Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Una nueva técnica de transmisión segura de imágenes aplicando transformaciones de color reversibles en zonas ruidosas de la imagen

A new secure image transmission technique applying reversible color transformations in noisy regions of the image

Uma nova técnica para a transmissão segura de imagens através da aplicação de transformações de cores reversíveis em áreas ruidosas da imagem

Cristian Marcelo Vasco Estupiñan
Universidad de las Fuerzas Armadas ESPE, Ecuador
crisvasco93@hotmail.com
https://orcid.org/0000-0002-2997-9510

Freddy Roberto Acosta Buenaño
Universidad de las Fuerzas Armadas ESPE, Ecuador
fracosta@espe.edu.ec
https://orcid.org/0000-0002-2143-5471

Resumen

La esteganografía es un proceso que consiste en ocultar información dentro de un objeto (contenedor). Es un desafío mejorar las técnicas actuales de esteganografía con el fin de que proporcionen seguridad contra ataques de estegoanálisis estadístico. Este artículo propone una nueva técnica de transmisión segura de imágenes mediante la combinación de dos métodos: el primero basado en transformaciones reversibles de color, el cual transforma una imagen secreta en una imagen mosaico que luce similar a una imagen portadora seleccionada previamente; y el segundo busca las áreas más adecuadas (texturas y bordes) en la imagen mosaico creada para ocultar la información relevante requerida y posteriormente recuperar la imagen secreta. Estas zonas son de naturaleza ruidosa, por lo que representan un reto para el estegoanálisis al momento

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

de extraer características encargadas de determinar si una imagen tiene información embebida. La efectividad del método propuesto se evaluó mediante el análisis de histogramas y utilizando la herramienta de estegoanálisis StegExpose.

Palabras clave: estegoanálisis estadístico, esteganografía, estegoimagen, imagen mosaico, transformaciones reversibles de color.

Abstract

The steganography is a process that consists in hiding information inside an object (container). Improving current steganography techniques in order to provide robustness against statistical attacks is a challenge. This article proposes a new secure image transmission technique by combining 2 methods: The first one is based in reversible colors transformations, which turns the secret image into a mosaic that looks similar to the carrier image previously selected. The second one looks for the most suitable areas (border and texture) in the created mosaic to hide relevant information that is required to recover the secret image. These zones are noisy nature, so they represent a challenge for the steganalysis at the moment of extracting characteristics that determine if an image has embedded information. The effectiveness of the proposed method is evaluated by analysis of histograms and using the steganalysis tool StegExpose.

Keywords: statistical steganalysis, steganography, stego image, mosaic image, reversible color transformations.

Resumo

Esteganografia é um processo que envolve a ocultação de informações dentro de um objeto (container). É um desafio melhorar as técnicas atuais de esteganografia para fornecer segurança contra ataques estatísticos de steganánalise. Este artigo propõe uma nova técnica de transmissão segura de imagens, combinando dois métodos: o primeiro, baseado em transformações reversíveis de cores, que transforma uma imagem secreta em uma imagem em mosaico semelhante a uma imagem de portadora previamente selecionada; e a segunda pesquisa as áreas mais adequadas (texturas e bordas) na imagem em mosaico criada para ocultar as informações relevantes necessárias e, subsequentemente, recuperar a imagem secreta. Essas áreas são barulhentas por

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

natureza, razão pela qual elas representam um desafio para a esteganálise ao extrair características responsáveis por determinar se uma imagem incorporou informações. A eficácia do método proposto foi avaliada por análise histológica e utilizando a ferramenta steganoanalysis StegExpose.

Palavras-chave: stegananálise estatística, esteganografia, stegoimage, imagem em mosaico, transformações de cores reversíveis.

Fecha Recepción: Junio 2017 **Fecha Aceptación:** Diciembre 2017

Introducción

Con el fin de enviar mensajes secretos de distinta naturaleza, que son entendidos exclusivamente por el receptor al que fueron dirigidos, la esteganografía ha estado presente a lo largo de la historia humana. En la actualidad uno de los grandes avances en esta rama es el uso de contenido multimedia (audio, vídeo e imágenes) para ocultar los mensajes. El empleo de imágenes se ha incrementado porque la mayor parte de la información presente en todo el mundo es digital, y se transmite electrónicamente por el Internet. Por lo tanto, es relevante tener métodos de seguridad como técnicas de cifrado o claves de acceso para proteger información sensible o confidencial. Sin embargo, al igual que los datos son susceptibles de ser ocultados, también lo son de ser interceptados por personas diferentes al destinatario final. Recientemente se han propuesto distintos métodos para asegurar la transmisión de imágenes: los enfoques más comunes son la criptografía y la ocultación de datos, es decir, la esteganografía.

Como se menciona por Satwinder y Varinder (2015), la criptografía utiliza las propiedades características de la imagen para convertirla en una imagen ruidosa de tal manera que no se pueda visualizar su contenido, a menos que se disponga de la clave secreta para descifrarla. No obstante, el hecho de transmitir una imagen como ruido puede llamar la atención de un atacante y evidenciar la presencia de un mensaje oculto. Por ello, otra alternativa es la aplicación de la esteganografía.

La esteganografía tiene distintas clasificaciones. En esta investigación se aplicó la esteganografía de dominio espacial, basada en textura y bordes, debido a su baja complejidad y su gran capacidad de incrustación. Como se presenta por Nusrati y Karimi (2015) y también por Fridrich, Du y Meng (2000), en este método la información secreta viaja embebida en una imagen portadora, en la cual la cadena de bits del mensaje secreto se introduce en el flujo de bits de los pixeles de la imagen portadora.

La principal complejidad de ocultar información en una imagen es la capacidad de incrustación, puesto que, al momento de ocultar una imagen dentro de otra imagen portadora, es necesario asegurarse de que ambas sean del mismo tamaño; caso contrario se debe comprimir una de las imágenes antes del proceso de incrustación. Esta compresión ocasiona distorsiones y pérdidas en la imagen original, como se menciona por Lerch-Hostalot y Megías (2014), lo cual resulta perjudicial para imágenes con contenidos relevantes.

Muchos de los métodos esteganográficos actuales intentan mejorar el algoritmo de incrustación para lograr mayor robustez. Sin embargo, muy pocos se enfocan en las características del objeto contenedor donde se oculta la información.

Por tal motivo, este artículo propone un algoritmo que combina un método de transformación de imágenes, utilizando las características del color, y un nuevo método esteganográfico que emplea operadores diferenciales y filtros para detectar las zonas más adecuadas de la imagen para incrustar la información, con el objetivo de tener imágenes esteganográficas difícilmente detectables por herramientas de estegoanálisis.

Este nuevo método se ha planteado a partir de la forma en que trabajan los estegoanalizadores: para detectar el uso de las técnicas más complejas conocidas como LSB matching (pareo de bit menos significativo), las cuales pueden ser encontradas con detalle en Hu, Zhang, Hu, Yu y Xianfeng (2013). Los estegoanalizadores utilizan una base de datos de imágenes y entrenan clasificadores que detectan imágenes que contienen información oculta. Para ello se buscan las características de la imagen que son susceptibles a ser alteradas al incrustar información y se modelan estas características para entrenar el clasificador.

En cuanto a los clasificadores, se conoce que existen zonas que son difíciles de modelar, como lo son los bordes y las texturas. Como se presenta por Lerch-Hostalot y Megías (2014), los sistemas esteganográficos modernos centran sus investigaciones, principalmente, en métodos que

ocultan información en zonas de naturaleza ruidosa, que son difíciles de modelar para entrenar a los clasificadores.

La siguiente sección de este artículo describe brevemente la metodología usada para la creación de la imagen mosaico y la recuperación de la imagen secreta. La tercera sección, por su parte, expone detalladamente el algoritmo para encontrar las zonas adecuadas y posteriormente embeber la información relevante en dichas zonas. La cuarta presenta los resultados experimentales obtenidos con el algoritmo propuesto que fueron comparados con los resultados adquiridos con el algoritmo de Ya-Lin y Wen-Hsiang (2014). Finalmente, se presentan las conclusiones de esta investigación.

Algoritmo usado por Ya-Lin y Wen-Hsiang

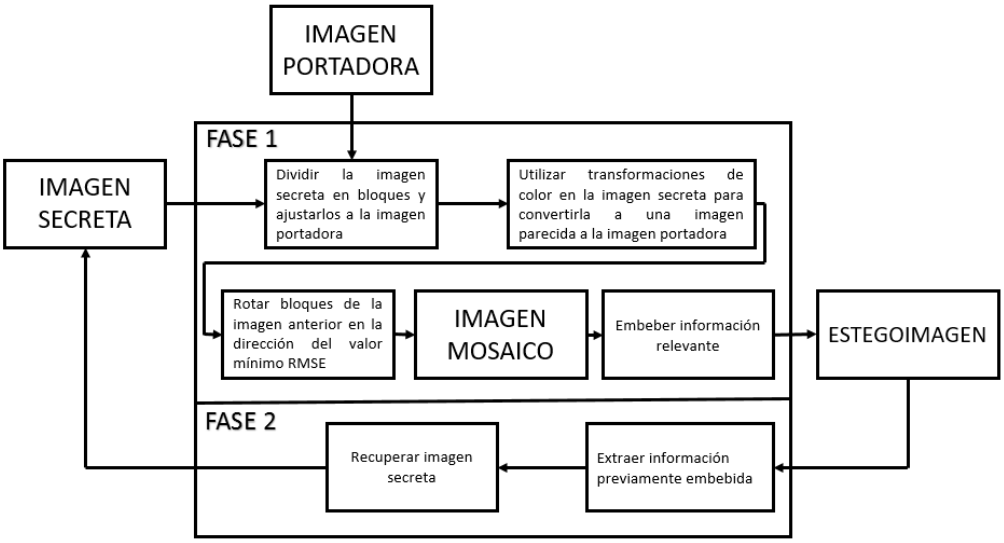
Basada la investigación en la metodología usada por Ya-Lin y Wen-Hsiang (2014), se elaboró un algoritmo que consta de dos secciones principales: la creación de una imagen mosaico y la recuperación de la imagen secreta (ver figura 1).

Al respecto, se observan cuatro elementos fundamentales:

1. Imagen secreta: imagen que se quiere ocultar.
2. Imagen portadora: imagen base para la creación del mosaico.
3. Imagen mosaico: imagen similar a la imagen portadora que contendrá a la imagen secreta.
4. Algoritmo empleado.

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Figura 1. Metodología del algoritmo empleado



Fuente: Elaboración propia

La primera fase del proceso tiene como objetivo obtener una imagen mosaico que luzca similar a la imagen portadora, gracias al uso de transformaciones reversibles de color, aplicadas a la imagen secreta. La imagen mosaico oculta información clave de las características del color (medias y desviaciones estándar) de la imagen secreta mediante métodos esteganográficos. A diferencia de la técnica original que usa el método LSB en toda la imagen mosaico, se utilizó una nueva técnica que busca las zonas más ruidosas (texturas y bordes) de la imagen para el proceso de incrustación. Este método usa filtros y operadores diferenciales con el propósito de obtener una imagen mosaico estadísticamente más imperceptible ante estegoanalizadores.

Una vez que la estegoimagen fue transmitida, se aplicó el procedimiento de la segunda fase del algoritmo, el cual consiste en la recuperación de la imagen secreta. Se realizó el proceso inverso de la primera fase utilizando nuevamente transformaciones reversibles de color y parámetros como medias y desviaciones estándar ocultas en la imagen mosaico. El proceso fue realizado en imágenes a color, por lo que todos los procedimientos aplicados se realizan en cada una de las tres matrices de color RGB (rojo, verde y azul).

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

El proceso de obtención de la imagen mosaico y la recuperación de la imagen secreta se desarrollaron mediante el método propuesto por Ya-Lin y Wen-Hsiang (2014), como ya se mencionó, el cual se describirá brevemente más adelante, mientras que la nueva técnica utilizada se expondrá con gran detalle en la tercera sección de este trabajo.

Creación de la imagen mosaico

En primer lugar, se verifica que la imagen portadora denotada como *P* y la imagen secreta *S* tengan el mismo tamaño. En el caso de no ser así, se debe establecer un tamaño común. Para este trabajo se utilizaron imágenes de 640 x 480 pixeles, debido a que son cantidades con capacidad de divisibilidad para cuatro, cinco y ocho pixeles (tamaños de bloque de imagen usados en la creación de la imagen mosaico).

Como segundo paso, *P* y *S* se dividieron en bloques del mismo tamaño. Al utilizar bloques de 8 x 8 pixeles se obtuvieron mejores resultados, tanto en relación con el valor RMSE (error cuadrático medio) como a la cantidad de pixeles a ocultar y el tiempo de ejecución, todo ello expuesto en la sección de resultados.

El objetivo de dividir la imagen secreta en bloques es tener una correspondencia con los fragmentos de la imagen portadora para hacer que sus distribuciones del color luzcan similares. Evidentemente las características de color entre ambas imágenes son diferentes, por lo que es necesario realizar con anterioridad transformaciones reversibles de color. Para ello, se requiere del cálculo de la media y desviación estándar por bloque en cada canal RGB, utilizando las siguientes ecuaciones presentadas por Ya-Lin y Wen-Hsiang (2014):

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i \quad , \quad \mu_c{}' = \frac{1}{n}\sum_{i=1}^{n} c_i{}' \tag{1}$$

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu_c)^2} \quad , \quad \sigma_c{}' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i{}' - \mu_c{}')^2} \tag{2}$$

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Donde μ_c y μ_c' denotan la media y σ_c y σ_c' la desviación estándar de la imagen secreta y la imagen portadora, respectivamente; c corresponde a los valores de pixel del bloque en cada canal (RGB) y n es el número total de pixeles en cada bloque. Después se obtiene el nuevo valor de color de cada pixel c_i'' con la siguiente ecuación:

$$c_i'' = q_c(c_i - \mu_c) + \mu_c' \tag{3}$$

Además $q_c = \sigma_c'/\sigma_c$ corresponde al coeficiente de desviación estándar. Luego se puede obtener fácilmente el color original del pixel mediante la inversa de la ecuación (3).

$$c_i = \left(\frac{1}{q_c}\right)(c_i'' - \mu_c') + \mu_c' \tag{4}$$

Con la ecuación (4) se pueden recuperar los valores originales de la imagen secreta, siendo necesario incrustar previamente en la imagen mosaico la información relevante expuesta en la sección siguiente.

Asimismo, para ajustar de mejor manera los bloques de la imagen secreta, tras la transformación de las características de color, se rotan los bloques en cuatro direcciones: 0º, 90º, 180º y 270º. De esta forma, se obtienen nuevos bloques rotados al ángulo óptimo, para así tener el menor valor RMSE con respecto al bloque de la imagen portadora, tal como se puede apreciar en la figura 2.

Figura 2. Imagen tras aplicarse las transformaciones reversibles de color en la imagen secreta (a) e imagen tras aplicarse la rotación de bloques también llamada imagen mosaico (b)

(a) (b)

Fuente: Elaboración propia

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Tras finalizar la creación de la imagen mosaico, se aplica la nueva técnica, que consiste en la detección de zonas ruidosas (texturas y bordes) de la imagen e incrustación de la información relevante en las mismas, todo ello expuesto en la sección siguiente.

Como resultado de ambos procesos, se obtiene la imagen mosaico con la información oculta denominada *estegoimagen*, la cual posee un flujo de bits que contienen el número de iteraciones, número de pixeles utilizados para el proceso de incrustación y el mapa de bordes y texturas. Este flujo de bits se usa como una clave *K* para mejorar la seguridad del algoritmo. La estegoimagen puede ser observada en la figura 3 .

Figura 3. Resultado obtenido por el método propuesto. Imagen secreta (a), imagen portadora (b), imagen mosaico creada a partir de (a) y (b) mediante el método propuesto (c) y estegoimagen con información embebida (d)

(a) (b) (c) (d)

Fuente: Elaboración propia

Recuperación de la imagen secreta

El receptor debe contar con la clave *K*, formada en el apartado anterior, para recuperar la imagen secreta. Mediante la misma, se puede obtener la información secreta a través del proceso de extracción de bits. Una vez identificados los pixeles alterados por medio del mapa de bordes y texturas, se aplica el algoritmo inverso de la incrustación de la información. Esta aplicación se

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

realiza únicamente en las áreas especificadas, para así obtener el mensaje oculto y la imagen mosaico, tal como se observa en la figura 4 .

Figura 4. Resultado de la recuperación de imágenes. Imagen mosaico recuperada por el método de extracción de bits (a) e imagen secreta recuperada (b)

(a) (b)

Fuente: Elaboración propia

El mensaje oculto presenta los suficientes datos para recuperar la imagen secreta a través del siguiente proceso inverso:

1. Rotar los bloques en la dirección inversa del ángulo óptimo para obtener el bloque original.
2. Aplicar la ecuación (4), usando las medias y los coeficientes para obtener el valor de pixel original.
3. Ordenar los bloques de acuerdo con las posiciones iniciales y así recuperar la imagen secreta.

Algoritmo esteganográfico propuesto

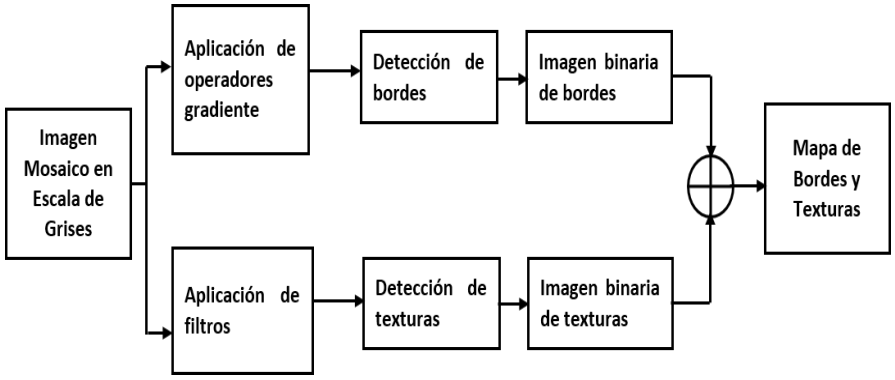
Una vez que la imagen mosaico fue creada, se aplica el algoritmo esteganográfico propuesto, el cual consta de dos etapas: *a)* detección de zonas adecuadas y *b)* incrustación de la información relevante.

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Detección de zonas adecuadas para la creación del mapa de bordes y texturas

Estudios anteriores han planteado técnicas con las que se establece un umbral y se trabaja con pares de pixeles, en los cuales, si la diferencia es mayor o igual al umbral, se consideran como bordes y texturas de la imagen, tal y como lo menciona Lerch-Hostalot y Megías (2014). Sin embargo, para esta investigación se utilizaron operadores diferenciales y filtros que consideran más pixeles vecinos para detectar variaciones significativas en los valores de pixeles (ver figura 5). Además, la imagen mosaico RGB se debe convertir a una imagen a escala de grises, para luego aplicar los algoritmos de detección de bordes y texturas.

Figura 5. Diagrama de bloques de algoritmo de búsqueda de zonas adecuadas para la incrustación de información



Fuente: Elaboración propia

Para la detección de bordes existen diferentes métodos basados en operadores gradiente, como el de Sobel, Prewitt, Roberts y el detector Canny, que son expuestos detalladamente en Moreira, Vladimir y Chávez (2009).

En el algoritmo propuesto, se utilizó el operador Canny debido a que arrojó mejores resultados. Este operador, a diferencia de los otros métodos, consta de dos etapas principales: la primera utiliza el filtro gaussiano para reducir el ruido en la imagen (texturas y detalles no significativos), y la segunda usa operadores diferenciales para detectar los bordes en todas las direcciones (horizontal, vertical y diagonal).

Reci
Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

El resultado de la aplicación del operador Canny es una imagen en binario, donde se representan las zonas consideradas bordes en la imagen con el valor de uno y las zonas uniformes con valor de cero, como se muestra en la figura 6.

Figura 6. Métodos de detección de bordes: Canny (a), Sobel (b), Prewitt (c) y Roberts (d)

(a) (b) (c) (d)

Fuente: Elaboración propia

Por otro lado, para la detección de texturas se aplicaron filtros en un pixel y en un grupo de pixeles aledaños, en donde se determinan ciertas características para detectar texturas en la imagen. Las características más comunes que se encuentran en una imagen son la entropía de la distribución de niveles de grises, la desviación estándar (distribución de niveles de grises en una región) y el rango de valores (máximos y mínimos). Al respecto, se puede observar el resultado de la aplicación de los diferentes filtros a la imagen mosaico en escala de grises en la figura 7.

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Figura 7. Filtros para detección de texturas: entropía (a), desviación estándar (b) y rango de valores (c)

(a) (b) (c)

Fuente: Elaboración propia

El algoritmo propuesto requiere de una gran capacidad de incrustación, y se eligió el filtro entropía, por su cantidad de niveles de grises y la frecuencia de cada nivel. Las zonas con menor entropía representan las texturas en la imagen.

Al aplicar dicho filtro a la imagen mosaico, se obtiene una salida con el valor de entropía de una matriz 9 x 9 de pixeles vecinos alrededor del pixel seleccionado en la imagen original, como se menciona por Benet (2016). Esta salida se convierte a binario para tener un mapa de los pixeles que pueden ser utilizados en el proceso de incrustación de información. De esta forma, la imagen binaria contiene unos, que representan las texturas de la imagen, y ceros, que son zonas uniformes de la misma.

Luego de obtener dos imágenes binarias con los bordes y texturas de la imagen mosaico, se realizó una operación de suma de ambas imágenes. De esta forma se obtuvo el mapa de bordes y texturas para la incrustación de información relevante (ver figura 8).

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Figura 8. Mapa de bordes y texturas formadas de las figura 6 (a) + figura 7 (a)

Fuente: Elaboración propia

Incrustación de información relevante

La información que se oculta en el mosaico es mostrada en los ítems siguientes:

1. Los índices de las posiciones originales de la imagen portadora.
2. El ángulo de rotación de los bloques de la imagen mosaico.
3. Las medias y el coeficiente de desviaciones estándar de cada bloque dentro del rango establecido.
4. Los residuos de desbordamiento y subdesbordamiento.

Se debe establecer un número de bits fijo para cada ítem a ocultar, por ejemplo, se usaron dos bits para el ángulo, ya que el mismo posee cuatro diferentes direcciones posibles de rotación. Los ítems de todos los bloques se deben concatenar formando un solo flujo de bits *M* para los canales RGB; es decir, se forman tres flujos que se ocultarán independientemente en la matriz del canal correspondiente. La gran cantidad de bits a ocultar hace necesario realizar varias iteraciones en el proceso de incrustación. Esto ocurre debido a que el número de bits disponibles en el mapa de texturas y bordes es menor al flujo de bits que se deben ocultar.

Se requiere también crear otro flujo de bits, *I*, con los siguientes datos: número de iteraciones requeridas por canal, número de pixeles usados en la última iteración por canal y la tabla Huffman utilizada para la codificación de los residuos. Además, se necesita ocultar el mapa de texturas y bordes en otro flujo de bits llamado *M'*, para conocer las zonas donde se ocultó información. Los flujos *I* y *M'* se ocultan en el canal R y en el canal G, respectivamente, obteniendo finalmente una estegoimagen a transmitir, mostrada en la figura 3 (d).

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Se aplicó una técnica en las parejas de pixeles indicadas con los unos en el mapa de bordes y texturas obtenido anteriormente. Para ello se requiere el uso de dos fórmulas fundamentales, donde *e* y *f* representan el par de pixeles del mosaico y *e'* y *f'* el par de pixeles transformados, como se explica en Coltuc y Chasery (2007).

$$e' = 2e - f \quad , \quad f' = 2f - e \tag{5}$$

$$e = \left[\frac{2}{3}e' + \frac{1}{3}f'\right] \quad , \quad f = \left[\frac{1}{3}e' + \frac{2}{3}f'\right] \tag{6}$$

El procedimiento para ocultar información consiste en desplazar la imagen horizontalmente o verticalmente, teniendo cada vez un par diferente de pixeles vecinos y aplicando la ecuación (5). Por otro lado, el valor original de los pixeles puede ser obtenido a partir de la ecuación (6). Este método proporciona altas capacidades de incrustación debido a que permite tener varias iteraciones. Además, es posible recuperar el valor de los pixeles originales con la complejidad operacional más baja y extraer el mensaje oculto.

Resultados experimentales

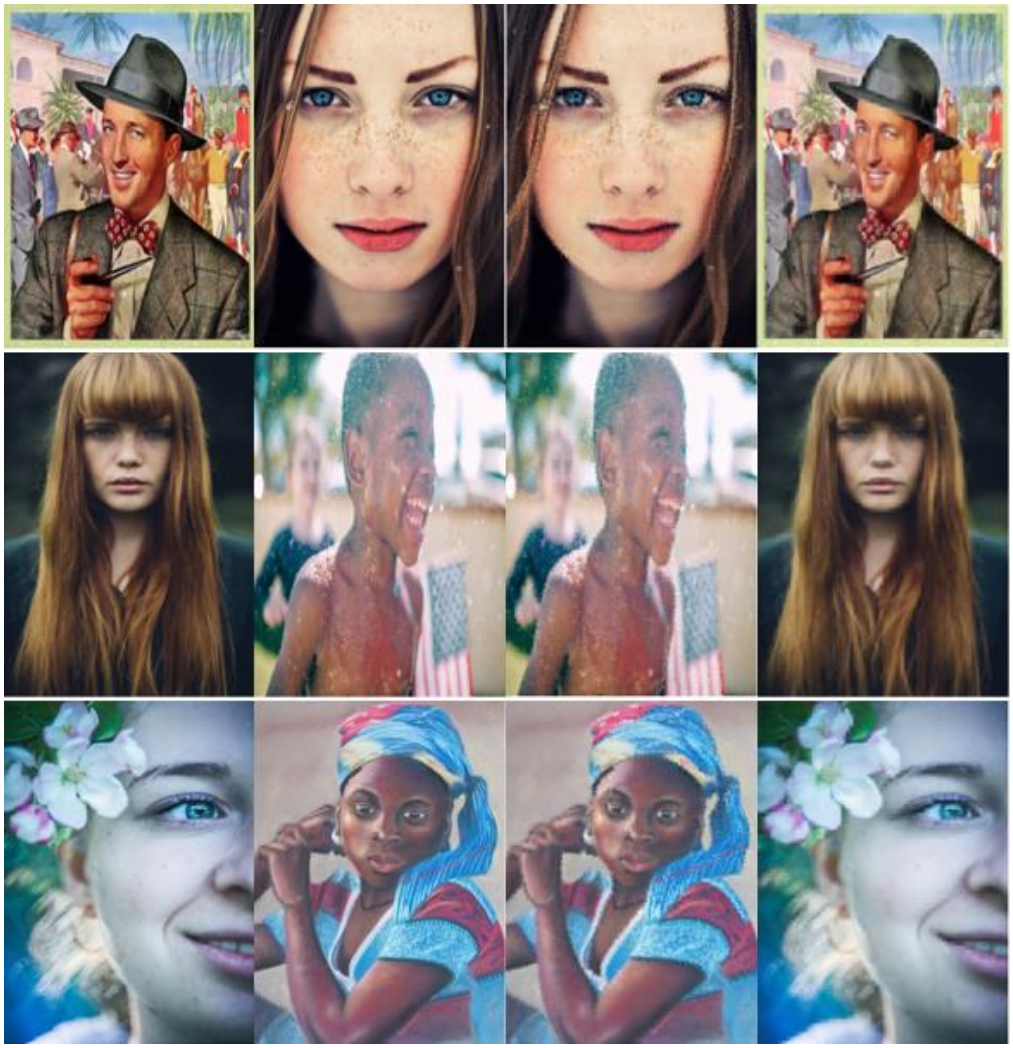
Como parte de la investigación se realizó una serie de experimentos para probar el algoritmo propuesto. Las pruebas se realizaron con imágenes extraídas de una base de datos de uso libre seleccionadas arbitrariamente y con un tamaño preestablecido de 640 x 480.

El estudio consistió en comparar las estegoimágenes creadas según el algoritmo de Ya-Lin y Wen-Hsiang y las estegoimágenes según el algoritmo propuesto. En ambos casos se compilaron los valores de los tiempos de ejecución del algoritmo y el número de bits embebidos. Finalmente, se obtuvieron las mediciones de nivel de ruido en imágenes PSNR (relación señal a ruido de pico), del valor RMSE y los histogramas de las imágenes portadoras y de las estegoimágenes obtenidos con ambos algoritmos.

Algunas de las estegoimágenes creadas usando el método propuesto se pueden observar en la figura 9, es específico en la columna (c).

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Figura 9. Resultados obtenidos por el método propuesto. Columna con imágenes secretas (a), columna con imágenes portadoras (b), columna con estegoimágenes con información embebida (c) y columna con imágenes secretas recuperadas (d)



(a) (b) (c) (d)

Fuente: Elaboración propia

Reci
Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Selección del tamaño de bloque

Asimismo, se realizaron pruebas con distintos tamaños de bloques. Los resultados obtenidos indican que el valor RMSE con los tamaños de bloques de pixeles de 16 x 16 y 32 x 32, si bien tienen un bajo tiempo de ejecución, presentan un valor alto RMSE, es decir, una baja calidad de la imagen con distorsiones notorias, como bien se puede observar en la figura 10. En el caso de las imágenes con tamaño 5 x 5, se observa un valor RMSE alto debido a las distorsiones ocasionados por la gran cantidad de información embebida y además un tiempo de ejecución alto en comparación a las pruebas con otros tamaños de bloques.

Figura 10. Estegoimágenes obtenidas con dimensiones de pixeles de 5 x 5 (a), 8 x 8 (b), 10 x 10 (c), 16 x 16 (d) y 32 x 32 (e)

(a) (b) (c) (d) (e)

Fuente: Elaboración propia

Los mejores resultados se obtuvieron con las imágenes de tamaños de bloque 8 x 8 y 10 x 10. Sin embargo, se seleccionó la primera debido a que presentó menores valores RMSE como se expone en la Tabla 1.

Reci
Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Tabla 1. Comparación de parámetros de imágenes para diferentes tamaños de bloque

Tamaño de bloque					
Parámetros de medición	**5 x 5**	**8 x 8**	**10 x 10**	**16 x 16**	**32 x 32**
RMSE de estegoimagen obtenida	27 709	13 487	14 014	18 676	28 981
Bits incrustados	1 455 506	575 596	376 311	186 640	144 033
Tiempo de ejecución (min)	6819	2644	1824	1061	875

Fuente: Elaboración propia

Comparación de parámetros de medición

Se realizaron 200 experimentos, es decir, se crearon 200 estegoimágenes, una centena según el algoritmo de Ya-Lin y Wen-Hsiang y la otra según el algoritmo propuesto. En cada experimento se obtuvieron tres parámetros de medición: tiempo de ejecución, PSNR y valor RMSE.

Para el caso de tiempo de ejecución, se utilizaron tres variables: *T1* (tiempo de creación de la imagen mosaico), *T2* (tiempo de recuperación de imagen secreta) y *T3* (tiempo total). La figura 11 expone el resultado de la comparación de tiempo de ejecución entre ambos métodos.

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Figura 11. Tiempo de ejecución promedio entre algoritmo propuesto y el algoritmo de Ya-Lin y Wen-Hsiang

Fuente: Elaboración propia

Se puede notar que el tiempo de ejecución total promedio del algoritmo propuesto es mayor, con dos minutos más aproximadamente (7432 min y 5369 min); esto se debe principalmente a que el método propuesto necesita un mayor número de iteraciones para incrustar información.

Por otro lado, se usó el cálculo del valor PSNR, el cual es una forma de medir la cantidad de ruido en una imagen con respecto a otra imagen de referencia. Para ello se midió el ruido de la estegoimagen con respecto a la imagen portadora y el ruido de la imagen secreta con respecto a la imagen recuperada. La figura 12 indica los valores promedio obtenidos en las mediciones realizadas, donde un valor más alto indica una mejor calidad de imagen.

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Figura 12. Tiempo de ejecución promedio entre el algoritmo propuesto y el algoritmo de Ya-Lin y Wen-Hsiang

Fuente: Elaboración propia

Al comparar las tres mediciones promedio PSNR, se evidencia que la imagen secreta recuperada, en ambos algoritmos, tiene el mayor valor promedio, lo que significa una mejor calidad en la imagen. Sin embargo, se obtuvo un valor mayor en las estegoimágenes creadas con el algoritmo de Ya-Lin y Wen-Hsiang debido a que el ruido es directamente proporcional al número de iteraciones.

Con respecto al valor RMSE promedio, como medida de calidad de la imagen, se realizaron las siguientes mediciones: el error RMSE entre la imagen portadora y la estegoimagen y el error RMSE entre la imagen secreta y la imagen secreta recuperada. En la tabla 2 se presentan los valores RMSE de las cuatro mediciones, tomando en cuenta que el error RMSE entre la imagen secreta y la imagen secreta recuperada tiene el mismo valor usando ambos algoritmos.

Reci
Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Tabla 2. Comparación de error RMSE

	RMSE de imagen portadora		**RMSE de imagen secreta**
Algoritmo	Propuesto	Ya-Lin y Wen-Hsiang	Ambos algoritmos
Promedio RMSE	29 342	21 647	16 625

Fuente: Elaboración propia

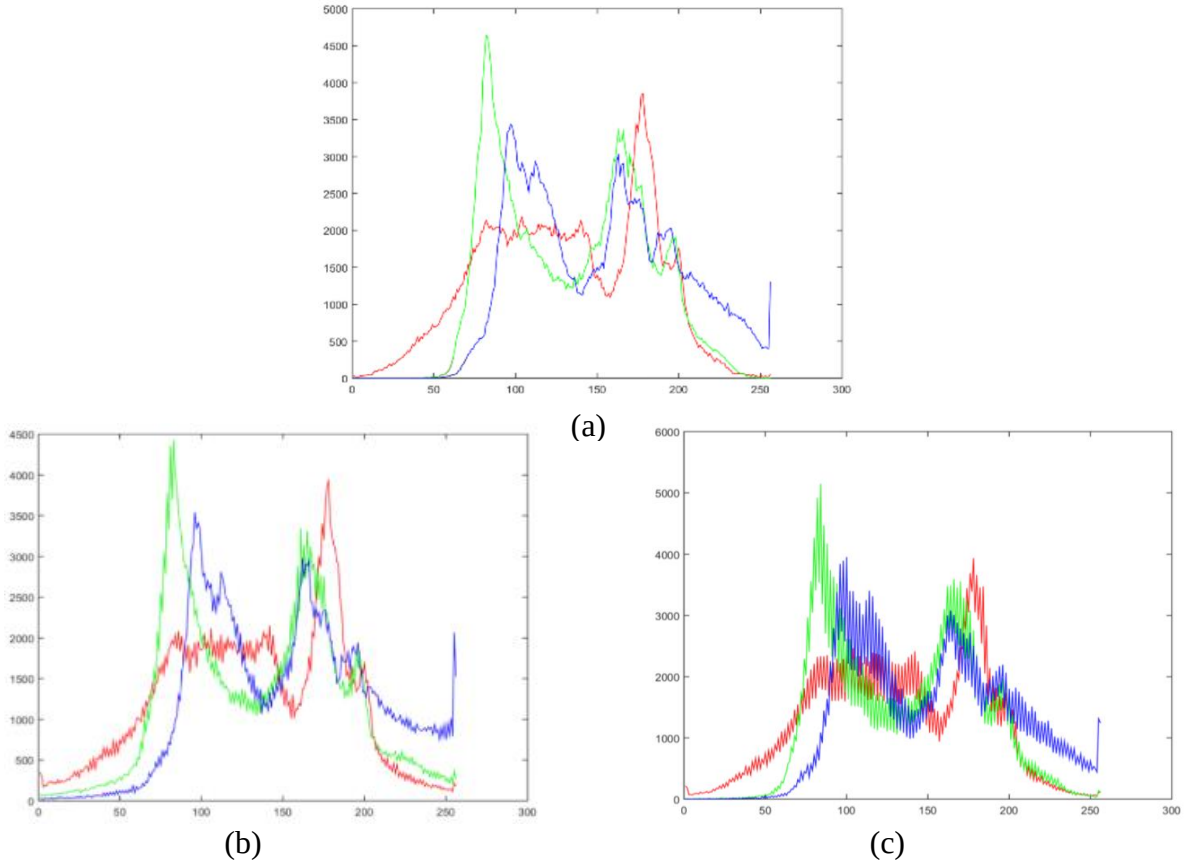
Las mediciones promedio presentadas en la tabla anterior muestran que el error RMSE entre la estegoimagen y la imagen portadora fueron mayores con el algoritmo propuesto, en comparación al algoritmo de Ya-Lin y Wen-Hsiang. Esto ocurre debido a que para el segundo algoritmo existe una distribución de bits embebidos en toda la imagen; mientras que en el método propuesto se incrusta una mayor cantidad de bits en determinadas zonas de la imagen. Por otro lado, el error RMSE promedio de la imagen secreta con respecto a la imagen secreta recuperada tiene en ambos algoritmos un valor menor al de los anteriores casos.

Indetectabilidad ante ataques estadísticos

Con el objetivo de evaluar la calidad de la imagen, se expusieron las medidas de las degradaciones en la estegoimagen con respecto a la imagen portadora original, calculando errores percibidos y cambios en la información estructural referente a la percepción visual de la imagen. Sin embargo, el objetivo principal de la investigación es evaluar la indetectabilidad de imágenes ante ataques estadísticos, los más comunes cuando se analiza una gran cantidad de imágenes. Para ello, se realizó un análisis de algunos histogramas obtenidos, los cuales se pueden observar en la figura 13.

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Figura 13. Resultado de un histograma obtenido. Imagen portadora (a), estegoimagen con algoritmo propuesto (b) y estegoimagen con algoritmo de Ya-Lin y Wen-Hsiang



(a)

(b)

(c)

Fuente: Elaboración propia

Se evidencia que los histogramas de las estegoimágenes obtenidos con el algoritmo propuesto (figura 13 [b]) tienen mayor similitud a los histogramas de la imagen portadora original mostrados (figura 13 [a]). Esto ocurre debido a que el algoritmo propuesto tiene una distribución de valores de pixeles más uniforme, puesto que tiene bits embebidos únicamente en las zonas adecuadas de la imagen. Mientras tanto, en los histogramas de las estegoimágenes con el algoritmo de Ya-Lin y Wen-Hsiang (figura 13 [c]) se pueden notar mayores variaciones en la distribución de pixeles. Esto ocasiona irregularidades estadísticas que tienen mayor probabilidad de ser detectadas con estegoanálisis estadístico.

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Asimismo, se utilizó la herramienta Steg-Expose de uso libre. Esta herramienta permite identificar imágenes que tengan información oculta. Los resultados se pueden observar en la figura 14.

Figura 14. Resultado del estegoanálisis por medio de la herramienta StegExpose utilizando ambos algoritmos: algoritmo propuesto y algoritmo de Ya-Lin y Wen-Hsiang

Fuente: Elaboración propia

En la figura 14, se expone que un 84 % de las 100 estegoimágenes obtenidas con el algoritmo propuesto no fueron detectadas mediante la herramienta StegExpose. Mientras que para las estegoimágenes obtenidas con el método de Ya-Lin y Wen-Hsiang únicamente un 3 % no fueron detectadas. Finalmente, estos resultados indican que el método propuesto es estadísticamente más robusto ante ataques de estegoanalizadores.

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Conclusiones

Se ha propuesto un nuevo algoritmo de transmisión segura de imágenes, en el cual se crearon estegoimágenes usadas como camuflaje para transmitir imágenes secretas. Para ello, no solo se utilizaron transformaciones reversibles de color, sino que también se emplearon operadores diferenciales y filtros para seleccionar las zonas más adecuadas para ocultar la información relevante. Además, las imágenes secretas originales pueden ser recuperadas casi sin pérdidas de las estegoimágenes creadas. Asimismo, al embeber la información relevante en las zonas más adecuadas (texturas y bordes), se demostró que las estegoimágenes son más difíciles de detectar por herramientas de estegoanálisis como StegExpose. Los resultados experimentales son satisfactorios y han demostrado la viabilidad del algoritmo propuesto. Futuros estudios pudiesen estar dirigidos a la aplicación de este nuevo método en diferentes ámbitos, como el videográfico, donde las estegoimágenes se encuentren ocultas en ciertos fotogramas del video.

Reconocimientos

La presente investigación se realizó con el apoyo de la Universidad de las Fuerzas Armadas ESPE. Un reconocimiento especial a la ingeniera electrónica en telecomunicaciones Gabriela Estefanía Onofre Concha y al profesor Julio César Larco Bravo por su colaboración en la investigación y redacción del artículo.

Referencias

Benet, M. (2016). *Análisis de texturas de imágenes de resonancia magnética de tumores cerebrales para la caracterización y clasificación de distintas regiones de interés.* (trabajo de fin de grado). Ingeniería Biomédica. Escuela Técnica Superior Ingenieros Industriales Valencia. Universidad Politécnica de Valencia. Valencia, España. Recuperado de https://riunet.upv.es/bitstream/handle/10251/67519/35593872_TFG_146773757656651 80638801430301192.pdf?sequence=2&isAllowed=y.

Coltuc, D. and Chasery, J. M. (2007). Very Fast Watermarking by Reversible Contrast Mapping. *IEEE Signal Processing Letters, 14*(4), 255-258.

Fridrich, J., Du, R. and Meng, L. (2000). Steganalysis of LSB Encoding in Color Images. *Proceedings IEEE International Conference on Multimedia and Expo.* New York City.

Hu, X., Zhang, W., Hu, X., Yu, N. and Xianfeng, Z. (2013). Fast Estimation of Optimal Marked-Signal Distribution for Reversible Data Hiding. *IEEE Transactions on Information Forensics and Security*, 779-788.

Lerch-Hostalot, D. y Megías, D. (2014). Esteganografía en zonas ruidosas de la imagen. *RECSI*, 173-178.

Moreira, J., Vladimir, V. and Chávez, P. (2009). Implementación de un algoritmo para la detección y conteo de células en imágenes microscópicas. *Dspace*.

Nusrati, M. A. and Karimi, R. (2015). Steganography in Image Segments Using Genetic Algorithm. *ACCT*. Haryana.

Satwinder, S. and Varinder, K. (2015). State of the art Review on Steganographic Techniques. *International Journal of Signal Processing Image, Processing and Pattern Recognition, 8*(7), 161-170.

Ya-Lin, L. and Wen-Hsiang, T. (2014). A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations. *IEEE Transactions on circuits and systems for video technology, 24*(4), 695-703.

Revista Iberoamericana de las Ciencias Computacionales e Informática
ISSN: 2007 - 9915

Rol de Contribución	Autor(es)
Conceptualización	**Freddy Roberto Acosta Buenaño**
Metodología	**Gabriela Estefanía Onofre Concha <<igual>> Cristian Marcelo Vasco Estupiñan <<igual>>**
Software	**Gabriela Estefanía Onofre Concha <<igual>> Cristian Marcelo Vasco Estupiñan<<igual>> Freddy Roberto Acosta Buenaño <<que apoya>>**
Validación	**Cristian Marcelo Vasco Estupiñan**
Análisis Formal	**Gabriela Estefanía Onofre Concha <<igual>> Cristian Marcelo Vasco Estupiñan <<igual>>**
Investigación	**Gabriela Estefanía Onofre Concha <<igual>> Cristian Marcelo Vasco Estupiñan <<igual>>**
Recursos	**Freddy Roberto Acosta Buenaño**
Curación de datos	**Gabriela Estefanía Onofre Concha <<igual>> Cristian Marcelo Vasco Estupiñan <<igual>>**
Escritura - Preparación del borrador original	**Cristian Marcelo Vasco Estupiñan**
Escritura - Revisión y edición	**Cristian Marcelo Vasco Estupiñan <<principal>> Freddy Roberto Acosta Buenaño <<que apoya>>**
Visualización	**Cristian Marcelo Vasco Estupiñan**
Supervisión	**Freddy Roberto Acosta Buenaño**
Administración de Proyectos	**Freddy Roberto Acosta Buenaño**
Adquisición de fondos	**Cristian Marcelo Vasco Estupiñan <<principal>> Freddy Roberto Acosta Buenaño <<que apoya>> Gabriela Estefanía Onofre Concha <<que apoya>>**