Polo del Conocimiento

Pol. Con. (Edición núm. 3) Vol. 2 No 1
Enero 2017, pp. 51-67
ISSN: 2550 - 682X
DOI: 10.23857/pc.v2i1.10

Recepción: 03/ 06/ 2016
Aceptación: 27 / 10/ 2016
Publicación: 06/ 01/2017

Ciencias de la computación
Artículo de revisión

Análisis de técnicas de esteganografía aplicadas en archivos de audio e imagen

Analysis of steganography techniques applied in audio and image files

Técnicas de análise de esteganografia aplicados em arquivos de áudio e imagem

Gabriela Maholy Velásquez Moreira[I]
gabrielamv@yahoo.com
Lizandro Antonio Molina Sabando[II]
lizandro.molina@gmail.com
Ítalo Bécquer Briones Véliz[III]
ibbriones@yahoo.com

Correspondencia: gabrielamv@yahoo.com

[I] Ingeniera, Departamento de Tecnología de Información de la Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador

[II] Magister, Docente de la Facultad de Hotelería y Turismo de la Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador

[III] Magister, Director de la Unidad Central de Coordinación Informática, Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador

Resumen

El presente trabajo realiza un análisis descriptivo de las principales técnicas de esteganografía utilizadas en medios digitales específicos como los archivos de audio e imagen. Para esto se efectúo una revisión literaria de dominios, métodos y técnicas que son parte de este conjunto, identificando su funcionamiento, cualidades y debilidades. Se concluye que existe una amplia relación entre las técnicas de esteganografía de audio e imagen en su forma de implementación, se determina que LSB es una de las técnicas más débiles, y también se presentan cuáles son las técnicas más seguras y robustas dentro de cada tipo de medio.

Palabras clave: Audio; esteganografía; imagen.

Abstract

This paper provides a descriptive analysis of the main techniques used in specific steganography digital media such as audio and image files. For this a literature review of domains, methods and techniques that are part of this set was performed, identifying its functioning, strengths and weaknesses. It is concluded that there is a broad relationship between the techniques of audio and image steganography in its implementation. It is determined that LSB is one of the weakest techniques and are, also, presented the most secure and robust within each type of cover media.

Key words: Audio; steganography; image.

Resumo

Este documento oferece uma análise descritiva das principais técnicas usadas em mídia digital esteganografia específicos, tais como arquivos de áudio e imagem. Para esta uma revisão da literatura de domínios, métodos e técnicas que fazem parte deste conjunto foi realizada, identificando o seu funcionamento, os pontos fortes e fracos. Concluiu-se que há uma ampla relação entre as técnicas de áudio estenografia e imagem sob a forma de execução, é determinado que LSB é uma das técnicas mais fracos, e são também apresentados são as técnicas mais seguras e robustas estão dentro de cada tipo médio.

Palavras chave: áudio; esteganografia; imagem.

Introducción

La esteganografía ha ganado mucho espacio en el ámbito informático con el crecimiento del internet y el acceso a medios digitales, pero esto no significa que es una ciencia reciente, ya que la misma ha existido desde épocas muy antiguas (Kaur, Bansal & Bansal, 2014). De acuerdo a la revisión histórica realizada por Amirtharajan y Rayappan (2013) fueron los griegos, los primeros en usar lo más cercano a la esteganografía, teniéndose evidencia de esto desde antes del año 440 A.C., de tal manera que la palabra, como tal, tiene su origen en el lenguaje griego.

En particular, Dutta, Bhattacharyya y Kim (2009) muestran que las técnicas de esteganografía han encontrado su principal aplicación dentro del mundo de los negocios, entre ellos las marcas comerciales y la industria musical, en vista de la necesidad de mantener secretos de diseño comercial, proteger los derechos de autor en los medios digitales, y principalmente prevenir que personas no autorizadas lleguen a conocer la existencia del mensaje oculto. Del mismo modo, Zielinska, Mazurczyk y Szczypiorski (2014) exponen que la esteganografía es usada en actividades ilegales, como el terrorismo, tanto así que métodos esteganográficos fueron utilizados para planear los ataques de septiembre 11 de 2001. A causa de estos dos factores, durante la última década se observa una investigación intensiva en la esteganografía y sus métodos de detección.

Actualmente, existen diversos tipos de esteganografía, y también aplicaciones informáticas disponibles que facilitan su aplicación en la rama de los medios digitales, donde sobretodo destacan los archivos de imagen y audio, dado que han sido los más explotados, debido a los numerosos métodos creados para ocultar información en estos; y porque, generalmente, otros tipos de archivos digitales como los videos utilizan las mismas técnicas que se aplican en audio (Zielinska, Mazurczyk & Szczypiorski, 2014). Adicionalmente Ker et al. (2014) destacan que la esteganografía es mucho más sofisticada en el medio digital que en otros dominios como los canales de red, puesto que consideran que la esteganografía basada en redes aún debe aprender bastante de la basada en los medios digitales.

Con base en lo expuesto anteriormente, se hace evidente el alto grado de investigación dentro de la esteganografía, en el ámbito de medios digitales con los archivos de audio e imagen. Todo

esto, ha conllevado a que se tenga una gran cantidad de técnicas aplicables a estos tipos de archivos que con el paso del tiempo han evolucionado o generado otras nuevas.

Por tanto, es necesario efectuar el presente trabajo de revisión que permita analizar las técnicas de esteganografía que son usadas en los archivos de imagen y audio, con el objetivo de presentar una revisión actualizada de estas principales técnicas con sus fortalezas y debilidades, a través de las diferentes investigaciones que se han realizado en este campo.

Desarrollo

Esteganografía

La Esteganografía suele confundirse con la criptografía, por ser ambas parte de los procesos de protección de la información, son disciplinas distintas, tanto en su forma de implementar como en su objetivo mismo. Mientras que la criptografía se utiliza para cifrar información de manera que sea ininteligible para un probable intruso, a pesar del conocimiento de su existencia. (Esteganografía. 2017).

Según Provos y Honyeman (2003), la esteganografía es el arte de esconder información, a través de un sistema esteganográfico que incrusta los datos ocultos en otro medio de comunicación normal sin dejar sospechas. Adicionalmente, Dixit, Waskar y Bombale (2015) consideran que la esteganografía es la ciencia que se encarga de esconder la existencia de determinada comunicación.

Por otro lado, Wang y Wang (2004) exponen que la esteganografía difiere de la criptografía, puesto que esta última no oculta la información sino que sólo codifica los datos, lo que las convierte en dos ciencias complementarias y ortogonales, ya que es posible aplicar un algoritmo criptográfico a la información antes de ser ocultada; de esta manera, si los datos encubiertos son revelados, se mantiene una seguridad adicional con estos, porque también estarían encriptados.

También Wang y Wang (2004) destacan que son requerimientos relevantes de la esteganografía contar con un alto grado de imperceptibilidad, proveer de algoritmo sin detectables y ser capaz de sobrevivir a la compresión normal por código.

Técnicas de esteganografía en archivos de audio

Según Antony, Sobin y Sherly (2012), la esteganografía en audio es más importante que en otros medios de esteganografía (texto, imagen, video), debido a que puede transportar más información redundante en comparación de otros medios, para esto se requiere de un medio de cobertura para ocultar el mensaje secreto que al unirlos se convierten en el estegano-objeto (Figura 1).

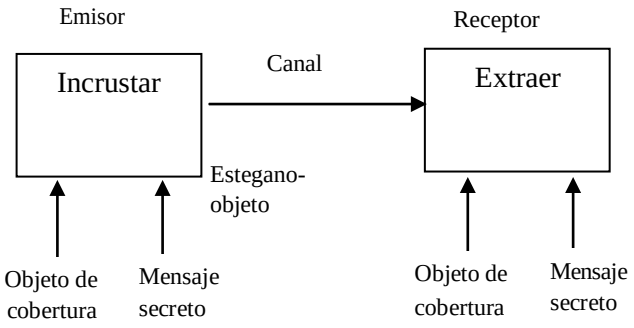

Figura 1: Diagrama de bloque para esteganografía en audio
Fuente: Antony, Sobin y Sherly (2012)

En este ámbito de la esteganografía en audio, Djebbar, Ayad, Hamam y Abed-Marian (2011) proponen la siguiente clasificación: 1) dominio temporal, 2) dominio de frecuencia, 3) dominio de ondícula y 4) dominio de códecs.

Dominio Temporal

Este dominio lo conforman principalmente las siguientes técnicas: 1) Low bit encondig y 2) Echo Higing. También se las conoce como técnicas de dominio espacial. (Malhotra, y Tahilramani, 2014).

- Low Bit Encoding

De acuerdo con Olanrewaju, Khalifa & Rahman (2013), esta técnica, conocida también con el nombre de Least Significant Bit (LSB), es una de las primeras estudiadas para el ocultamiento de datos en las señales de audios. El funcionamiento se basa en seleccionar, por medio del codificador de marca de agua LSB, un subconjunto de muestras de audios elegidas por una clave secreta, y en este subconjunto de datos se realiza la sustitución de los bits a ocultar por el valor de los bits originales.

Adicionalmente, Atony, Sobin y Sherly (2012) resumen que la principal ventaja al hacer uso de LSB es la facilidad que presta para su aplicación de forma sencilla, y siendo, al mismo tiempo, una gran debilidad esa misma simplicidad, puesta que los datos ocultos son extraídos por personas no autorizadas fácilmente.

- Echo Hiding

Según Gruhl, Lu y Bender (1996), esta es una técnica que incrusta información dentro de una señal de audio, y basa su funcionamiento en encontrar "huecos" dentro los rangos de percepción del sistema auditivo humano, donde los datos pueden ser ocultados, con el objetivo principal de que estos tengan una degradación mínima con respecto a los datos originales, lo que permite que el cambio en el audio sea más difícil de percibir para el oyente.

Por otro lado, Dutta, Bhattacharyya y Kim (2009) afirman que si se produce solamente un eco en la señal original, solamente un bit puede ser codificado, además de ofrecer ventajas como la alta tasa de transmisión de datos y mayor robustez que otros métodos.

Dominio de Frecuencia

Las principales técnicas de dominio de frecuencia, acorde con Anthony, Sobin y Sherly (2012), son: 1) Tone insertion, 2) Phase Coding, 3) Amplitude modification y 4) Spread sepctrum. A continuación se describe cada una de ellas.

- Tone insertion

De acuerdo con Gopalan y Wenndt (2004), Tone Insertion se encarga de conseguir la imperceptibilidad auditiva de tonos de bajo poder, dentro de un espectro más grande. Para esto, el audio original es dividido en segmentos de 16ms de duración, donde se calcula el poder de cada marco y únicamente un bit de los datos, es incrustado en el audio original.

Ahora bien, Djebbar, Ayad, Meraim y Hamam (2012) resaltan que Tone insertion es resistente a ataques de filtro low-bass y truncado de btis, sin embargo una limitante es la baja capacidad de incrustación de datos, lo cual permite que los tonos insertados sean fáciles de detectar.

- Phase Coding

Según Malik, Ansari y Khokhar (2007) esta técnica se encarga de incrustar información en la fase de la señal huésped, lo que la caracteriza es el buen rendimiento que posee respecto a la fidelidad del dato oculto. No obstante, uno de sus limitantes es la poca capacidad de incrustación, ya que embebe 16-32 bits de datos en archivos de audio de 1 segundo de duración.

- Amplitude modification

Jenkins y Martina (2010), indican que al implementar esta técnica se realiza una traducción del algoritmo dentro del código, donde lo más relevante de dicho código es el ordenamiento de las amplitudes principales. Adicionalmente, Amplitude modification puede incrustar de manera separada dentro de cada canal, utilizando tres secciones de 512-frame, y logrando una muy buena compresión, pero con el riesgo de que se pierdan los datos en la compresión mono. Este método presenta una gran debilidad en términos de audición, mas tiene un gran potencial si se realizan algunos ajustes de reducción de volumen y uso de segmentos de longitud de variables criptográficas.

- Spread Sepectrum

Giallorenzi, Lake, Kingston y Harris (2010) afirman que los dos tipos más comunes de spread spectrum son los saltos de frecuencia, donde el código de un seudo-ruido se utiliza seudo-aleatoriamente para ayudar al cambio de transmisión de frecuencia periódicamente, y la secuencia directa, donde el código de seudo-ruido se usa para modular secuencialmente la señal en una alta tasa. Estos autores destacan que una de las ventajas de esta técnica es la dificultad de la transmisión en ser detectada.

Dominio de ondícula

Conforme a lo que describen Anthony, Sobin y Sherly (2012), el Dominio de ondícula, o mejor conocido en inglés como Wavelet Domain, tiene propiedades de multi-resolución que lo convierten en apropiado para el análisis de frecuencia, además de trabajar con coeficientes de ondículas, logrando que, al aplicarse una transformación inversa, sea posible reconstruir la estegano-señal.

Adicionalmente, Cvejic y Seppänen (2002), proponen un método general para trabajar con Wavelet Domain, a través de la descomposición de la señal con eluso de LSB al ocultar la información, demostrando así que una gran ventaja de esta técnica es una mayor transparencia y capacidad de ocultamiento en comparación con otros dominios.

Dominio de codificador

Djebbar, Ayad, Hamam y Abed-Marian (2011) exponen que forman parte de este dominio las técnicas Codebook modification y Bistream hiding, siendo ambas utilizadas en conjunto para ocultar datos en comunicaciones de tiempo real, por medio del uso de códecs de voz como: AMR, ACELP o SILK.Estos autores destacan que una de las fortalezas de estas técnicas es la alta robustez, sin embargo, su debilidad radica en tener una baja tasa de incrustación.

Técnicas de esteganografía en archivos de imagen

Según, Fridrich (2009) existen dos formas de crear imágenes digitales, una es a través de la computadora, con herramientas de dibujo o diseño que generan diagramas, gráficos estadísticos u otros, y la otra es con los sensores que generan imágenes digitales, los cuales son el corazón de dispositivos como escáneres, cámaras digitales y video cámaras digitales. Por tanto, afirma que este segundo tipo de imágenes son las favoritas para la esteganografía, debido a que se las más usadas y por ende se ha desarrollado un mejor ambiente para el uso de estas.

En este caso, Hussain y Hussain (2013), clasifican a las técnicas de imagen en esteganografía en los siguientes dominios: 1) métodos de domino espacial, 2) técnica del dominio de transformación, 3) técnicas de distorsión y 4) enmascaramiento y filtrado.

Dominio espacial

Swain y Lenka (2014) aseguran que existen muchos métodos en el dominio de espacial, de los cuales se destacan los siguientes: 1) Least Significant Bit, 2) RGB based steganography, 3) Pixel Value Differencing (PVD) y 4) Mapping based steganography. Seguidamente, se presentan cada una de estas técnicas.

- Least Significant bit

Con respecto a esta técnica, Kaur, Bansal y Bansal (2014), sostienen que es la más popular y simple en el trabajo con imágenes, puesto que cuenta con una baja complexidad computacional y alta capacidad de incrustación. También Swain y Lenka (2014) indican que LSB oculta los mensajes dentro de una imagen remplazando el bit menos significativo de cada pixel, es decir el bit de menor valor, por los datos a incrustar.

En particular, Singla y Juneja (2014) señalan que esta técnica no es segura, dado que la estego-imagen contiene manchas en los lugares donde se ocultan los bits, y al aplicar ataques, como el análisis de pares de muestras, análisis de histograma de imagen u otros, se puede obtener fácilmente la información.

- RGB based steganography

Bairagi, Mondal y Debnath (2014) exponen que esta técnica se denomina de tal manera a causa de los tres colores primarios en inglés, Red (R), Green (G) y Blue (B), donde un valor por cada tres valores describen un pixel, es decir cada pixel es una combinación de los componentes R, G y B en un esquema de color de 24 bits. Ahora bien, Gutub (2010) propone un método usando pixeles de imagen RGB como medio de cobertura, a través del uso de un canal para la indicación de los datos secretos en los otros canales, en el que el canal de indicación cambia de un pixel a otro con valores aleatorios naturales que dependen de los píxeles de la imagen.

En el caso del estudio de Gutub (2010), las comparaciones, realizadas entre esta técnica basa en RGB y otras técnicas de LSB, demuestran que tiene más capacidad con el mismo de nivel de seguridad.

- Pixel Value differencing

Respecto a PVD, Wu y Tsai (2003) refieren que este método facilita la incorporación de mensajes secretos en una imagen, sin que se produzca grandes cambios en el archivo original, puesto que su mecanismo se basa en incrustar los datos secretos en una imagen de cobertura, mediante la sustitución de los valores de la diferencia de los bloques de dos píxeles de dicha imagen, con otros similares donde se incluyen bits de datos incrustados. De la misma manera,

estos autores señalan que una de sus características es el aprovechamiento a la sensibilidad de la vista humana para las variaciones de valores grises.

Otros autores, como Shen y Huang (2014), destacan que PVD puede incrustar más datos en parejas de píxeles con más grandes diferencias. Sin embargo, en estos casos, PVD provoca una distorsión considerable que conlleva a la degradación de la calidad de la imagen.

- Mapping Based Steganography

Según, Bhattacharyya, et al. (2011), esta técnica se la puede llamar Pixel Mapping Method (PMM), y puede ocultar datos dentro de cualquier imagen con escala de grises. Esto lo hace, seleccionando los pixeles de incrustación por medio de funciones matemáticas dependiendo de la intensidad del valor del pixel semilla. Antes de la incrustación, se realiza un chequeo que define si los pixeles seleccionados o sus vecinos se encuentran dentro de los límites de la imagen o no, y luego la incrustación de datos se efectúa con un mapeo de cada dos o cuatro bits del mensaje secreto en cada pixel vecino. Dentro de la tabla 1 se aprecia este mapeo de la información para incrustación de dos bits.

Tabla 1: Técnica de mapeo de PMM para incrustación de dos bits.

Pareja de bit	Intensidad de valor del pixel	No of ones (Bin)
01	Par	Impar
10	Impar	Par
00	Par	Par
11	Impar	Impar

Fuente: (Bhattacharyya et al., 2014)

Por otro lado, Banerjee, Bhattacharyya y Sanyal (2013) han desarrollado un método extendido de PMM, donde se ha medido el rendimiento de PMM a través de varias técnicas de métricas como Mean Square Error (MSE), Peak Signal-to-Noise Radio(PSNR), Root Mean Square Error(RMSE)y Structural Similarity Index(SSI), y también se ha hecho una medición con técnicas de estegoanálisis comoRS analysis, SP analysis y Chi-square analysis, dando como resultado una alta seguridad medida y probada.

Dominio de transformación

Según Hussain y Hussain (2013), el dominio de transformación se clasifica en las siguientes técnicas: 1) Discrete Fourier Transformation (DFT), 2) Discrete Cosine Transformation (DCT), 3) Discrete Wavelet Transformation (DWT). Además afirma que las técnicas de esteganografía más fuertes, al día de hoy, trabajan en el dominio de transformación, puesto que tienen una ventaja sobre las técnicas de dominio espacial, al ocultar la información en áreas que están menos expuestas a la compresión, recorte y al procesamiento de imagen. Las técnicas de este dominio se exponen a continuación.

- Discrete Fourier Transformation

De acuerdo con Morkel, Eloff y Olivier (2005), DFT es una técnica basada en transformaciones matemáticas que convierten los píxeles de tal manera que da el efecto de difundir la ubicación de los valores de los píxeles sobre una parte de la imagen. Por otro lado, Soni, Jain y Roshan (2013) recogen en su trabajo las ventajas de la esteganografía en imagen con Fractional Fourier Transform (FrFT), la cual es una generalización de DFT, que por su orden fraccional (α) logra un dominio óptimo, dado que en las pruebas de desempeño con PSNR y MSE obtiene resultados ideales. Así, FrFt con un parámetro adicional fraccional (α) presenta una mayor seguridad frente a otras técnicas del dominio de transformación.

- Discrete Cosine Transform

En relación a la técnica DCT, Walia, Jain Y Navdeep (2010) sostienen que actúa, en la esteganografía, incrustando el mensaje secreto en el bit menos significativo del coeficiente del coseno discreto de una imagen digital. Asimismo, estos autores explican que su funcionamiento se basa en descomponer la imagen en bloques de píxeles de 8x8; así de derecha a izquierda y de arriba hacia abajo, DCT es aplicado a cada bloque, hasta que finalmente el mensaje es incrustado en los coeficientes de DCT.

Además, Chandran y Bhattacharyya (2015), en un análisis efectuado a DCT concluyen que posee ventaja en comparación a algoritmos como LSB y DWT puesto que los resultados de PSNR son altos respecto a los otros dos algoritmos, aunque dentro de los mismos resultados también se observa que la robustez DCT es mediana.

- Discrete Wavelet Transform

La técnica Discrete Wavelet Transform (DWT), de acuerdo a Kashyap y Sinha (2012) es una herramienta matemática utilizada para la descomposición de las imágenes que se basa en transformación de pequeñas ondas, llamadas ondículas, de diferentes frecuencias.

Técnicas de distorsión

Acerca de las técnicas de distorsión, Hamid, Yahya, Ahmad, (2012), explican que estas se caracterizan por necesitar conocimiento de la imagen original de cobertura durante el proceso de decodificación con el fin de comprobar si hay diferencias ente la imagen original y la imagen distorsionada. Por el contario, el codificador añade una secuencia de modificaciones en la imagen de cobertura, creándose un estego-objeto. Esta secuencia de modificaciones se selecciona para que coincida con el mensaje que se requiere enviar.

Así pues, Kruus, Scace, Heyman, (2003), señalan que esta técnica limita ciertas ventajas al tener que necesariamente enviar la imagen de cobertura, considerando que las técnicas de esteganografía no deben usar la imagen de cobertura más de una vez

Enmascaramiento y filtrado

En relación al enmascaramiento y filtrado, Krenn (2004) describe que esta técnica tienen una efectividad similar a las marcas de agua de documentos, creando máscaras en una imagen. Aunque el enmascaramiento sí cambia las propiedades de la imagen, este se puede realizar de tal forma que a la vista humana no se identifiquen las anomalías. Este autor, también destaca que el enmascaramiento y filtrada presenta mayor robustez que LSB con respecto a la compresión, recorte y procesamiento de imágenes.

No obstante, Hussain y Hussain (2013) mencionan que esta técnica, generalmente, está restringida a trabajar con imágenes de 24 bits o imágenes con escales de grises, pero tiene a su favor que los datos se ocultan en la parte visible de la imagen y no en otro nivel, lo que le brinda resistencia a los algoritmos de compresión, en el caso de formatos JPEG.

Conclusiones, limitaciones y trabajos futuros

Al finalizar el presente análisis se puede concluir que tanto la esteganografía en audio como en imagen guardan mucha relación en cuanto a la forma de implementación de las técnicas y al fin mismo de cada una que es ocultar un mensaje y mantener imperceptible e indetectable, tanto a la vista como al oído humano, los datos incrustados. No obstante, existen técnicas muy débiles que ya han sido vulneradas, como LSB, la cual es una de la más simples de aplicar pero ofrece muy poca seguridad y robustez ya que los datos ocultos son fácil de extraer. Por otro lado, hecho hiding y Spread Spectrum se encuentran dentro los métodos más seguros para la esteganografía en audio; asimismo, PMM y Discrete Cosine Transformcuentan con mayor seguridad con respecto a otras técnicas.

Dentro de las limitaciones del presente documento se encuentran la cantidad de información analizada puesto que, durante la última década, se han publicado un gran número de trabajos relevantes relacionados al presente tema de estudio y, por ende, no todos han sido revisados. Otra de las limitantes es la realización del análisis, solo, en función de un enfoque cualitativo.

Vale destacar, entonces, que para futuros trabajos se puede considerar el llevar a cabo un análisis cuantitativo o meta análisis que ayude a determinar, con mayor precisión y de manera estadística, las ventajas y desventajas, así como las cualidades y debilidades de estas técnicas aquí estudiadas. Adicionalmente, se puede ahondar en nuevas investigaciones que permitan establecer en qué nuevas áreas se está haciendo uso de la esteganografía, tal como ya han empezado a hacerlo los autores Zielinska, Mazurczyk, y Szczypiorski (2014) en su trabajo Trends in Steganogarphy,donde se hace una revisión del uso actual de la esteganografía en protocolos de redes, archivos de medios sociales, entre otros.

Referencias bibliográficas

Amirtharajan, R., & Rayappan, J. B. (2013). Steganography—Time to Time: A Review. Research Journal of Information Technology, 5(2), 58-66.

Antony, J., Sobin, C. C., & Sherly, a. P. (2012). Audio Steganography in Wavelet Domain A Survey. International Journal of Computer Applications, 52(13), 33–37. http://doi.org/10.5120/8265-1810

Bairagi, A. K., Mondal, S., & Debnath, R. (2014, March). A robust RGB channel based image steganography technique using a secret key. In Computer and Information Technology (ICCIT), 2013 16th International Conference on (pp. 81-87). IEEE

Bhattacharyya, S., Khan, A., Nandi, A., Dasmalakar, A., Roy, S., & Sanyal, G. (2011, December). Pixel mapping method (PMM) based bit plane complexity segmentation (BPCS) steganography. In Information and Communication Technologies (WICT), 2011 World Congress on (pp. 36-41). IEEE.

Banerjee, I., Bhattacharyya, S., & Sanyal, G. (2013). Hiding & Analyzing Data in Image Using Extended PMM. In International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) (Vol. 10, pp. 157–166). http://doi.org/10.1016/j.protcy.2013.12.348

Cvejic, N., & Seppänen, T. (2002). A wavelet domain LSB insertion algorithm for high capacity audio steganography. Proceedings of 2002 IEEE 10th Digital Signal Processing Workshop, DSP 2002 and 2nd Signal Processing Education Workshop, SPE 2002, 53–55. http://doi.org/10.1109/DSPWS.2002.1231075

Chandran, S., & Bhattacharyya, K. (2015, January). Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography. In Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on (pp. 1-5). IEEE.

Dutta, P., Bhattacharyya, D., & Kim, T. (2009). Data Hiding in Audio Signal : A Review. International Journal of Database Theory and Application, 2(2), 1–8.

Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H. (2012). Comparative study of digital audio steganography techniques. EURASIP Journal on Audio, Speech, and Music Processing, 2012(1), 1-16.

Dixit, P. H., Waskar, K. B., & Bombale, U. L. (2015). Multilevel Network Security Combining Cryptography and Steganography on ARM Platform, 3(1), 11–15. Recuperado de http://doi.org/10.12691/jes-3-1-2

Esteganografía. 2017. EcuRed. Recuperado de https://www.ecured.cu/Esteganograf%C3%ADa

Fridrich, J. (2009). Steganography in digital media: principles, algorithms, and applications. Cambridge University Press.

Gutub, A. A. A. (2010). Pixel indicator technique for RGB image steganography. Journal of Emerging Technologies in Web Intelligence, 2(1), 56–64. http://doi.org/10.4304/jetwi.2.1.56-64

Giallorenzi, T., Lake, M., Kingston, S, & Harris, J (2010). U.S. Patent No. US 7,643,537 B1. Washington, DC: U.S. Patent and Trademark Office.

Hussain, M., & Hussain, M. (2013). A survey of image steganography. International Journal of Advanced Science and Technology, 54, 1–13.

Hamid, N., Yahya, A., Ahmad, R., & Al-Qershi, O. (2012). Image steganography techniques: an overview. International Journal of Computer Science and Security (IJCSS), 6(3), 168-187

Jenkins, N., & Martina, J. E. (2009). Steganography in Audio. Anais Do IX Simpósio Brasileiro Em Segurança Da Informação E de Sistemas Computacionais, 269–278.

Kaur, S., Bansal, S., & Bansal, R. K. (2014). Steganography and classification of image steganography techniques. In 2014 International Conference on Computing for Sustainable Global Development, INDIACom 2014 (pp. 870–875). New Delhi: IEEE. Recuperado de http://doi.org/10.1109/IndiaCom.2014.6828087

Kruus, P., Scace, C., Heyman, M., & Mundy, M. (2003). A survey of steganography techniques for image files. Advanced Security Research Journal. [On line], 5(1), 41-52.

Ker, A. D., Bas, P., Böhme, R., Cogranne, R., Craver, S., Filler, T., & Pevný, T. (2013), Junio). Moving steganography and steganalysis from the laboratory into the real world. In Proceedings of the first ACM workshop on Information hiding and multimedia security (pp. 45-58). ACM.

Krenn, R. (2004, Enero). Steganography andSteganalysis. Recuperado de http://www.krenn.nl/univ/cry/steg/article.pdf

Malhotra, N., & Tahilramani, N. (2014). Survey on Speech and Audio Steganography Techniques in Temporal, Transform and Coded Domains. International Journal of Advanced Research in Computer Science and Software Engineering, 4(3), 800–809

Malik, H. M. A., Ansari, R., & Khokhar, A. A. (2007). Robust data hiding in audio using allpass filters. IEEE Transactions on Audio, Speech and Language Processing, 15(4), 1296–1304. http://doi.org/10.1109/TASL.2007.894509

Morkel, T., Eloff, J. H. P., & Olivier, M. S. (2005). An Overview of Image Steganography. In Proceedings of the ISSA 2005 New Knowledge Today Conference (Vol. 83, pp. 51–107). South Africa.

Olanrewaju, R. F., Khalifa, O., & Rahman, H. (2013). Increasing the hiding capacity of low-bit encoding audio steganography using a novel embedding technique. World Applied Sciences Journal, 21(SPECIAL ISSUE1), 79–83. ttp://doi.org/10.5829/idosi.wasj.2013.21.mae.99926

Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE Security and Privacy, 1(3), 32–44. http://doi.org/10.1109/MSECP.2003.120322

Swain, G., & Lenka, S. K. (2014). Classification of Image Steganography Techniques in Spatial Domain : A Study. International Journal of Computer Science & Engineering Technology, 5(03), 219–232.

Singla, D., & Juneja, M. (2014, March). An analysis of edge based image steganography techniques in spatial domain. In Engineering and Computational Sciences (RAECS), 2014 Recent Advances in (pp. 1-5). IEEE

Shen, S. Y., & Huang, L. H. (2015). A data hiding scheme using pixel value differencing and improving exploiting modification directions. Computers & Security, 48, 131-141.

Soni, A., Jain, J., & Roshan, R. (2013). Image steganography using discrete fractional Fourier transform. In 2013 International Conference on Intelligent Systems and Signal Processing (ISSP) (pp. 97–100). Gujarat: IEEE. http://doi.org/10.1109/ISSP.2013.6526882

Wang, H., & Shuozhong, W. (2004). Cyber Warfare: Steganography vs. Steganalysis. Communications of the ACM, 47(10), 76–82.

Wu, D, & Tsai, W. (2003). A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 24(9), 1613-1626.

Walia, E., Jain, P., & Navdeep, N. (2010). An analysis of LSB & DCT based steganography. Global Journal of Computer Science and Technology, 10(1).

Zielinska, E., Mazurczyk, W., & Szczypiorski, K. (2014). Trends in Steganography. Communications of the ACM, 57, 86–96.