Ciencias Matemáticas, Vol. 33, No. 2, Pag. 161-169, 2019
Recibido 02-2019, Aceptado 09-2019

Algoritmo esteganográfico pseudo-asimétrico basado en una tabla de cuantificación no estándar
Pseudo-asymmetric stganographic algorithm based upon a quantization table non-standard

A. Figueroa-Romero[1], A. Soria-Lorente[2]

Resumen En este artículo, se propone un novedoso método esteganográfico basado en la comprensión JPEG. El algoritmo esteganográfico propuesto inserta la información secreta en algunos coeficientes localizados en el área de las medias frecuencias de la imagen original (RGB), utilizando una nueva matriz de cuantificación distinta a la estándar. Por otro lado, el método propuesto utiliza una clave pública y otra privada, ambas de 128 bits, las cuales generan dos secuencias binarias que deciden respectivamente en qué bloque y qué posición se ocultará el mensaje secreto encriptado mediante el algoritmo criptográfico AES. Finalmente, presentamos un análisis experimental para la validación del método propuesto.

Abstract In this article, a novel steganographic method based on the compression JPEG is proposed. The steganographic algorithm proposed embedded the secret information in some coefficients located in the middle-frequency area of the cover image (RGB), using a new quantization matrix different to the standard. In addition, the proposed method uses a public key and another private, both of 128 bits, which generate two binary sequences that indicate respectively in what block and what position the secret message encrypted by the cryptographic algorithm AES will be embedded. Finally, we present a experimental analysis for the validation of the proposed method.

Palabras Claves
Estaganografía — Pseudo-asimétrico — Matriz cuantización

[1] *Departamento de Matemática, Universidad de la Habana, Ciudad Habana, Cuba, jpp@aguacate.edu.cu, mgp@aguacate.edu.cu*
[2] *Facultad de Ciencias Técnicas, Universidad de Granma, Cuba, asorial@udg.co.cu, asorial1983@gmail.com*
***A. Soria-Lorente**

Introduction

A lo largo de la historia han sido empleados diversos medios y métodos para garantizar la seguridad de la información y al mismo tiempo han sido creados un sin número de técnicas y procedimientos para vulnerar los medios de seguridad y con ello revelar la información objeto de protección. De modo que reviste especial trascendencia trabajar con el propósito de lograr, cada día con mayor eficiencia, la implementación de métodos y procedimientos que garanticen la protección y seguridad de la información, los cuales se desarrollan en el campo de la criptografía y la esteganografía y juegan un papel significativo en la sociedad actual.

La criptografía es la ciencia de proteger y custodiar la información digital de forma segura mediante técnicas de cifrado, su objetivo no es ocultar la existencia de un mensaje, sino más bien ocultar su significado, un proceso que se conoce como codificación. La ventaja de esta es que si el enemigo intercepta un mensaje cifrado, éste es ilegible [26, 29, 28].

Por otro lado, la esteganografía constituye un conjunto de técnicas las cuales permiten ocultar o camuflar cualquier tipo de datos dentro de información considerada como válida. Además, la misma permite burlar la vigilancia electrónica en el Internet, o simplemente que terceras personas no tengan acceso a información no autorizada [29]. La esteganografía utiliza medios digitales, tales como archivos de texto [12, 27], audio [10, 13, 14, 17], imagen [20, 3, 4, 8, 16, 23] y video [6, 30], que son utilizados como el archivo de transporte para ocultar la información, a este medio se le conoce como contenedor o cubierta.

Entre las técnicas más usadas en la esteganografía se encuentran las correspondientes al dominio espacial [15, 29, 28]. La aplicación de la esteganografía en el dominio espacial, radica en que los algoritmos son utilizados en la manipulación de los píxeles y en la inserción de la información secreta en los bits menos significativos o bien de mayor redundancia [29, 28].

Otra de las técnicas dentro de la esteganografía tiene que ver con el dominio de la frecuencia [2, 21, 25, 26, 32], la cual está vinculada a los cambios de las altas y bajas frecuencias de la imagen, de forma tal, que las altas frecuencias como

los bordes, las líneas y ciertos tipos de ruidos son utilizados para ocultar información [26, 27]. Dentro de esta técnica se utilizan transformadas tales como la de Fourier [11], la transformada discreta de los cosenos [26, 32] y la de wavelets [6, 7, 19, 22].

El interés concreto de un sistema esteganográfico dependerá de tres características: capacidad (cantidad de información que puede ser ocultada), seguridad/invisibilidad (probabilidad de detección por un estegoanalista) y robustez (cantidad de alteraciones dañinas que el medio puede soportar antes de que se pierda la información oculta). Este último puede verse afectado ya que en las mayorías de las redes, a los medios digitales que se transmiten por ella, se le realizan transformaciones con el objetivo de reducir su tamaño y ganar en velocidad de transmisión, provocando con esto la pérdida de información.

Este hecho es bien conocido por la comunidad internacional, de aquí que, muchos países tienen como política, realizar transformaciones a los medios digitales que se transmiten a través de sus redes, no solo para ganar en velocidad, sino para de alguna manera restringir el uso de la Esteganografía. Entre los métodos más usados se encuentran la compresión de imágenes, archivos y otros datos.

Una de las técnicas más utilizadas para comprimir imágenes es la técnica de compresión JPEG (Joint Photographic Experts Group), el cual constituye uno de los estándares conocidos y más utilizados para la compresión de imágenes con perdida [23, 24, 33]; es decir, la imagen descomprimida no es exactamente la misma que aquella con la que se empezó.

En este trabajo se presenta un algoritmo esteganográfico basado fundamentalmente en la comprensión JPEG. El mismo a partir de una clave pública y una privada, oculta la información secreta en algunos coeficientes localizados en el área de las medias frecuencias de la imagen original, utilizando una nueva matriz de cuantificación diferente a la estándar. En la Sección 1 se describe el algoritmo propuesto, mientras que en la Sección 2 se presenta el análisis experimental realizado.

1. Algoritmo esteganográfico propuesto

El método propuesto utiliza el algoritmo criptográfico simétrico AES, con el objetivo de fortalecer la seguridad de la información secreta. El algoritmo AES también conocido como Rijndael fue diseñado por los belgas Joan Daemen y Vincent Rijmen y fue el ganador del concurso lanzado por el NIST en 1997 debido a que presentó la mejor combinación de seguridad, velocidad, eficiencia, sencillez y flexibilidad [1]. Su publicación oficial se presento bajo el nombre de FIPS PUB 197 en el año 2001. Se utiliza actualmente en instituciones bancarias, gubernamentales, de comunicaciones e industria privada entre otras.

Es un cifrador de bloques de tamaño fijo de 128 bits que puede utilizar llaves de (128, 192 ó 256 bits) realizando n rondas dependiendo de la llave (10, 12 ó 14 rondas) respectivamente. El proceso de cifrado comprende una ronda inicial, $n-2$ rondas estándar y una ronda final. Las transformaciones básicas son AddRoundKey, SubByte, ShiftRows, MixColumns y Key Schedule. Por cierto, la fortaleza del AES radica en los procedimientos de sus funciones y en la longitud de sus claves.

En este trabajo denotaremos por $\mathscr{L}$ a la longitud de la secuencia binaria del mensaje secreto

$$\mathscr{M} = \{m_i \in \{0,1\}\colon 1 \le i \le \mathscr{L}\}.$$

Por otro lado, denotaremos por $\mathscr{D}$ y

$$\mathscr{A} = \{a_\ell \in \{0,1\}\colon 1 \le \ell \le \mathscr{T}\}$$

las secuencias binarias que determinan los bloques de bytes y las posiciones donde los elementos de la secuencia binaria del mensaje secreto serán insertados, respectivamente.

1.1 Generación del camino de inserción

Denotemos por $|X|$ la cantidad de bit iguales a 1 de la secuencia binaria X. Aquí, las secuencias binarias $\mathscr{A}$ y $\mathscr{D}$, se determinan del siguiente modo:

- Solicitar una clave pública de 128 bits, generada por el emisor o extraída de una base de datos.
- Aplicar la operación $0 \oplus 0 = 1 \oplus 1 = 0$ and $0 \oplus 1 = 1 \oplus 0 = 1$ entre la clave pública y la correspondiente clave privada de 128 bits no transmitida, para generar una nueva secuencia $\mathscr{S}$ de 128 bits.
- A partir de $\mathscr{S}$, generar mediante el algoritmo propuesto en [26], la secuencia $\mathscr{A}$ con $|\mathscr{A}| = \mathscr{L}$ y $\text{card}(\mathscr{A}) = \mathscr{T}$.
- $\mathscr{D} = \bigcup_{1 \le i \le n} (\mathscr{P}_i \oplus \mathscr{S}) = \{d_r \in \{0,1\}\colon r \ge 1\}$,

  donde $\mathscr{A} = \mathscr{P}_1 || \mathscr{P}_2 || \ldots || \mathscr{P}_i || \ldots || \mathscr{P}_n$, siendo

  $$\mathscr{P}_i = \left\{p_j^i \in \{0,1\}\colon 1 \le j \le 64\right\}, \quad 1 \le i \le n,$$

  con $n = \mathscr{T}/64$.

1.2 Regla de reemplazamiento

Denotemos por $R(x,\beta)$ la función que reemplaza el LSB de $x \in \mathbb{N}$ por el correspondiente bit β de la secuencia binaria del mensaje secreto. Para $\beta = 0$ la regla $R(x,0)$ viene definida mediante

$$R(x,0) = \begin{cases} x-1, & \text{si } x \text{ es impar,} \\ x, & \text{si } x \text{ es par.} \end{cases} \tag{1}$$

De manera análoga, para $\beta = 1$ definimos $R(x,1)$ como

$$R(x,1) = \begin{cases} x, & \text{si } x \text{ es impar,} \\ x+1, & \text{si } x \text{ es par.} \end{cases} \tag{2}$$

La regla para la operación inversa R^{-1} viene dada mediante la siguiente función de extracción definida como

$$x = R^{-1}(y) = \begin{cases} 0, & \text{si } y \text{ es par,} \\ 1, & \text{si } y \text{ es impar.} \end{cases} \tag{3}$$

1.3 Proceso de cuantificación

En este trabajo, se modifica la tabla cuantificación estándar, conocida como matriz de Lohscheller

$$\begin{pmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{pmatrix} \tag{4}$$

con el propósito de incrementar la calidad de la estego-imagen.

En el proceso de cuantificación, cada bloque de 8×8 byte seleccionado por la secuencia binaria $\mathscr{D}$ es cuantificando usando la matriz de cuantificación Q^{α} con un factor de calidad α, dada mediante

$$\begin{pmatrix} 16 & 11 & 10 & 16 & \sigma_5^{\alpha} & \sigma_6^{\alpha} & 51 & 61 \\ 12 & 12 & 14 & \sigma_4^{\alpha} & \sigma_7^{\alpha} & 58 & 60 & 55 \\ 14 & 13 & \sigma_3^{\alpha} & \sigma_8^{\alpha} & 40 & 57 & 69 & 56 \\ 14 & \sigma_2^{\alpha} & \sigma_9^{\alpha} & 29 & 51 & 87 & 80 & 62 \\ \sigma_1^{\alpha} & \sigma_{10}^{\alpha} & 37 & 56 & 68 & 109 & 103 & 77 \\ \sigma_{11}^{\alpha} & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{pmatrix} \tag{5}$$

donde

$$\sigma^{\alpha} = \chi(\alpha)\,(18,17,16,19,24,40,26,24,22,22,24),$$

siendo $\chi(\alpha) = \dfrac{100-\alpha}{50}$, cuando $50 < \alpha < 100$.

Así los coeficiente DCT cuantificados $\Theta_{u,v}^{k}$ son calculados mediante

$$\Theta_{u,v}^{k} = \text{round}\left(\frac{\mathscr{B}_{u,v}^{k}}{Q_{u,v}^{\alpha}}\right), \quad 0 \le u,v \le 7. \tag{6}$$

1.4 Proceso de inserción y extracción

En este trabajo la información secreta es ocultada dentro de la imagen cubierta mediente el procedimiento descrito en Algoritmo 1.

Entrada: Mensaje secreto, imagen cubierta C de tamaño $M \times N$, clave privada, clave pública, factor de calidad α.

Salida: Estego-imagen S.

Procedimiento: En el algoritmo propuesto se asume que tanto el emisor como el receptor poseen el mismo sistema de claves privadas, las cuales no se deben transmitir por los canales inseguros de comunicación. El emisor genera la estego-imagen siguiendo los siguientes pasos:

- Convierte C del espacio de color RGB al YUV mediante:

$$\begin{pmatrix} Y \\ U \\ V \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ -0.147 & -0.289 & 0.436 \\ 0.615 & -0.515 & -0.100 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix}. \tag{7}$$

- Divide C en $3MN/64$ bloques (B^k) disjuntos de 8×8 bytes y luego procesa cada uno de ellos de manera independiente.

- Resta 128 a cada bloque de bytes para centrar los valores entre -128 y 127.

- Aplica la transformada discreta de coseno (DCT), a cada bloque de bytes de la imagen, con lo que se obtiene un dominio de la frecuencia (matriz de los coeficientes DCT).

- Cuantifica los coeficientes DCT mediante los valores de la matriz o tabla de cuantificación ya preestablecida (4)-(5). Esto es, cada coeficiente DCT del bloque de bytes, es dividido por la correspondiente constante de la matriz de cuantificación y luego se redondea a su número entero más cercano, véase (6). Este es el proceso donde se produce la pérdida de información de manera irreversible.

- Con el propósito de aprovechar el patrón ordenado de componentes de frecuencia, el algoritmo reordena los coeficientes cuantificados a un vector $v^k = \{v_i^k : 1 \le i \le 64\}$ de longitud 64, siguiendo un recorrido en Zig Zag, para lograr un mejor ordenamiento de las componentes de frecuencia, véase la Figura 1. De este modo, se obtiene un vector en el cual, el primer coeficiente es el coeficiente DC o de frecuencia cero y el resto son los coeficientes AC, divididos en tres partes, los de baja, media y altas frecuencias, respectivamente.

- Selecciona el correspondiente bloque de coeficientes cuantificados siempre y cuando el correspondiente elemento de la secuencia binaria $\mathscr{D}$ es igual a 1.

- Inserta los bits secretos m_i en los LSBs de las 10 primeras componentes de media frecuencia de los bloques de bytes seleccionados, siempre y cuando el correspondiente elemento de la secuencia binaria $\mathscr{A}$ es igual a 1 y dichas componentes sean distintas de -1, 0 y 1.

- Para finalizar comprime los coeficientes reordenados usando la codificación entrópica (Huffman coding, Run-Length coding, y DPCM [18]).

Por brevedad denotemos $\sigma(x) = \sqrt{2^{-1}}$ para $x = 0$ y $\sigma(x) = 1$ en caso contrario.

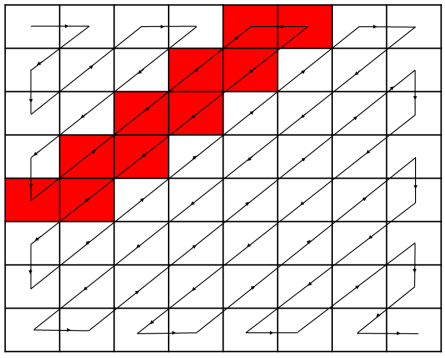

Figura 1. Escaneo en ZigZag

Algorithm 1 Algoritmo esteganográfico

▷ Convertir C del modelo RGB al YUV de acuerdo a (7);
▷ Particionar $C = B^1||B^2||\cdots||B^k||\cdots$, con $k \in \mathscr{K}$;
▷ Substraer 128 a cada byte de B^k;
for $k \in \mathscr{K}$ **do**
▷ Calcular para $0 \leq u, v \leq 7$:

$$\mathscr{B}^k_{u,v} = 4^{-1}\sigma(u)\sigma(v) \sum_{0\leq i,j\leq 7} B^k_{i,j} \times \cos\left(\frac{\pi u(2i+1)}{16}\right)\cos\left(\frac{\pi v(2j+1)}{16}\right);$$

end for
• $i = \ell = r = 0$;
for $k \in \mathscr{K}$ **do**
▷ $\Theta^k \leftarrow \mathscr{B}^k$: Cuantificar $\left(\mathscr{B}^k_{u,v}\right)$ de acuerdo a (6);
▷ $\nu^k \leftarrow \Theta^k$: Aplicar el escaneo en zigzag, Figura 1;
$r = \mathrm{mod}(r, \mathrm{card}(\mathscr{D})) + 1$;
if $d_r = 1$ **then**
for $j = 10, \ldots, 20$ **do**
$\ell = \mathrm{mod}(\ell, \mathscr{T}) + 1$;
if $a_\ell = 1$ **then**
if mode = EMBEDDING **then**
if $\nu^k_j \notin \{-1, 0, 1\}$ **then**
$i = i + 1$;
if $\nu^k_j < 0$ **then**
$\bar{\nu}^k_j \leftarrow -\mathrm{R}(|\nu^k_j|, m_i)$: Aplicar la regla de remplazamiento de acuerdo a (1)–(2);
else
$\bar{\nu}^k_j \leftarrow \mathrm{R}(\nu^k_j, m_i)$;
end if
end if
◁ Aplicar la codificación entrópica (Huffman coding, Run-Length coding, y DPCM), para comprimir cada vector $\bar{\nu}^k$;
◁ Generar el archivo JPEG S;
else
if $\nu^k_j \notin \{-1, 0, 1\}$ **then**
◁ Aplicar la codificación entrópica en sentido inverso (Huffman coding, Run-Length coding, y DPCM), para descomprimir cada vector comprimido $\bar{\nu}^k$;
$s_i = R^{-1}(|\nu^k_j|)$:
Aplicar la regla de extracción (3)
end if
end if
end if
end for
end if
end for

2. Resultados experimentales

En este capítulo se presentan los resultados experimentales del algoritmo propuesto. El mismo fue implementado en

Matlab. Se utilizaron 4 imágenes diferentes, de tamaño 784×512 pixeles, con un factor de calidad igual para $qF = 67$. Las imágenes originales y su correspondiente estego-imagen son mostradas en la Figura 2. Para realizar los experimento fueron tomadas a la azar 100 pares claves de 128 bits cada una. Se probó el algoritmo propuesto insertando en cada una de las 4 imágenes un mensaje de tamaño 20616 bits. Además, se realizó una comparación intercambiando las matrices de cuantificación (4) y (5), respectivamente.

Figura 2. Las imágenes antes y despues de la inserción del mensaje secreto. La primera columna contiene las imágenes cubiertas mientras que la segunda las estego-imágenes

3. Prueba de imperceptibilidad

Una medida de distorsión es la conocida PSNR (Relación Señal a Ruido Pico) en el esteganograma con respecto a la imagen original. El PSNR es muy común en el proceso de una imagen, su utilidad reside en dar una relación del grado de supresión de ruido entre la imagen original y el esteganograma, proveyendo de esta manera una medida de calidad [28]. El PSNR está dado en unidades llamadas decibelios (dB) y se escribe de la siguiente forma [27, 28, 29]

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{256^2}{\mathrm{MSE}}\right),$$

donde

$$\mathrm{MSE} = (3MN)^{-1}\sum_{\gamma\in\Gamma}(C(\gamma)-S(\gamma))^2.$$

Además, el conjunto índice $\gamma = (\gamma_1,\gamma_2,\gamma_3)$ se suma sobre el conjunto de bytes como

$$\Gamma = \{1,\ldots,M\}\times\{1,\ldots,N\}\times\{1,2,3\},$$

y $C,S \in \{0,1,\ldots,255\}$.

El primer experimento, arrojó que el algoritmo propuesto produce estego-imágenes de muy buena calidad, donde los valores de PSNR están en correspondencia con los valores heurísticos de PSNR (30 para 50 db) encontrados en la literatura [9], veáse las Figuras 3–4. Además, estos resultados muestran que se logra un menor grado de distorsión al utilizar la matriz de cuantificación modificada en lugar de la estándar, alcanzándose mayor nivel de imperceptibilidad para las imágenes Lenna y Air-plane.

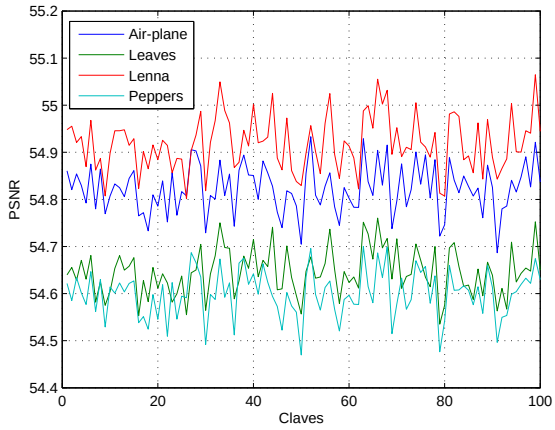

Figura 3. Valores de PSNR correspondientes a la tabla de cuantificación modificada

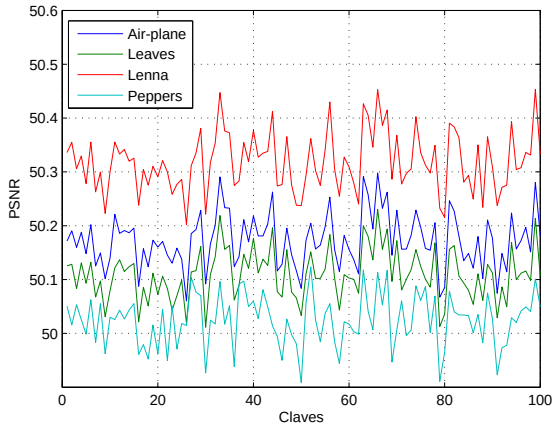

Figura 4. Valores de PSNR correspondientes a la tabla de cuantificación estándar

4. Medida de Calidad de Imagen

Entre las medidas de calidad de la imagen basadas en la diferencia de distorsión se incluye la Diferencia Absoluta (AD) [31] representada mediante:

$$\mathrm{AD} = (3MN)^{-1} \sum_{\gamma \in \Gamma} |C(\gamma) - S(\gamma)|.$$

Para esta métrica, mientras más cercano el valor es a cero, mayor será la calidad de la estego-imagen; es decir, disminuye la distorsión global de la misma con respecto a la imagen cubierta.

El segundo experimento mostró que los valores de AD son cercanos a cero, por consiguiente, entre las imágenes cubiertas y las estego-imágenes no existen diferencias significativas. Cabe señalar, que los mejores resultados fueron alcanzados a partir de la matriz de cuantificación modificada, como se puede observar en las Figuras 5–6.

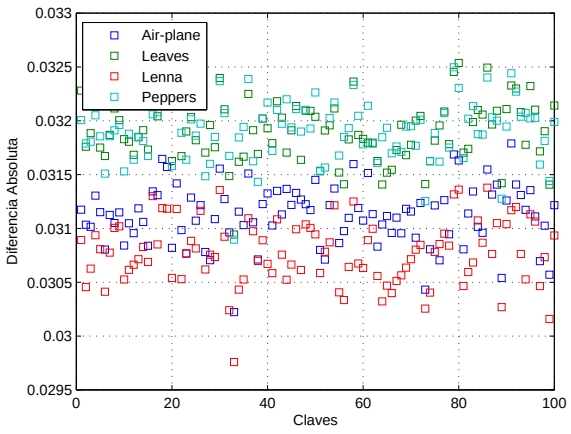

Figura 5. Valores de AD correspondientes a la tabla de cuantificación modificada

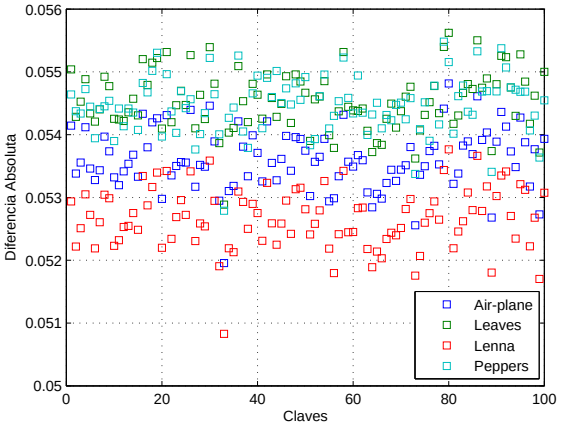

Figura 6. Valores de AD correspondientes a la tabla de cuantificación estándar

5. Análisis de Histograma

En el tercer experimento fue usada la imagen Peppers. En la Figura 8, se muestran los histogramas para el bloque rojo de la imagen analizada. Una métrica de distorsión es la Similitud del Histograma (HS), la cual es calculada mediante

$$\mathrm{HS} = \sum_{0 \le l \le 255} |f_C(l) - f_S(l)|,$$

donde $f_C(l)$ es la frecuencia relativa del l-ésimo nivel de gris de la imagen, véase [31]. Esta medida está vinculada con las diferencias entre cada par histograma. La Figura 7 muestra que los valores de HS están próximos a cero, lo cual se corresponde a los valores calculados en el ejemplo anterior.

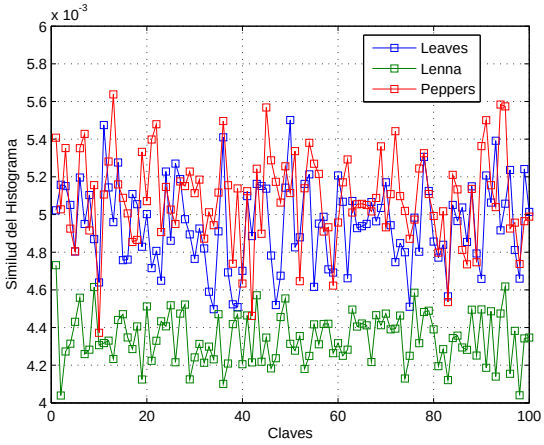

Figura 7. Valores de HS correspondientes a la tabla de cuantificación modificada

6. Prueba de Seguridad

La seguridad de un sistema esteganográfico es evaluada tras examinar la distribución de la cubierta y del esteganograma. Cachin [5], propuso una medida que cuantifica la seguridad del sistema esteganográfico llamada ε-seguro, la cual viene dada mediante la expresión

$$\mathrm{RE}(P_C||P_S) = \sum P_C \left| \log \frac{P_C}{P_S} \right| \le \varepsilon,$$

donde P_C y P_S representan la distribución de los histogramas de la cubierta y del esteganograma respectivamente. La última expresión representa la entropía relativa entre las dos probabilidades de distribución P_C y P_S. Hay que destacar que un sistema esteganográfico se llama perfectamente seguro si $\mathrm{ER}(P_C||P_S) = 0$, sin embargo, conforme aumenta la cantidad de información que se oculta, aumenta al mismo tiempo la robustez, por lo cual esta entropía también aumenta, de forma tal que, la seguridad de un sistema esteganográfico es medida a través de un valor ε, para cualquier tipo de imagen [5].

En el cuarto experimento se observa que los valores de entropía relativa se aproximan a cero, lo cual evidencia que el

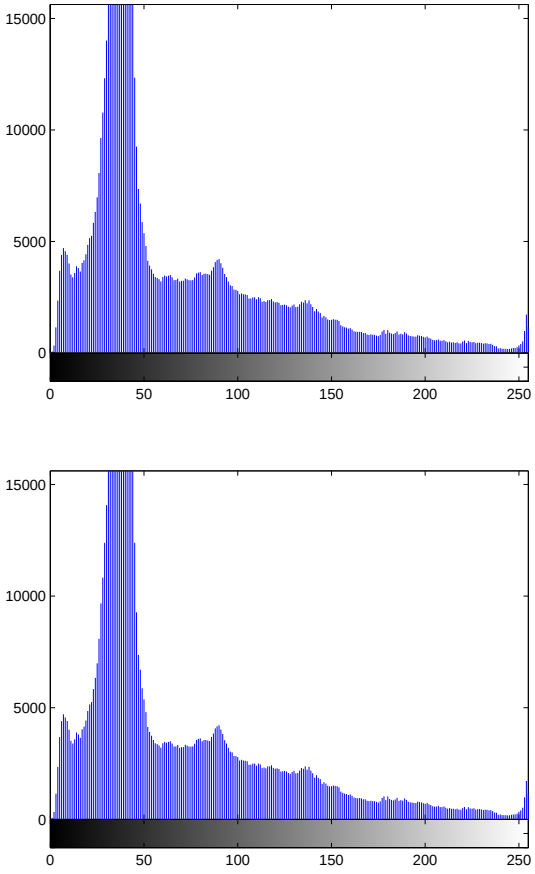

Figura 8. El histograma de imagen Peppers antes y después de insertado el mensaje secreto.

sistema esteganográfico obtenido a partir del algoritmo propuesto es suficientemente seguro, ver Figura 9.

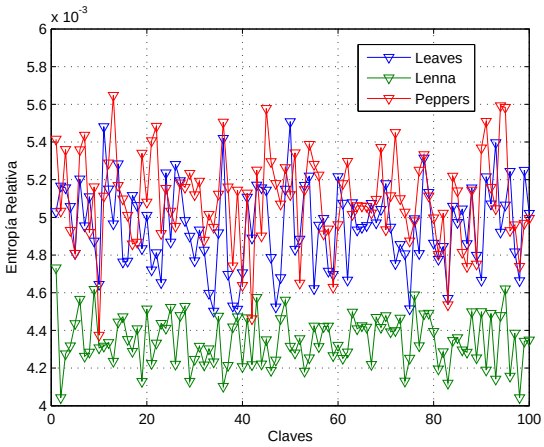

Figura 9. Valores de la RE correspondientes a la tabla de cuantificación modificada

7. Conclusiones

En este artículo, se ha presentado un algoritmo esteganográfico que utiliza una matriz de cuantificación distinta a la estándar así como dos claves, una pública y otra privada, las cuales contribuyen a localizar las partes de la imagen donde serán insertados los elementos de la secuencia binaria del mensaje secreto. De acuerdo con el análisis experimental realizado, quedó demostrado que no existen anomalías detectables a simple vista, en la estego-imagen con relación a la imagen cubierta. Además, los valores conseguidos para la entropía relativa, ponen de manifiesto que el sistema esteganográfico obtenido a partir del algoritmo propuesto, es suficientemente seguro.

Acknowledgments

Los autores expresan sus más sinceros agradecimientos al proyecto ClaveMat, financiado por la unión Europea, www.clavemat.com y a la Universidad de Granma donde el artículo fue escrito.

Referencias

[1] Specification for the advanced encryption standard (aes) federal information processing standards (fips) publication 197 http://csrc.nist.gov/encryption/aes/frn-fips197.pdf. November, 2001.

[2] M. Amin, H. Abdullkader, H. Ibrahem1, and A. Sakr. A steganographic method based on dct and new quantization technique. *International journal of Network Security*, 16:265–260, 2014.

[3] D. Bandyopadhyay, K. Dasgupta, J. K. Mandal, and P. Dutta. A novel secure image steganography method

based on chaos theory in spatial domain. *International Journal of Security, Privacy and Trust Management (IJSPTM)*, 3(1):11–22, 2014.

[4] D. Biswasa, S. Biswasb, A. Majumdera, D. Sarkara, D. Sinhaa, and A. Chowdhurya. Digital image steganography using dithering technique. *Procedia Technology*, 4:251–255, 2012.

[5] C. Cachin. An information-theoretic model for steganography. 1525:306–318, 1998.

[6] B. Carvajal-Gámez, M. Acevedo, and J. López-Bonilla. Técnica esteganográfica para ocultar un video dentro de otro utilizando la transformada wavelet discreta. *Journal of Vectorial Relativity*, 2(4):54–61, 2009.

[7] B. Carvajal-Gámez, F. Gallegos-Funes, and J. López-Bonilla. Esteganografía para imágenes rgb: Factor de escalamiento. *Journal of Vectorial Relativity*, 4(3):66–77, 2009.

[8] C. Chang, X. Lin, and C. Tseng. Reversible hiding in dct-based compressed images. *Inform. Sci.*, 177:2768–2786, 2007.

[9] I. Coskun, F. Akar, and O. Cetin. A new digital image steganography algorithm based on visible wavelength. *Turk. J. Elec. Eng. & Comp. Sci.*, 21:548–564, 2013.

[10] S. Geetha, N. Ishwarya, and N. Kamaraj. Evolving decision tree rule based system for audio stego anomalies detection based on hausdorff distance statistics. *Information Sciences*, 180:2540–2559, 2010.

[11] S. Kalaivanan, V. Ananth, and T. Manikandan. A survey on digital image steganography. *International Journal of Emerging Trends & Technology in Computer Science*, 4(1):30–33, 2015.

[12] G. Kumar and A. Rana. Data hiding techniques in digital multimedia. *International Journal of Engineering Science Invention Research and Development*, I:333–337, 2015.

[13] S. Kumar, B. Barnali, and G. Banik. Lsb modification and phase encoding technique of audio steganography revisited. *International Journal of Advanced Research in Computer and Communication Engineering*, 1(4):1–4, 2012.

[14] S. Kumar, B. Barnali, and G. Banik. Lsb modification and phase encoding technique of audio steganography revisited. *International Journal of Advanced Research in Computer and Communication Engineering*, 1(4):1–4, 2012.

[15] X. Liao, Q. Wen, and J. Zhang. A steganographic method for digital images with four-pixel differencing and modified lsb substitution. *Journal of Visual Communication and Image Representation*, 22:1–8, 2011.

[16] X. Liao, Q. Wena, and J. Zhang. A steganographic method for digital images with four-pixel differencing and modified lsb substitution. *J. Vis. Commun. Image R.*, 22:1–8, 2011.

[17] B. Linu, J. Jais, B. Parameshachari, C. Muruganantham, and M. Divakara. Steganographic method for data hiding in audio signals with lsb and dct. *International Journal of Computer Science and Mobile Computing*, 2:54–62, 2013.

[18] S. Mansi and H. Vijay. Current status and key issues in image steganography: A survey. *Computer Science Review*, http://dx.doi.org/10.1016/j.cosrev.2014.09.001, 2014.

[19] J. Mazumder and K. Hemachandran. A high capacity and secured color image steganographic technique using discrete wavelet transformation. *International Journal of Computer Science and Information Technologies*, 4(4):583–589, 2013.

[20] A. Nag, S. Biswas, D. Sarkar, and P.P. Sarkar. A novel technique for image steganography based on block-dct and huffman encoding. *International Journal of Computer Science and Information Technology*, 2(3):103–112, 2010.

[21] H. Noda, M. Niimi, and E. Kawaguchi. High-performance jpeg steganography using quantization index modulation in dct domain. *Pattern Recognition*, 27:455–461, 2006.

[22] I. Orea-Flores, M. Acevedo, and J. López-Bonilla. Wavelet and discrete transform for inserting information into bmp images. *Anziam Jour*, 48(1):23–35, 2006.

[23] S. Sachdeva, A. Sharma, and V. Gill. Colour image steganography using modified jpeg quantization technique. *International Journal of Latest Research in Science and Technology*, 1:1–5, 2012.

[24] S. Sachdeva, A. Sharma, and Gill V. Colour image steganography using modified jpeg quantization technique. *International Journal of Latest Research in Science and Technology*, 1:1–5, 2012.

[25] T. Shahana. A secure dct image steganography based on public-key cryptography. *International Journal of Computer Trends and Technology (IJCTT)*, 4(7):2038–2043, 2013.

[26] A. Soria-Lorente and S. Berres. A secure steganographic algorithm based on frequency domain for the transmission of hidden information. *Security and Communication Networks*, 2017, Article ID 5397082, https://doi.org/10.1155/2017/5397082:1–14, 2017.

[27] A. Soria-Lorente, R. Cumbrera-González, and Y. A Fonseca-Reyna. Steganographic algorithm of private key on the domain of the cosine discrete transform. *Revista Cubana de Ciencias Informáticas*, 10(2):116–131, 2016.

[28] A. Soria-Lorente, R. Manuel-Sánchez, and A. Ramírez-Aberasturis. Steganographic algorithm of private key. *Revista de investigación, G.I.E Pensamiento Matemático*, 3(2):59–72, 2013.

[29] A. Soria-Lorente, R. Mecías, A. A. Pérez, and D. Rodríguez. Pseudo-asymmetric steganograph algorithmy. *Lect. Mat.*, 35(2):183–196, 2014.

[30] J. Steffy, G. Yogaraj, and K. Rajalakshmi. Lsb approach for video steganography to embed images. *International journal of Computer Science and Information Technologies*, 5:319–322, 2014.

[31] K. Thung, R. Paramesran, and C. L. Lim. Content-based image quality metric using similarity measure of moment vectors. *Pattern Recognition*, 45(6):2193–2204, 2012.

[32] C. Velasco, J. López, M. Miyatake, and H. Pérez. Esteganografía en una imagen digital en el dominio dct. *Científica*, 11:169–176, 2007.

[33] L. Yu, Y. Zhao, R. Ni, and Z. Zhu. M1 steganography in jpeg images using genetic algorithm. *Soft Computing*, 13(4):393–400, 2009.