Ingeniería y Ciencia
ISSN: 1794-9165
ingciencia@eafit.edu.co
Universidad EAFIT
Colombia

Renza, Diego; Ballesteros L., Dora M.; Rincón, Ramiro
Método de ocultamiento de píxeles para esteganografía de imágenes en escala de gris sobre imágenes a color
Ingeniería y Ciencia, vol. 12, núm. 23, enero-junio, 2016, pp. 145-162
Universidad EAFIT
Medellín, Colombia

Disponible en: http://www.redalyc.org/articulo.oa?id=83544436008

Ingeniería y Ciencia
ISSN:1794-9165 | ISSN-e: 2256-4314
ing. cienc., vol. 12, no. 23, pp. 145–162, enero-junio. 2016.
http://www.eafit.edu.co/ingciencia

Método de ocultamiento de píxeles para esteganografía de imágenes en escala de gris sobre imágenes a color

Diego Renza [1], Dora M. Ballesteros L. [2] y Ramiro Rincón [3]

Recepción: 08-10-2015 | Aceptación: 21-01-2016 | En línea: 01-02-2016

PACS:07.05.Pj

doi:10.17230/ingciencia.12.23.8

Resumen

El proceso de ocultar datos secretos dentro de una señal huésped se conoce como esteganografía; sus parámetros de diseño son la imperceptibilidad, la capacidad de ocultamiento y la calidad de los datos recuperados. En el caso de imágenes, uno de los métodos existentes basado en la modificación de los píxeles de la imagen huésped es el denominado Block Pixel Hiding Method (BPHM), el cual presenta una buena imperceptibilidad y alta capacidad de ocultamiento, pero no garantiza la calidad de la imagen secreta recuperada. Este artículo propone un método que mejora los resultados de BPHM basado en la selección de banda y un algoritmo de búsqueda global denominado Improved Pixel Hiding Method (IPHM). De acuerdo a las simulaciones realizadas, los resultados obtenidos con IPHM son mejores a los obtenidos con BPHM y son similares a uno de los métodos más populares en esteganografía de imágenes conocido como Quantization Index Modulation (QIM).

[1] Universidad Militar Nueva Granada, Bogotá, Colombia, diego.renza@unimilitar.edu.co.
[2] Universidad Militar Nueva Granada, Bogotá, Colombia, dora.ballesteros@unimilitar.edu.co.
[3] Universidad Militar Nueva Granada, Bogotá, Colombia, u1400932@unimilitar.edu.co.

Palabras clave: esteganografía; método de ocultamiento de pixeles por bloques; método Quantization Index Modulation; imagen digital; marca de agua invisible.

Improved Pixel Hiding Method for Steganography of Gray Images Within Color Images

Abstract

Steganography is the process of data hiding into a host signal with three main characteristics: imperceptibility, payload and quality of the recovered data. For images, one of the pixel modification methods is the BPHM (Block Pixel Hiding Method) which has good imperceptibility and payload, but it does not ensure the good quality of the recovered secret image. In this paper, we propose an improvement of the BPHM with the purpose to obtain similar results to the well-known QIM (Quantization Index Modulation) method. According to the results, the imperceptibility of the stego image and the quality of the recovered secret image were improved, and then, our results are closer to QIM results.

Key words: steganography; block pixel hiding method; quantization index modulation; digital image; invisible watermark.

1 Introducción

Transmitir información de manera segura a través de cualquier canal siempre ha sido una necesidad en las comunicaciones. En muchos casos, cuando se utilizan canales públicos, un intruso puede interceptar la información transmitida, accediendo a contenidos sensibles o manipulando la información. Una alternativa a este problema es el ocultamiento de datos (*data hiding*), con el propósito de ocultar información sensible o secreta (esteganografía) o incrustar una marca para protección de derechos de autor (*watermarking*) [1]. Aunque la esteganografía es una técnica antigua, la esteganografía digital ha tenido un gran auge con aplicaciones en nuevos escenarios como medios digitales, redes de computadores y servicios de telecomunicaciones [2]. Independiente del método esteganográfico utilizado, se deben garantizar tres condiciones, en su orden: alta imperceptibilidad vista como la no generación de sospecha de la existencia del mensaje secreto oculto, adecuada capacidad de ocultamiento que permita incrustar la información secreta, y alta calidad de la información recuperada en términos de

similitud con la información secreta original. En el caso de *watermarking*, la imperceptibilidad no es la condición principal y toma su lugar la robustez, vista como la resistencia a ataques pasivos que pretenden eliminar o deteriorar la marca incrustada para evitar que el autor puede demostrar que es el dueño de la información protegida [3]. En ambos casos, esteganografía y *watermarking*, señales multimedia como audio, texto, vídeo o imagen pueden actuar como huéspedes de la información secreta [3],[4]. Cuando este procedimiento se realiza con imágenes, la información secreta se inserta dentro de la imagen huésped, obteniendo como resultado una nueva imagen conocida como imagen stego [5].

La imagen stego puede obtenerse a partir de diferentes métodos, los cuales se pueden clasificar en dos grandes grupos: métodos en el dominio espacial [6],[7],[8],[9] y métodos basados en transformadas. El primer grupo abarca métodos que modifican directamente los valores de los píxeles en la imagen huésped en función de los valores de píxel de la imagen secreta [10],[11]. El segundo grupo incluye métodos que utilizan algún tipo de transformada con el fin de realizar el ocultamiento de la información en el dominio de la frecuencia o espacio-frecuencia [5],[12],[13].

Dentro de los métodos más comunes en el dominio del espacio se resaltan los siguientes:

i. Método LSB (Least Significant Bit). Reemplaza algunos de los bits menos significativos de un píxel de la imagen huésped con bits provenientes de la imagen secreta. La cantidad de bits a modificar en la imagen huésped depende de la imperceptibilidad y capacidad de ocultamiento deseados. A mayor cantidad de bits modificados, menor será la imperceptibilidad, pero mayor será la capacidad de ocultamiento. Convencionalmente, los esquemas basados en LSB son reversibles, es decir que la imagen recuperada es exactamente igual a la imagen secreta original [14],[5].

ii. Método BPHM (Block Pixel Hiding Method). Divide la imagen huésped en N bloques cuadrados de igual tamaño, donde N es igual al número total de píxeles de la imagen secreta. Se realiza un barrido en cada uno de los bloques de la imagen huésped (de izquierda a derecha y de arriba a abajo) hasta encontrar un píxel coincidente o similar con el valor de píxel de la imagen secreta a ocultar, el cual reemplaza el píxel

respectivo. El proceso continúa hasta alcanzar la totalidad de píxeles en la imagen secreta (y por consiguiente la totalidad de bloques en la imagen huésped). El resultado final de este proceso de sustitución genera la imagen stego y una clave que registra las posiciones de los píxeles donde se ocultó la información [7],[8].

iii. Método QIM (Quantization Index Modulation). Este método se basa en un proceso de cuantización para ocultar información binaria (0/1). Cada píxel de la imagen huésped puede ocultar un bit de la imagen secreta. Los píxeles de la imagen huésped se cuantizan de acuerdo a una regla de cuantización y a un valor de paso pre-definido (Δ). Se utiliza una regla de cuantización para ocultar un '0' y otra para ocultar un '1'. En forma general, los píxeles cuantizados pertenecerán al conjunto de datos $[0, \Delta, 2\Delta, \ldots n\Delta]$ cuando se oculta un '0' y al conjunto $[\Delta/2, 3\Delta/2, \ldots ...n\Delta/2]$ cuando se oculta un '1'. El método QIM genera mejores resultados en términos de calidad de la imagen recuperada respecto al método BPHM y mejor imperceptibilidad de la imagen stego en relación a los métodos LSB y BPHM [5],[7],[8]; sin embargo, la máxima capacidad de ocultamiento puede ser menor.

Por otro lado, entre los métodos basados en trasformadas, los más comunes son:

i. DCT (Discrete Cosine Transform). En este caso la imagen portadora se separa en sub-bandas con respecto a sus componentes de frecuencia (alta, media y baja frecuencia) obteniendo los coeficientes de la DCT. Los coeficientes cuyo valor no superen un umbral dado, determinan las ubicaciones susceptibles para la inserción de la información secreta [12],[13].

ii. DWT (Discrete Wavelet Transform). Se aplica la DWT a la imagen huésped, obteniendo cuatro sub-imágenes o sub-bandas, correspondientes a la aproximación, detalles horizontales, verticales y diagonales de la imagen original. De estas cuatro sub-bandas, la de más baja frecuencia (aproximación) es la más similar a la imagen original, mientras que las sub-bandas de alta frecuencia (detalle) sólo relacionan información de bordes, texturas, entre otros. Por esta razón, típicamente los datos

secretos se incrustan en los coeficientes de detalle de la imagen huésped para generar la menor distorsión posible en la imagen stego [15],[16].

Otras alternativas incluyen técnicas de espectro ensanchado [17], métodos estadísticos [18] o esteganografía adaptativa [19],[18].

Aunque los métodos basados en transformadas pueden tener mayor imperceptibilidad que los métodos en el dominio espacial, el costo computacional de los primeros es mayor al de los segundos, tanto para la etapa de ocultamiento, como para la etapa de recuperación. En este contexto, se propone una mejora a un método en el dominio espacial, específicamente al método BPHM, con el objetivo de aumentar la imperceptibilidad de la imagen stego y la calidad de la imagen secreta recuperada, sin desmejorar la máxima capacidad de ocultamiento del método original. Se espera con la mejora propuesta alcanzar resultados similares a los obtenidos con el método QIM en términos de imperceptibilidad y calidad, y mejorar la máxima capacidad de ocultamiento de QIM.

2 Método propuesto: IPHM

El método propuesto se basa en el método BPHM, el cual se denominará de aquí en adelante como IPHM (Improved Pixel Hiding Method). También hace parte de los métodos en el dominio espacial basados en la modificación de píxeles de la imagen huésped. Las diferencias principales entre el método propuesto, IPHM, y el método original, BPHM, son: los datos de la imagen secreta se ocultan en una única banda la cual es seleccionada de acuerdo a la similitud entre la banda de color de la imagen huésped y la imagen secreta; el proceso de búsqueda de píxel no se realiza por bloques sino en toda la banda seleccionada; no existe restricción de capacidad de ocultamiento por zonas de la imagen huésped, es decir no es homogénea la modificación de píxeles dentro de la banda seleccionada; se adiciona un criterio de reemplazo en caso de no encontrar un píxel en la banda seleccionada que sea similar al píxel de la imagen secreta.

A continuación, se explican los módulos de ocultamiento y de recuperación.

2.1 Módulo de ocultamiento

El objetivo de este módulo es el de insertar una imagen secreta en escala de gris dentro de una imagen huésped a color, obteniendo una imagen stego, la cual debe ser lo más similar posible a la imagen huésped original. Las entradas al módulo son: una imagen huésped a color de $N_1 \times M_1 \times 3$ y una imagen secreta en escala de gris de $N_2 \times M_2$.

Los pasos del módulo son (ver Figura 1):

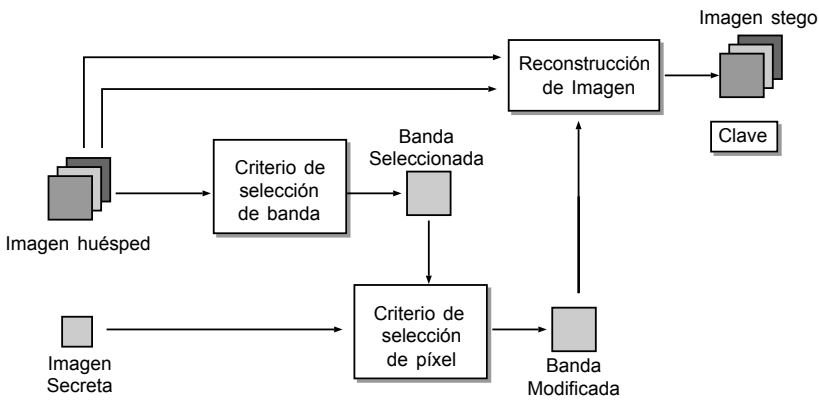


Figura 1: Módulo de ocultamiento.

a. Se inicializa la clave con tres datos: el total de filas de la imagen secreta, el total de columnas de la imagen secreta y el valor promedio de los píxeles de la imagen secreta.

b. Se separan las tres bandas de color de la imagen huésped y se selecciona la banda más idónea para la inserción de los datos secretos. La selección se basa en el criterio de correlación entre el histograma de la imagen secreta y el histograma de cada una de las bandas de la imagen huésped. El histograma de la banda que presente mayor grado de correlación (similitud) con el histograma de la imagen secreta, determinará la banda seleccionada.

c. Se incluye en la cuarta posición de la clave el número de la banda seleccionada en el paso anterior, así: 1 si la banda es la roja, 2 si es la verde y 3 si es la azul.

d. Se realiza el proceso de búsqueda de un píxel de la banda seleccionada de la imagen huésped que sea similar al píxel de la imagen secreta a ocultar. El criterio de similitud implica que no necesariamente deben ser iguales los dos píxeles, sino que se tolera cierto margen de error. Este margen de error se conoce como rango, de tal forma que el valor del píxel que se busca está comprendido entre el valor del píxel de la imagen secreta $\pm$ el valor de rango.

e. Cuando se encuentra el píxel que satisface el criterio de búsqueda, se reemplaza por el valor del píxel de la imagen secreta y se guarda en la clave la posición absoluta del píxel modificado. Por ejemplo, si se tiene una imagen huésped de 100 filas $\times$ 80 columnas y el píxel modificado se encuentra en la segunda fila, séptima columna, la posición absoluta del píxel haciendo un barrido en zigzag de izquierda a derecha y de arriba abajo es de 87 (80 posiciones de la primera fila más 7 posiciones de la segunda fila). Con el propósito de modificar solamente una vez el píxel seleccionado de la imagen huésped, esté píxel se bloquea y se omite para búsquedas futuras.

f. Si ningún píxel de la imagen huésped satisface el criterio de búsqueda, entonces se guarda en la clave el valor de 0. En el módulo de extracción se explicará qué valor se sustituye en la imagen recuperada cuando la clave tiene un 0.

g. Los pasos d-f se repiten para cada uno de los píxeles de la imagen secreta. Al finalizar el proceso de búsqueda, se tiene una banda de la imagen huésped que presenta modificaciones en algunos de sus píxeles y dos bandas que no sufrieron cambios en el proceso de ocultamiento de información. El total de posiciones de la clave es igual al total de datos de información complementaria (4 valores correspondientes a N_2, M_2, promedio, banda seleccionada) más el total de píxeles de la imagen secreta ($N_2 \times M_2$).

h. Con la banda modificada y las dos restantes sin modificar, se reconstruye la imagen a color la cual corresponde a la imagen stego. Esta imagen junto con la clave se trasmite por dos canales independientes al usuario autorizado.

2.2 Módulo de recuperación

Este módulo permite extraer la imagen secreta contenida dentro de la imagen stego por medio de la clave secreta. El módulo tiene como entradas la imagen stego de dimensiones $N_1 \times M_1 \times 3$ y la clave de $(4 + N_2 * M_2)$ elementos.

Los pasos para recuperar la imagen secreta, son:

a. Identificar la banda en la cual está contenida la imagen secreta: la imagen stego se descompone en las tres bandas de color (R, G, B) y a continuación se selecciona el número de la banda que fue almacenado en la clave. Esta información quedó registrada en la cuarta posición de la clave en el proceso de ocultamiento.

b. Con la información contenida en la clave, a partir de la quinta posición, se seleccionan los píxeles de la banda de la imagen huésped que fueron modificados y que contienen la información de la imagen secreta. Se hace un barrido en zigzag de izquierda a derecha y de arriba abajo para extraer los píxeles modificados. Este barrido se hace de la misma forma que en el módulo de ocultamiento, ya que el valor de las posiciones de los píxeles modificados corresponden a la posición absoluta dentro de la banda.

c. Si en la clave se encuentra el valor de 0, significa que el píxel de la imagen secreta no se pudo ocultar dentro de la banda seleccionada de la imagen huésped. De tal forma que, se asigna a ese píxel de la imagen secreta el promedio de los píxeles, que previamente fue almacenado en la clave en la tercera posición. Este promedio es muy similar al valor esperado de la imagen (el de mayor probabilidad de ocurrencia), pero computacionalmente de menor coste.

d. Al finalizar el proceso de extracción de píxeles, se obtiene un vector de $N_2 * M_2$ elementos. Este vector se redimensiona de acuerdo a la información contenida en las dos primeras posiciones de la clave ((número de filas y columnas de la imagen secreta).

En la Figura 2 se presenta un esquema del módulo de recuperación.

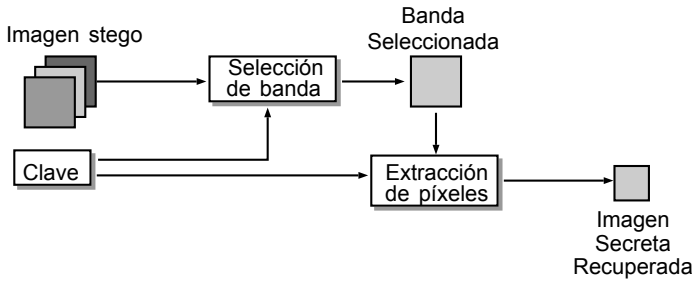


Figura 2: Módulo de recuperación.

3 Metodología y resultados

Para la validación del método propuesto se seleccionaron 10 imágenes a color (RGB) y 10 imágenes en escala de gris. Las bases de datos de imágenes fueron tomadas del sitio web `http://www.imageprocessingplace.com/`, en particular las correspondientes a las del capítulo 6 del libro Digital Image Processing, 3a edición de González y Woods [20] y las imágenes de prueba estándar, ofrecidas por esa misma web. Las imágenes a color fueron recortadas a 512×512 píxeles y las imágenes en escala de gris redimensionadas a 128×128 píxeles. La relación de píxeles de la imagen huésped versus la cantidad de píxeles de la imagen secreta es de 16:1.

El protocolo de pruebas utilizado para validar los tres métodos bajo estudio es el siguiente:

a. La primera imagen secreta se oculta en cada una de las imágenes huésped. Se calcula la imperceptibilidad de las imágenes stego generadas.

b. A partir de las imágenes stego y de las correspondientes claves, se obtienen las imágenes secretas recuperadas. Se calcula la calidad de las imágenes recuperadas.

c. Los pasos a y b se repiten para cada una de las imágenes secretas.

d. Al finalizar el paso c, se obtienen 10 imágenes stego por cada imagen secreta, es decir, en total se obtienen 100 imágenes stego por cada método.

Para los tres métodos el total de simulaciones realizadas fue de 300. BPHM e IPHM trabajaron con un rango de 20, mientras que el método QIM con un paso de 10. Con las 100 simulaciones por método, se calculan los siguientes parámetros de evaluación:

Imperceptibilidad: su objetivo es cuantificar qué tan diferente es la imagen stego de la imagen huésped y si existen zonas en las cuales la distorsión es apreciable. La similitud entre las imágenes se mide con el coeficiente de correlación normalizado (NC) y la distorsión por medio del grado de variación entre vecinos (GVD). Una buena imagen stego es aquella que tiene un alto NC (lo más cercano a 1) y un bajo GVD (lo más cercano a 0).

Para calcular el valor de GVD se utilizan las siguientes ecuaciones [9]:

$$GN\left(x,y\right)=\frac{\sum\left[S\left(x,y\right)-S'\left(x,y\right)\right]^{2}}{4} \tag{1}$$

GN es una matriz que corresponde a la diferencia en el nivel de gris entre el píxel central y sus cuatro píxeles vecinos. $S(x,y)$ es el píxel evaluado en las coordenadas (x,y) y $S'(x,y)$ son los cuatro vecinos del píxel central, entendiéndose los vecinos como el píxel derecho, el píxel izquierdo, el píxel superior y el píxel inferior.

El total de valores de GN en una imagen de tamaño $N \times M$ es de $(N-2)\times(M-2)$, dado que se excluyen del cálculo la primera y última columna, y la primera y última fila de la imagen.

Posteriormente, se calcula el promedio de diferencia en el nivel de gris, dado por la ecuación:

$$AG=\sum_{x=2}^{i-1}\sum_{y=2}^{j-1}GN\left(x,y\right) \tag{2}$$

Donde AG es un escalar.

Para obtener el nivel de distorsión global entre la imagen stego y la imagen huésped, se calcula el GVD entre ellas, por medio de la ecuación:

$$GVD=\frac{AG'-AG}{AG'+AG} \tag{3}$$

Siendo AG' el valor promedio de la imagen stego y AG el valor promedio de la imagen huésped. GVD es un escalar. Se resalta que si la imagen stego fuese exactamente igual a la imagen huésped, el valor de GVD sería de 0, y a medida que se distorsiona más la imagen stego, el valor de GVD se aleja de 0.

Calidad de la imagen secreta recuperada: en el módulo de recuperación se mide qué tan parecida es la imagen recuperada en relación a la imagen secreta original y qué tantos datos se perdieron en el proceso. La similitud se mide a través del coeficiente de correlación normalizado (NC) entre la imagen secreta original y la imagen huésped, y la cantidad de datos que se pierden en el proceso se mide a través del BER (Bit Error Rate). El BER cuantifica la cantidad de bits erróneos de la imagen recuperada. Convencionalmente se expresa como valor porcentual.

(a) Imagen Huésped (b) QIM (c) IPHM (d) BPHM

(e) Imagen Secreta (f) QIM (g) IPHM (h) BPHM

Figura 3: Ejemplo 1. (a)-(d) Imagen huésped e imágenes stego. (e)-(h) Imagen secreta e imágenes recuperadas.

3.1 Resultados preliminares

Con el fin de ilustrar el rendimiento del sistema propuesto, las Figuras 3 y 4 muestran los resultados de cada uno de los tres métodos, junto con los índices de calidad correspondientes.

En la Figura 3, el método QIM obtuvo NC=0.9994, GVD=0.3064 en la imagen stego y NC=1, BER=0 % en la imagen recuperada. Por su parte , el método IPHM obtuvo resultados similares, siendo NC=0.9991, GVD=0.0277 en la imagen stego y NC=1, BER=0.03 % para la imagen recuperada. Finalmente, el método BPHM obtuvo los siguientes resultados, para la imagen stego NC=0.9999, GVD=0.02 y para la imagen recuperada NC=0.5047, BER=31.78 %.

(a) Imagen Huésped (b) QIM (c) IPHM (d) BPHM

(e) Imagen Secreta (f) QIM (g) IPHM (h) BPHM

Figura 4: Ejemplo 2. (a)-(d) Imagen huésped e imágenes stego. (e)-(h) Imagen secreta e imágenes recuperadas.

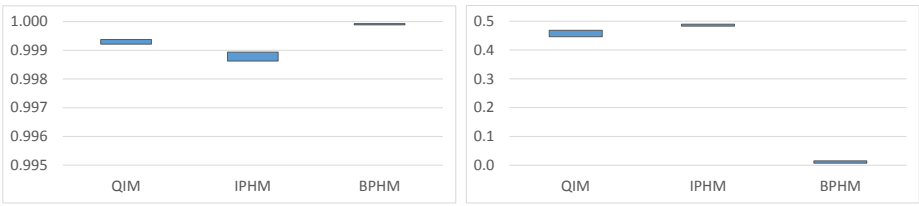
En la Figura 4 los resultados son muy similares y fueron los siguientes: QIM: Imagen Stego (NC=0.9987, GVD=0.4895) e imagen recuperada (NC=1, BER=0 %). Para IPHM, se obtuvo en la imagen stego (NC=0.9981, GVD=0.0570) y en la imagen recuperada (NC=0.9999, BER=0.13 %). En

BPHM, la imagen stego obtuvo (NC=0.9997, GVD=0.0014) y la imagen recuperada (NC=0.5998, BER=32.92 %).

De acuerdo a los resultados de las Figuras 3 y 4, se puede corroborar que los tres métodos tiene un alto valor de imperceptibilidad, pero solamente QIM e IPHM permiten recuperar la imagen secreta en gran parte o en su totalidad. Es importante tener en cuenta que el método BPHM no garantiza el ocultamiento de todos los píxeles de la imagen secreta, y por consiguiente, la imagen recuperada puede estar incompleta.

3.2 Consolidado de resultados en términos de imperceptibilidad

Para cada uno de los métodos utilizados en la fase de validación se obtienen 100 imágenes stego, las cuales se comparan contra las imágenes huésped originales, utilizando los parámetros NC y GVD. Las Figuras 5(a) y 5(b) presentan el consolidado de los resultados por medio de gráficas de rango de confianza. En estas gráficas, cada "caja" contiene el 95 % de los resultados por método.



(a) NC entre imagen huésped e imagen stego.

(b) GVD entre imagen huésped e imagen stego.

Figura 5: Consolidado de imperceptibilidad: NC y GVD.

De acuerdo a los resultados obtenidos, en los tres métodos los valores de similitud están por encima de 0,998 y la distorsión es muy baja. El método con menor distorsión es BPHM y los valores para QIM e IPHM son muy similares.

3.3 Consolidado de resultados en términos de calidad de la imagen recuperada

Para medir la calidad de la imagen recuperada se utilizaron los parámetros de NC y BER. La imagen con mejor calidad es aquella que tiene un NC alto (lo más cercano a 1) y un BER muy bajo (lo más cercano a 0 %). De nuevo, se utilizan gráficas de confianza para mostrar el rango en el que se ubican el 95 % de los resultados, para cada uno de los métodos evaluados.

La Figura 6 presenta el consolidado en términos de NC. De acuerdo a los resultados, la calidad de la imagen recuperada con el método propuesto IPHM es muy alta al igual que con el método QIM. La calidad del método BPHM es baja.

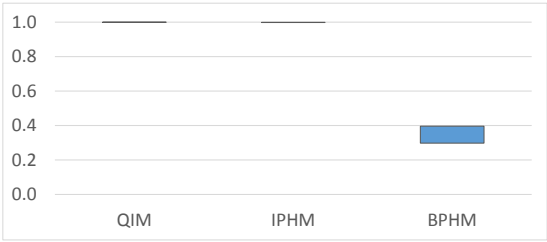


Figura 6: Consolidado de calidad: en términos de NC.

La Figura 7 presenta el consolidado en términos de BER. Tanto en los métodos QIM como en IPHM, el valor del BER es menor al 5 %, mientras que con el método BPHM se obtienen valores cercanos al 40 %.

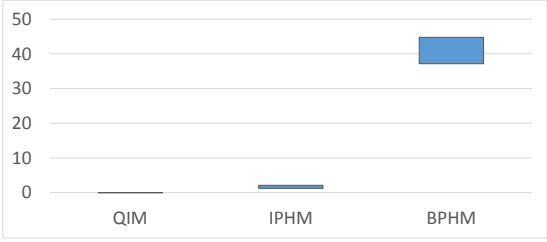


Figura 7: Consolidado de calidad: en términos de BER.

Al analizar en conjunto los resultados de imperceptibilidad y de calidad

de la imagen recuperada, se puede concluir que el método BPHM genera menor distorsión en la imagen stego debido a que es el método que oculta menor cantidad de píxeles de la imagen secreta. Es decir, el método BPHM no garantiza que toda la información secreta se oculta y por lo tanto que pueda ser recuperada por el usuario autorizado. Por otro lado, la distorsión en la imagen stego y la calidad en la imagen recuperada son muy similares entre los métodos QIM e IPHM, cumpliendo el objetivo de la presente investigación.

3.4 Ventajas de IPHM sobre QIM

De acuerdo a los resultados de imperceptibilidad y de calidad, el desempeño de los métodos QIM e IPHM es muy similar y superior al del método BPHM. En esta sección se analiza la ventaja del método IPHM sobre QIM en el tercer parámetro de evaluación de un esquema de esteganografía: la capacidad de ocultamiento.

A partir de diversas pruebas realizadas con IPHM, se encontró que la mínima relación de tamaño entre la imagen huésped y la imagen secreta es de 4:1, es decir, que por cada 4 píxeles de la banda seleccionada de la imagen huésped se puede ocultar un píxel de la imagen secreta. Con la anterior relación, suponga que se quiere ocultar una imagen secreta a color de 24-bits dentro de una imagen huésped a color de 24-bits, de tal forma que en cada banda de la imagen secreta se oculta una banda de la imagen a color (conservando la relación 4:1). De esta forma, en IPHM la capacidad de ocultamiento total es de 1 píxel de la imagen secreta por cada 4 píxeles de la imagen huésped, es decir, una capacidad de ocultamiento del 25 %. Por otro lado, en el método QIM se puede ocultar un solo bit de la imagen secreta en cada píxel de la imagen huésped, es decir, para ocultar un píxel de la imagen secreta se necesitan 8 píxeles de la imagen huésped, y por lo tanto su capacidad de ocultamiento es del 12.5 %.

Al comparar los resultados anteriores, se concluye que la máxima capacidad de ocultamiento del método IPHM es el doble de la máxima capacidad de ocultamiento del método QIM, o en otras palabras, que con el método IPHM se puede ocultar una imagen secreta del doble del tamaño de la imagen que se oculta en QIM.

4 Conclusión

En esta investigación se describe el método IPHM, el cual plantea una mejora a uno de los métodos de esteganografía de imágenes en escala de gris sobre imágenes a color, conocido como método BPHM. Las mejoras realizadas al método se basaron en las siguientes condiciones: selección de la banda que oculta la imagen secreta de acuerdo a un criterio de similitud de histogramas, búsqueda global, y criterio de reemplazo en los datos que no se pueden ocultar. Aunque el método propuesto no es completamente reversible, la cantidad de información que se pierde es menor al 5 %, lo que permite recuperar la imagen secreta con una alta similitud respecto a la imagen secreta original. En términos de imperceptibilidad, se obtienen resultados similares a los obtenidos con uno de los métodos más utilizados en esteganografía de imágenes en imágenes, el método QIM. Adicionalmente, el método propuesto, permite una mayor capacidad de ocultamiento que el método QIM, consolidándose como una solución que permite un buen balance entre los tres criterios de diseño de un esquema de esteganografía: imperceptibilidad, calidad de la información recuperada y capacidad de ocultamiento.

Agradecimiento

Esta investigación fue financiada por la Vicerrectoría de Investigaciones de la Universidad Militar Nueva Granada bajo el proyecto INV-ING-1768 de 2015.

Referencias

[1] Y. Lin and W. H. Abdulla, *Audio Watermark*. Springer, 2015. 146

[2] E. Zielińska, W. Mazurczyk, and K. Szczypiorski, "Trends in steganography," *Communications of the ACM*, vol. 57, no. 3, pp. 86–95, 2014. 146

[3] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer Science Review*, vol. 13, pp. 95–113, 2014. 147

[4] G. Shrivastava, A. Pandey, and K. Sharma, "Steganography and its technique: Technical overview," in *Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing*. Springer, 2013, pp. 615–620. 147

[5] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing*, vol. 90, no. 3, pp. 727–752, 2010. 147, 148

[6] N. N. EL-Emam, "Hiding a large amount of data with high security using steganography algorithm," *Journal of Computer Science*, vol. 3, no. 4, pp. 223–232, 2007. 147

[7] M. Juneja and P. S. Sandhu, "An improved lsb based steganography technique for rgb color images," *International Journal of Computer and Communication Engineering*, vol. 2, no. 4, pp. 513–517, 2013. 147, 148

[8] K. Moustafa and W. Badawy, "(color/gray) image in color cover hiding using modification of spatial domain hiding method," in *Future Generation Communication and Networking (FGCN 2007)*, vol. 1. IEEE, 2007, pp. 56–61. 147, 148

[9] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognition Letters*, vol. 31, no. 5, pp. 347–354, 2010. 147, 154

[10] A. Daneshkhah, H. Aghaeinia, and S. H. Seyedi, "A more secure steganography method in spatial domain," in *Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on*. IEEE, 2011, pp. 189–194. 147

[11] J. Mandal and D. Das, "Colour image steganography based on pixel value differencing in spatial domain," *International journal of information sciences and techniques*, vol. 2, no. 4, 2012. 147

[12] H. Patel and P. Dave, "Steganography technique based on dct coefficients," *International Journal of Engineering Research and Applications*, vol. 2, no. 1, pp. 713–717, 2012. 147, 148

[13] A. Abdelwahab, L. Hassaan *et al.*, "A discrete wavelet transform based technique for image data hiding," in *Radio Science Conference, 2008. NRSC 2008. National*. IEEE, 2008, pp. 1–9. 147, 148

[14] S. Bhattacharyya, "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier," *Journal of global research in computer science*, vol. 2, no. 4, 2011. 147

[15] P.-Y. Chen, H.-J. Lin *et al.*, "A dwt based approach for image steganography," *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275–290, 2006. 149

[16] V. Kumar and D. Kumar, "Performance evaluation of dwt based image steganography," in *Advance Computing Conference (IACC), 2010 IEEE 2nd International*. IEEE, 2010, pp. 223–228. 149

[17] M. M. Kiah, B. Zaidan, A. Zaidan, A. M. Ahmed, and S. H. Al-bakri, "A review of audio based steganography and digital watermarking," *Int. J. Phys. Sci*, vol. 6, no. 16, pp. 3837–3850, 2011. 149

[18] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: an overview," *International Journal of Computer Science and Security (IJCSS)*, vol. 6, no. 3, pp. 168–187, 2012. 149

[19] G. K. Selvi, L. Mariadhasan, and K. Shunmuganathan, "Steganography using edge adaptive image," in *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on*. IEEE, 2012, pp. 1023–1027. 149

[20] C. Rafael Gonzalez and R. Woods, *Digital image processing*. Prentice Hall, 2008. 153