

Stinson, D. R. (1997). An introduction to visual cryptography. Public Key Solutions, 97, 28-30.

Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.