Científica

ISSN: 1665-0654
revista@maya.esimez.ipn.mx
Instituto Politécnico Nacional
México

Velasco Bautista, Carlos L.; López Hernández, Julio C.; Nakano Miyatake, Mariko; Pérez Meana, Héctor M.

Esteganografía en una imagen digital en el dominio DCT

Científica, vol. 11, núm. 4, octubre-diciembre, 2007, pp. 169-176
Instituto Politécnico Nacional
Distrito Federal, México

Científica Vol. 11 Núm. 4 pp.169-176
 ISSN 1665-0654. Impreso en México

Esteganografía en una imagen digital en el dominio DCT

Carlos L. Velasco-Bautista
Julio C. López-Hernández
Mariko Nakano-Miyatake
Héctor M. Pérez-Meana

Sección de Estudios de Posgrado e Investigación
Escuela Superior de Ingeniería Mecánica y Eléctrica,
Unidad Culhuacán, Instituto Politécnico Nacional (IPN).
Av. Santa Ana núm. 1000,
Col. San Fco. Culhuacán,
México, DF.
MÉXICO.

correo electrónico: mariko@calmecac.esimecu.ipn.mx
lineo84@hotmail.com
julloeli@yahoo.com.mx

Recibido el 2 de agosto de 2006; aceptado el 24 de febrero de 2007.

1. Resumen

Este artículo presenta dos esquemas de ocultamiento de datos, *Entropy Thresholding* (ET) y *Selectively Embedding in Coefficients* (SEC) usando imágenes digitales. En ambos métodos el mensaje secreto se inserta en el dominio de DCT, pudiendo el mensaje oculto ser extraído perfectamente desde la stegoimagen aún después de realizar una compresión JPEG. Además de la robustez a la compresión, la distorsión causada por el ocultamiento de datos es mínima, ya que el PSNR de la stegoimagen respecto a la imagen encubridora es mayor que 45 dB. En este artículo se realiza una comparación de ambos métodos concluyéndose que el esquema SEC es superior al el esquema ET, desde el punto de vista de imperceptibilidad y máxima tasa de bits que se pueden ocultar.

Palabras clave: dominio DCT, jpeg, imagen digital.

2. Abstract (Digital Image Steganography in DCT Domain)

This paper presents two data hiding schemes, Entropy Thresholding (ET) and Selectively Embedding in Coefficients (SEC), these methods use digital images. In both methods the secret message is inserted in the DCT domain, the hidden message can be extracted with negligible distortion from stegoimage even after a JPEG compression is applied. In addition to robustness against the compression, the distortion caused by the data concealment is minimum, since the PSNR of stegoimage with respect to the cover image is greater than 45 dB. In this paper a comparison of both methods is done, concluding that SEC scheme is better than ET scheme, from the point of view of imperceptibility and maximum payload of the secrete message.

Key words: DCT domain, JPEG, digital image.

3. Introducción

La historia a través de los años ha proporcionado innumerables situaciones en las cuales la información ha tenido que atravesar un territorio hostil para alcanzar su destino, por lo cual se han usado muchos métodos ingeniosos para ocultar la información entre los que destaca la esteganografía; que es un arte antiguo que consiste en ocultar información. Las tecnologías digitales nos dan nuevas maneras para aplicar las técnicas esteganográficas, incluyendo uno de los más intrigantes que es el ocultamiento de información en imágenes digitales.

En la actualidad la comunicación por Internet se ha convertido en parte integral de la infraestructura del mundo contemporáneo. La información llega en numerosas formas y es usada en muchas aplicaciones. En la mayoría de las aplicaciones es deseable que la comunicación se realice en secreto, tal es el caso de las comunicaciones corporativas y cargos a tarjetas de crédito. Durante los últimos años los medios electrónicos han alcanzado un desarrollo importante lo que ha ocasionado un uso intensivo de los mismos, hecho que ha provocado una mayor vulnerabilidad de la seguridad de la información; ya que la mayor parte de estos medios son del uso público. Por tal motivo los mecanismos de seguridad de la información han cobrado mucha importancia encontrándose entre los más comunes la criptografía y la esteganografía. [1-3].

La esteganografía es el arte de ocultar información de tal manera que se prevenga la detección del mensaje oculto. La palabra esteganografía se deriva del griego "steganos" (encubierto) y "grafos" (escrito) lo que traducido significa

"escritura encubierta" y se refiere al arte o técnica que permite ocultar mensajes secretos en imágenes, audio o video para encubrir la información y prevenir la detección del mensaje oculto por usuarios no autorizados [4-5].

La criptografía, por su parte, es la tecnología que permite cifrar un mensaje secreto de tal forma que sea ilegible a terceras personas; mientras que la esteganografía trata de ocultar el mensaje, de tal manera que se desconozca la propia existencia de este, para evitar sospecha alguna de que datos secretos hayan sido ocultados [1]. Así la esteganografía no intenta reemplazar a la criptografía pero si complementarla ya que ocultando un mensaje utilizando la esteganografía reduce la probabilidad de que el mensaje sea detectado, sin embargo, si este mensaje también es cifrado le provee otra capa de protección.

Existen diferentes métodos que permiten ocultar información en imágenes digitales. El método LSB (*Least Significant Bit*) es quizá el más simple y sencillo de utilizar. Este, en la mayoría de los casos, proporciona una alta capacidad de inserción y una baja perceptibilidad, sin embargo, es vulnerable a ligeras modificaciones de la imagen como la compresión y a la extracción de la información por personas no autorizadas. [4,6]. Otros métodos más robustos para ocultar información en imágenes hacen uso del dominio de la transformada ya sea la DFT (*Discrete Fourier Transform*), la transformada DCT (*Discrete Cosine Transform*) o la transformada DWT (*Descrete Wavelet Transform*) para transformar una imagen en el dominio espacial al dominio espectral y así ocultar el mensaje secreto en áreas significativas de la imagen. En general, los métodos en el dominio espacial tienden a proporcionar mayor capacidad de inserción que los métodos en el dominio de la frecuencia, sin embargo los métodos en el dominio de la frecuencia son más robustos contra ataques, tales como compresión, recorte o algún otro procesamiento de imagen [4, 6, 7].

Este artículo presenta dos algoritmos esteganográficos basados en el método QIM (*Quantization Index Modulation*) propuesto por [8], los cuales usan una imagen digital como encubridora de datos y realizan la cuantización de coeficientes a través de la DCT para poder insertar el archivo secreto en los bits menos significativos de la cuantización de los coeficientes DCT. Los dos algoritmos recuperan el mensaje oculto con un mínimo de bits erróneos, aun cuando la imagen encubridora sufra la compresión JPEG con factor de calidad 50. En este artículo se presentan dos algoritmos de ocultamiento de datos, el primer método, llamado *Entropy Thresholding* (ET) es el método basado en un umbral de entropía que selecciona bloques de coeficientes de DCT que pueda ocultar el mensaje secreto, dependiendo de su entropía o energía comparando con un valor de umbral determinado anteriormente. El segundo esquema, llamado *Selectively Embedding in Coefficients* (SEC) selecciona los coeficientes individualmente dependiendo de su energía para poder insertar el mensaje en una manera imperceptible. Ambos algoritmos usan un criterio local para seleccionar conjuntos de coeficientes dentro de las bandas de baja y mediana frecuencia. Los dos algoritmos se comparan desde el punto de vista de imperceptibilidad y robustez del mensaje oculto y la capacidad máxima de bits que permiten ocultar.

4. Desarrollo

4.1 Definición de la esteganografía

El desarrollo de la informática y la Internet ha supuesto el marco perfecto para que la esteganografía tenga un mayor auge, ya que mientras los avances de la computación proporcionan los medios para calcular rápidamente los cambios necesarios en la ocultación de un mensaje, el Internet proporciona los medios necesarios para transportar grandes cantidades de información a cualquier punto del mundo.

La esteganografía actual trata de esconder datos binarios en los bits redundantes que supone un fichero. Los bits que componen el mensaje a ocultar se introducen (ya sea añadiéndolos, o realizando operaciones aritméticas con los datos originales) en el archivo ya existente, procurando que el archivo resultante después de realizar los cambios tenga un alto parecido con el original.

La esteganografía utiliza un medio digital como archivos de texto, audio, imagen y video que son utilizados como un archivo de transporte, para ocultar la información. A este medio se le conoce como contenedor o cubierta y tiene la característica de que ser un contenedor aparentemente inocente que no despierte ninguna sospecha. De igual manera el mensaje secreto o la información a ocultar puede ser cualquier medio digital descrito anteriormente. Aquí cuando el mensaje secreto es ocultado en el contenedor a través de una técnica esteganográfica se obtiene un esteganograma que contendrá el mensaje oculto en el archivo de transporte o cubierta. Este proceso se muestra en la figura 1, la cual muestra el contenedor y el mensaje secreto que puede o no hacer uso de técnicas de cifrado para darle una mayor protección a la información, seguidamente una vez que los datos han sido ocultados, la información puede ser transferida a través de medios de comunicación inseguros. Una vez en el canal, aunque ninguna persona sospechara la existencia del mensaje, éste está expuesto a cualquier ataque. Finalmente para recuperar el mensaje secreto se aplica el proceso inverso [9].

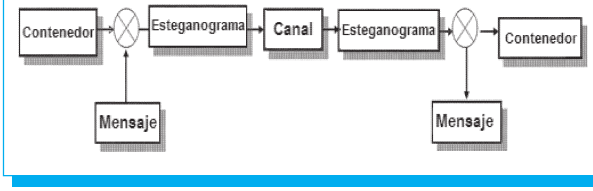

Fig. 1. Proceso esteganográfico.

En este caso particular vamos a ocupar una imagen digital como contenedora del mensaje secreto, la cual puede obtenerse de diferentes maneras entre las que destacan: el uso de una cámara digital, la captura de una trama o imagen fija de video, o la digitalización de una fotografía en formato impreso mediante el uso de un digitalizador.

Independientemente del medio de obtención de la imagen, la principal característica radica en el hecho de que la información se encuentra almacenada en formato digital, es decir codificada por medio de una secuencia determinada de bits (dígitos binarios).

Una fotografía digital es un conjunto de píxeles (*picture elements*) codificados mediante ceros y unos que forman un mapa de bits. Por tanto, como cualquier secuencia binaria, puede ser objeto de la ampliación de algoritmos de compresión con poca pérdida de calidad. Esta cualidad permite la presentación de las imágenes en páginas Web sin un tiempo excesivo de carga. Los formatos JPG y GIF son los más utilizados para fotografías digitales comprimidas.

4.2 Transformada discreta de coseno (DCT)

La transformada DCT es una transformada semejante a la transformada rápida de Fourier, ésta toma un conjunto de puntos de un dominio espacial y los transforma en una representación equivalente en el dominio de frecuencias.

La DCT está bastante relacionada con la DFT, con la diferencia de que es una transformada real, debido a que los vectores base se componen exclusivamente de funciones coseno muestreadas. Además la DCT minimiza algunos de los problemas que surgen con la aplicación de la DFT a series de datos. La transformada discreta de coseno es la más ampliamente utilizada en compresión de imágenes y videos. Esta transformada cuenta con una buena propiedad de compactación de energía, que produce coeficientes incorrelados, donde los vectores base de la DCT dependen sólo del orden seleccionado de la transformada y no de las propiedades estadísticas de los datos de entrada.

La decorrelación de coeficientes es muy importante para la compresión, ya que el posterior tratamiento de cada coeficiente se puede realizar de forma independiente, sin pérdida de eficiencia de compresión. Otro aspecto importante de la DCT es la capacidad de cuantificar los coeficientes utilizando valores de cuantificación que se eligen de forma visual. Esta transformada ha tenido una gran aceptación dentro el tratamiento digital de imágenes, debido al hecho de que para los datos de una imagen convencional tienen una alta correlación entre elementos.

La DCT unidimensional es útil en el procesamiento de señales de una dimensión, sin embargo para el análisis de una señal bidimensional (2D) como una imagen que es nuestro caso se necesita una versión bidimensional de la DCT. Así para una matriz F de nxm, la DCT 2D es calculada de una manera simple usando la versión en una dimensión de la DCT como sigue:

- Aplica DCT 1D (verticalmente) a cada columna.
- Aplica DCT 1D (horizontalmente) al resultado vertical DCT anterior.

Las siguientes ecuaciones proporcionan las definiciones matemáticas de las DCT y IDCT de un bloque de 8x8 de una imagen f, así, la transformada F está dada por:

$$F(u,v)=\frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7}f(x,y)*\cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right] \quad (1)$$

$$f(x,y)=\frac{1}{4}\left[\sum_{u=0}^{7}\sum_{v=0}^{7}C(u)C(v)\ F(u,v)*\cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right] \quad (2)$$

donde:

$$C(u),C(v)=1/\sqrt{2} \qquad \text{para } u,v=0$$

$$C(u),C(v)=1 \qquad \text{en otro caso}$$

4.3 Modificación de histograma

El histograma de una imagen contiene el número de píxeles que tienen el mismo nivel de gris, el cual proporciona información sobre el brillo y el contraste de la imagen, y puede ser utilizado para ajustar estos parámetros, eliminar ciertas tonalidades molestas, etc.

Para una imagen dada, después de insertar información en algunos coeficientes DCT (AC), es posible causar un exceso

o desbordamientos, lo cual significa que después de la IDCT los valores de la escala de grises de algunos píxeles en la imagen esteganografiada pueden exceder el límite superior (255 para una imagen en escala de grises de ocho bits) y/o el límite inferior (0 para una imagen en escala de grises de ocho bits). Para prevenir el exceso o desbordamiento, asumimos la modificación del histograma, que estrecha el histograma de ambos lados.

4.4. Método ET

El esquema de selección por umbral de entropía (ET) usa la energía de cada bloque de 8x8 para determinar si se inserta el mensaje secreto o no. Solo bloques con mayor energía que el valor de umbral determinado anteriormente son usados para ocultar el mensaje secreto. Las figuras 2 y 3 muestran el proceso de inserción y detección de mensaje secreto, respectivamente.

Proceso de inserción usando el método de ET

El proceso de inserción del mensaje secreto se muestra en los siguientes pasos.

1. Modificación de histograma.
2. La imagen es dividida en bloques de 8x8 píxeles.
3. Se aplica la DCT a cada bloque.
4. La entropía (Entropía Norma 2) de cada bloque se calcula en siguiente forma:

$$E = \sum_{i,j} ||c_{ij}||^2 \ , \forall \ i,j \in \{0,1,...,7\}, \ (i,j) \neq 0 \qquad (3)$$

donde $c_{i,j}$ es (i,j)-ésimo coeficiente de un bloque. En el cálculo de entropía no se usa el componente DC de los coeficientes.

5. Se hace una selección de bloques cuya entropía es mayor que el valor umbral Th.
6. Cada bloque seleccionado es divido usando una matriz de cuantificación M^{fc} que está dada con relación al factor de calidad de compresión.

$$\tilde{c}_{i,j} = \frac{c_{i,j}}{M^{fc}_{i,j}} \ , \forall \ i,j \quad \{0,1,...,7\} \qquad (4)$$

7. Se hace un escaneo en zig-zag a cada bloque seleccionado, obteniendo un vector de longitud 64.
8. El mensaje secreto es insertado en los primeros 8 coeficientes de ACs usando el método de plano de bit menos significativo (LSB). Aquí el signo de cada coeficiente es conservado.
9. Se reordena el vector con el mensaje oculto a una matriz de tamaño 8x8.
10. A cada bloque seleccionado se multiplica por la misma matriz de cuantificación y después se le aplica la IDCT para reconstruir la imagen, obteniendo así nuestro esteganográma.

Proceso de extracción en el método de ET

El proceso de extracción escribe en siguientes pasos:

1. El esteganográma es dividido en bloques de 8x8 píxeles.
2. Se aplica la DCT a cada bloque del esteganográma.
3. Se calcula la entropía de cada bloque para seleccionar los bloques con el mensaje oculto.
4. Cada bloque seleccionado es divido por la matriz de cuantificación M^{fc}.
5. Se hace un escaneo en zig-zag a cada bloque obteniendo un vector de longitud 64.
6. Se extrae el bit menos significativo de los primeros 8 ACs de cada bloque seleccionado.
7. Los bits obtenidos del paso anterior se unen obteniendo como resultado nuestro mensaje secreto.

4.5. Método de SEC

En el esquema de SEC, se realiza una selección de área de inserción para el mensaje de coeficiente por coeficiente para lograr una distorsión visual mínima. La figuras 4 y 5 muestran el proceso de inserción y extracción, respectivamente.

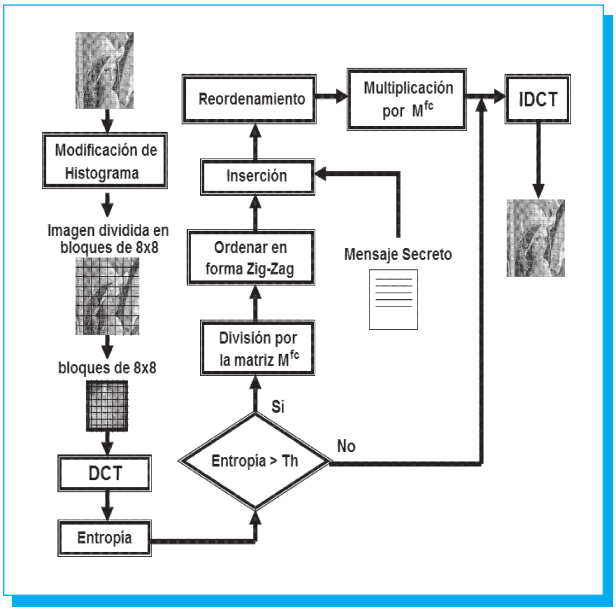

Fig. 2. Proceso de inserción método ET.

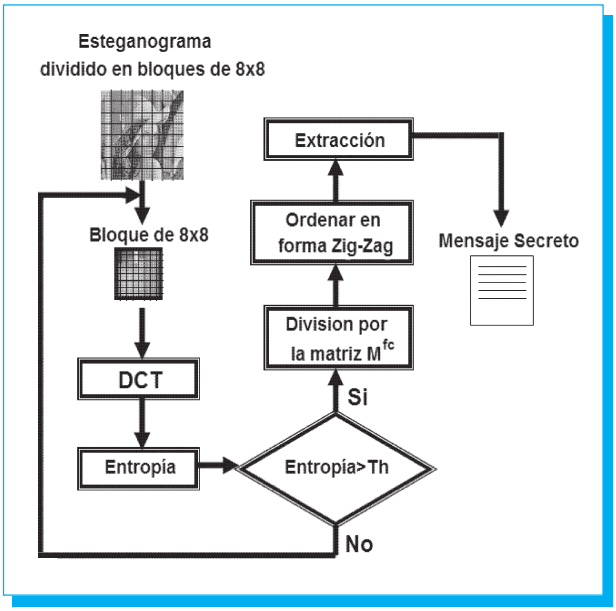

Fig. 3. Proceso de inserción método ET.

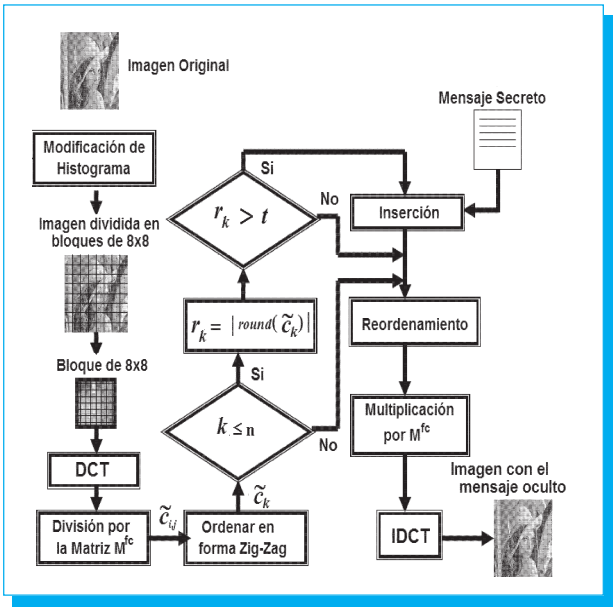

Fig. 4. Proceso de inserción método SEC.

Proceso de inserción usando el método de SEC

1. Modificación de histograma.
2. La imagen se divide en bloques de 8x8 píxeles.
3. Se aplica la DCT a todos los bloques de la imagen.
4. Los coeficientes de DCT de cada bloque es dividido por la matriz de cuantificación M^{fc}, como se muestra en (4).
5. Se hace un escaneo en zig-zag a cada bloque seleccionado, obteniendo un vector de longitud 64.
6. Se considera la banda de baja frecuencia para la inserción del mensaje secreto (*i.e.*, $1 \le k \le n$). Aquí n<<64.
7. El valor absoluto de cada coeficiente $\tilde{c}_{ij}$ es redondeado, como se muestra en (5).

$$r_k = |round(\tilde{c}_k)|,\ 1 \le k \le n \qquad (5)$$

8. Si $r_k > t$, entonces al bit menos significativo del coeficiente $\tilde{c}_k$ se le inserta un bit del mensaje secreto.
9. Se reordena el vector a una matriz de 8x8 para cada bloque.
10. A cada bloque seleccionado se multiplica por la misma matriz M^{fc} y se aplica IDCT para obtener la imagen con el mensaje oculto.

Proceso de extracción en el método de SEC

El proceso de extracción en el método de SEC se describe como:
1. El esteganograma se divide en bloques de 8x8 píxeles.
2. Se aplica la DCT a todos los bloques de la imagen.
3. Los coeficientes de DCT de cada bloque son divididos por la matriz de cuantificación M^{fc}, como se muestra en (4).

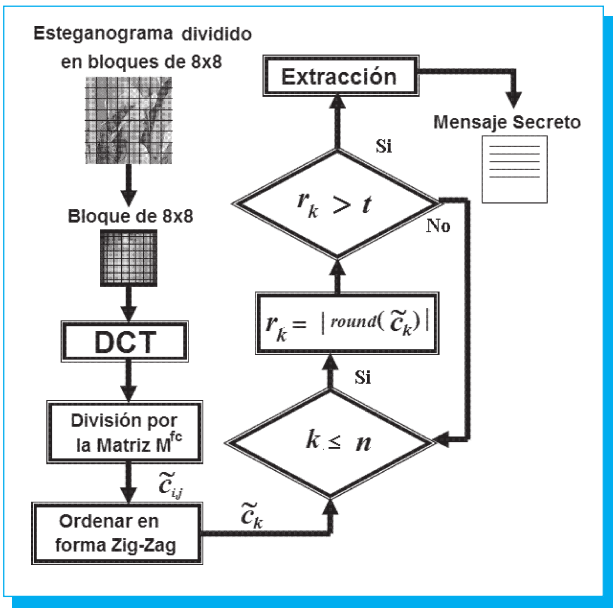

Fig. 5. Proceso de extracción método SEC.

4. Se hace un escaneo en zig-zag a cada bloque seleccionado obteniendo un vector de longitud 64.
5. Se calcula r_k aplicando la (5).
6. Si $r_k > t$ entonces se extra el bit menos significativo del r_k como bit del mensaje secreto.

5. Resultados

5.1. Criterios de evaluación

Un sistema esteganográfico tiene que generar un esteganográma suficientemente inocente, ya que no debe de levantarse ninguna sospecha. Por lo tanto el grado de distorsión o imperceptibilidad del esteganográma respecto a la imagen cubierta es un asunto muy importante. Una medida de distorsión comúnmente usada es el PSNR (relación señal a ruido pico) del esteganográma con respecto a la imagen cubierta (original), como se muestra en (6) y (7).

$$PSNR = 101 \log_{10} \frac{256^2}{MSE} \tag{6}$$

$$MSE = \frac{\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}(I_C - I_S)^2}{N_1 N_2} \tag{7}$$

Donde I_C,I_S son la imagen encubridora y el esteganográma, respectivamente, y N_1, N_2 son tamaño de ambos imágenes.

Además del asunto de imperceptibilidad, el asunto de capacidad de ocultamiento es sumamente importante. Manteniendo una distorsión pequeña posible, todos sistemas esteganográficos buscan aumentar la capacidad de ocultamiento. La capacidad de ocultamiento para un sistema esteganográfico cuando cubierta es imagen, se mide número de bits de mensaje secreto por píxel (bpp), como se muestra en (8).

$$Capacidad\_de\_Ocultamiento = \frac{Número\_de\_Bits(M_S)}{Número\_de\_Bits(I_C)} \tag{8}$$

donde M_S es el mensaje oculto.

Generalmente cuando un esteganograma se transmite por un canal ideal y no recibe ningún tipo de modificación, tal como compresión, el mensaje oculto debe de recuperarse al 100%. Sin embargo cuando el canal de transmisión no es ideal (introduce algún cantidad de ruido, por ejemplo) o recibe alguna modificación, no se puede recuperar al 100% el mensaje oculto. El error de recuperación del mensaje oculto

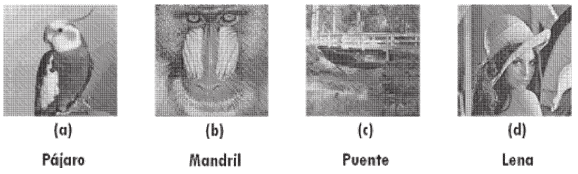

Fig. 6. Imágenes utilizadas en los criterios de evaluación.

se mide generalmente tasa de bits erróneo "Bit Error Rate" (BER) y se calcula en (9).

$$BER = \frac{Bits\_Erróneo}{Bits\_total\_transmitido} \tag{9}$$

Los tres asuntos mencionados anteriormente forman contrapartes, cuando trata de aumentar capacidad de ocultamiento, sacrificaría el grado de imperceptibilidad y robustez, mientras se trata de aumentar robustez del sistema, sacrificarían capacidad o imperceptibilidad y viceversa.

Los dos algoritmos de ocultamiento de datos se evalúan desde los diferentes puntos de vista, usando varias imágenes (Puente, Lena, Mandril, Pájaro), figura 6. La matriz de cuantificación usada para la evaluación es un matriz para factor de calidad 50, M^{50}.

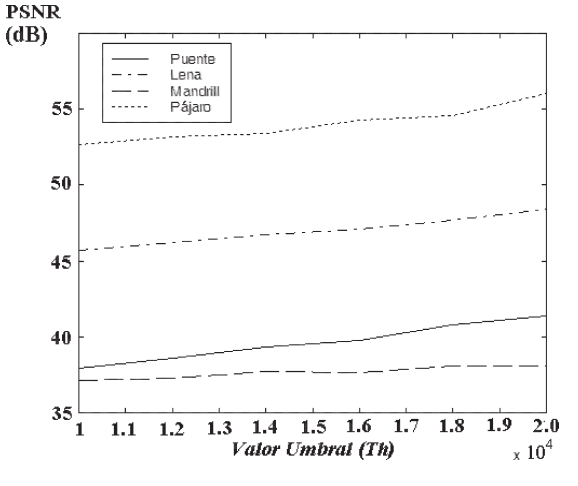

Fig. 7. Distorción del esteganograma con diferentes valores de umbral en el esquema ET.

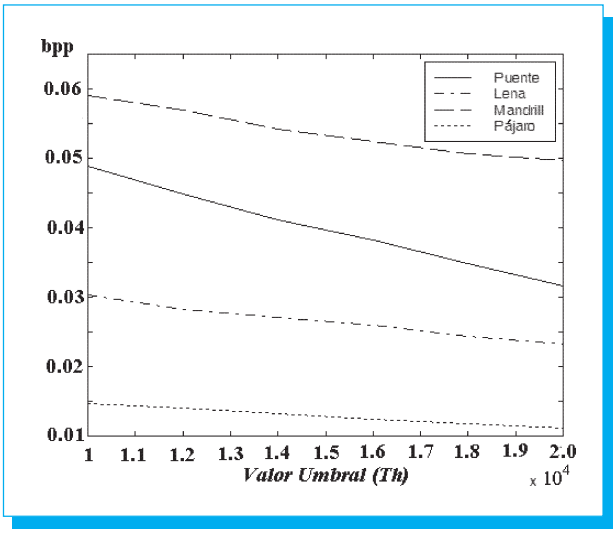

Fig. 8. Tasa de bits ocultos por pixel (bpp) con diferentes valores de umbral en el esquema ET.

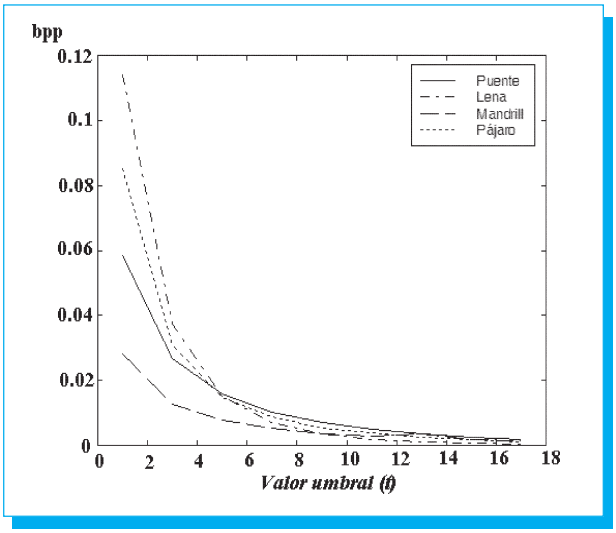

Fig. 10. Tasa de bits ocultaos poe pixel (bpp) con diferentes valores de umbral en el esquema SEC.

5.2. Valor de umbral

En ambos algoritmos, el valor de umbral es muy importante para obtener un buen funcionamiento del sistema. En el esquema ET, el valor de entropía de cada bloque de DCT se compara con el valor de umbral (Th) para determinar si el bloque es adecuado para inserción del mensaje secreto o no. En el esquema SEC, cada coeficiente de DCT, se compara con el valor umbral (t) para determinar el coeficiente es adecuado para inserción de un bit del mensaje secreto. La figura 7 muestra la relación entre el valor de umbral (Th) y PSNR del esquema ET, y la figura 8 muestra relación entre el valor del umbral (Th) y la máxima tasa de bits que pueda ocultar en cada imagen. De la misma forma la figura 9 muestra la relación entre el valor umbral (*t*) y PSNR, en

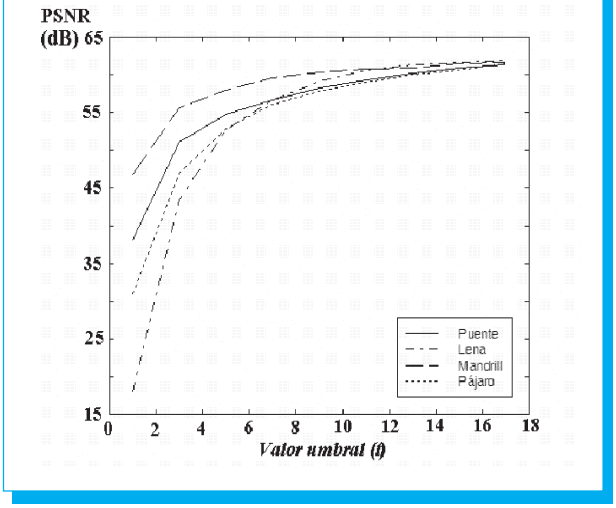

Fig. 9. Distorción del esteganograma con diferentes valores de umbral en el esquema SEC.

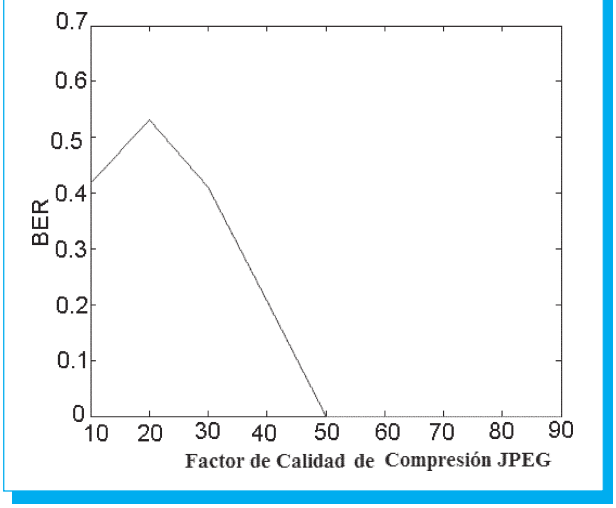

Fig. 11. Tasa de bits erróneo (BER) cuando la stegoimagen sufre compresión JPEG con diferentes factores de calidad.

Tabla. 1. Mensaje recuperado del esteganograma comprimido con diferentes factores de calidad.

Mensaje recuperado Fc ≥ 50 Tasa de compresión ≤ 12 BER=0	Mensaje recuperado Fc<50 Tasa de compresión>12 BER=0.3
1. Introducción Podemos pensar en la comunicación como un proceso mediante el cual transmitimos ideas, sentimientos o creencias a otros.	1. Introducción Podemos pensarbÁn la comunicaciÑí como un*XroceyjEMediante el cuÂî< tranîitimos ideaz {4ntimicnt>s oreenccãs a otros

la figura 10 la relación entre el valor umbral (t) y tasa de bits ocultos usando el esquema SEC.

5.3. Ataques JPGE

En ambos esquemas son robustos contra ataques de compresión JPEG, ya que la matriz de cuantificación M^{fi} está introducido en los procesos de ocultamiento de mensaje secreto, el cual garantiza una robustez contra compresión JPEG con factor de calidad *fc*. Si se usa un matriz de cuantificación M^{50}, factor de calidad *fc*=50, en el proceso de inserción y extracción, ambos esquemas son robustos contra compresión de JPEG con factor de calidad mayor o igual que 50. La figura 11 muestra la tasa de bits erróneo (BER) cuando el esteganográma sufre compresión JPEG con diferentes factores de calidad.

La tabla 1 muestra mensajes extraídas del esteganográma comprimido por JPEG con el factor de calidad mayor que 50 y menor que 50, respectivamente. De la figura 11 y la tabla 1, podemos observar que ambos esquemas se puede controlar el grado de robustez requerido, aplicando diferentes matrices de cuantificación en el proceso de inserción y detección. Considerando que una compresión JPEG con un factor de calidad 50 ocasiona una distorsión mínima que puede tolerar por sistema visual humano, ya que compresión con factor de calidad menor que 50 provoca una distorsión intolerable, la matriz de cuantificación M^{50} es una buena selección para ambos métodos.

6. Conclusiones

En este artículo, se presentaron dos esquemas de ocultamiento de datos: esquema ET y esquema SEC, los cuales insertan el mensaje secreto en el dominio de DCT de de una imagen digital. Los dos esquemas son diseñados para ser robustos contra ataques de JPEG, ya que en el proceso de inserción y extracción, se usa una matriz de cuantificación con diferentes factores de calidad, así los algoritmos garantizan robustez contra compresión hasta con el factor de calidad de la matriz de cuantificación.

De los resultados de comparación de ambos esquemas, podemos concluir que el esquema SEC ofrece un ocultamiento de datos mas transparente (PSNR= 42-55 dB, cuando *t*=3) que el esquema ET (PSNR=38-53dB con 0.03 bpp), manteniendo mismo tasa de bits ocultos (0.03 bpp).

Transparencia de mensaje oculto y tasa de bits ocultos dependen ligeramente de imágenes encubridoras, ya que imágenes con mayor detalle, tales como 'Puente' y 'Mandril' se puede ocultar mas información que imágenes planas, tales como 'Pájaro' y 'Lena', aunque distorsión numérica (PSNR) se disminuye cuando aumenta tasa de bits ocultos. En el esquema ET, las características de imagen influye más a su funcionamiento que ya la imperceptibilidad y tasa de bits ocultos varían bastante dependiendo de las imágenes encubridoras, mientras el funcionamiento del esquema SEC no varían tanto por las características de las imágenes encubridoras.

7. Referencias

[1] R. J. Anderson and A. P. Petitcolas, "On the limits of steganography", *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 474–481, May 1998.

[2] F. Petitcolas, R. Anderson, and M. Kuhn, "Information-Hiding:A Survey", *Proc. of the IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[3] D. Artz, "Digital Steganography:hiding data within dataV, *IEEE Internet Computing*, vol. 5, no. 3, pp. 75-80, 2001.

[4] F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen", *IEEE Computer Mag.*, vol. 31, no.2, pp. 26–34, 1998.

[5] Katzenbeisser S., Fabien, A.P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech Housea, 2001.

[6] R. Chandramouli and Nasier Memon, "Analysis of LSB Based Image Steganography Techniques", *Proceedings of the International Conference on Image Processing*, pp. 1019-1022, 2001.

[7] Neil F. Johnson and Sushil Jajodia, "Steganalysis: The Investigation of Hidden Information", *IEEE Conf. on Information Technology*, pp. 113-116, 1998.

[8] K. Solanki, N. Jacobsen, U. Madhow, B. Manjunath and S. Chandrasekaran, "Robust Image-Adaptive Data Hiding Using Erasure and Error Correction", *IEEE Transactions on Image Processing*, vol. 13, no. 12, pp. 1627-1639, 2004.

[9] S. Torres, M. Nakano and H. Pérez, "An Image Steganography Systems Based on BPCS and IWT", *Wseas Trans. on Communications*, vol. 5, no. 6, pp. 814-820, 2006.