ROCA. Revista científico- educacional de la provincia Granma.
Vol.14 No. 2, abril-junio 2018. ISSN: 2074-0735. RNPS: 2090. roca@udg.co.cu

Original

SEGURIDAD DE IMÁGENES DIGITALES MEDIANTE UN ALGORITMO ESTEGANOGRÁFICO EN EL DOMINIO DE LA FRECUENCIA

Security of digital images through a steganographic algorithm in the domain of frequency

Lic. Arioldis Figueroa-Romero. Universidad de Guantánamo, Cuba,
gtmoicc@mail.mn.co.cu ,
Lic. Alicia María Centurión-Fajardo. Profesor Asistente, Universidad de Granma,
Cuba, acenturionf@udg.co.cu
Dr. C. Anier Soria-Lorente, Profesor Titular. Universidad de Granma,
asorial@udg.co.cu, Cuba

Recibido: 20/12/2018 Aceptado: 13/3/2018

RESUMEN

En la actualidad, la sociedad demanda que su información, en la mayoría de las veces, confidencial, sea protegida de cualquier agente externo no autorizado a acceder a ella. Por tal razón se están desarrollando técnicas matemáticas e informáticas para impedir que la información sensible sea accedida, modificada, plagiada o destruida. En este trabajo, se presenta un algoritmo esteganográfico para la seguridad de la información privada y confidencial que transita por los diferentes canales de comunicación en el Internet. El método propuesto está vinculado al dominio de la frecuencia, el cual emplea un par de claves de 64 bits, una pública y una privada, para luego ocultar la información secreta en algunos coeficientes de las componentes de baja frecuencia. Finalmente, se presenta un análisis experimental para medir la calidad, imperceptibilidad y seguridad del sistema esteganográfico propuesto.

PALABRAS CLAVES: Algoritmo esteganográfico; dominio de la frecuencia; imágenes digitales; seguridad.

ABSTRACT

Nowadays, the society requires that its information, most of the times, confidential, be protected from any external agent not authorized to accede to it. For such a reason, mathematical and computer science techniques are being developed to impede that the perceptible information be acceded, modified, plagiarized or destroyed. In this work, a steganographic algorithm for the security of private and confidential information that transits for the different communication

channels on the internet is presented. The proposed method is connected to the frequency domain, which uses a pair of keys of 64 bits, one public and one private, with the purpose of hiding the secret information in some coefficients of the low frequency components. Finally, an experimental analysis to measure the quality, imperceptibility and security of the steganographic system proposed is showed.

KEY WORDS: Steganographic algorithm; frequency domain; digital images; security.

INTRODUCCIÓN

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización. La seguridad de la información es un conjunto de medidas para garantizar la disponibilidad, confidencialidad, e integridad de la información (Soria, A., 2017; Soria, A., Moreno, E.R. y Centurión, A.M., 2015).

Desde la antigüedad han sido empleados diversos medios y métodos para garantizar dicha seguridad, unido a ello se han creado diversas técnicas y procedimientos para quebrantarla, provocando de esta forma que deje de estar protegida, por lo que es imprescindible desarrollar procedimientos y métodos más sofisticados que garanticen la protección y seguridad de la información contra estas amenazas y se pueda ocultar información dentro de las imágenes y así garantizar la seguridad y privacidad de la información al transitar a través de los diferentes canales en la red (Soria, A., 2017; Soria, A., Moreno, E.R. y Centurión, A.M., 2015).

La criptografía es la ciencia que garantiza la seguridad de la información en cuanto a Integridad, autenticación, confidencialidad y lo realiza a través de técnicas de cifrado. Esta no oculta la existencia de un mensaje, sino que la codifica de tal manera que si el enemigo intercepta un mensaje cifrado, este sea ilegible (Soria, A. and Berres, S., 2017; Soria, et al., 2014; Soria, A., Manuel, R. and Ramírez, A. M., 2013).

A diferencia de la Criptografía, la Esteganografía es un conjunto de técnicas que permiten ocultar o camuflar cualquier tipo de datos dentro de información considerada válida, permitiendo burlar la vigilancia electrónica en el Internet, o del acceso de personas no admitidas. (Soria, et al., 2014; Centurión, A.M, Soria. A and Estrada, P.M., 2018). Los medios que utiliza para su fin son los digitales, tales como los archivos de texto (Kumar, G. and Rana, A., 2015; Soria, A., Cumbrera, R. and Fonseca, Y.A., 2016), audio (Kumar, S., Barnali, B. and Banik, G.,2012), imagen (Soria, et al., 2014; Centurión, A.M, Soria. A and Estrada, P.M., 2018; Chang, C., Lin, X. and Tseng, C. ,2007) y video (Steffy, J., Yogaraj, G., and Rajalakshmi, K., 2014), que son

utilizados como el archivo de transporte para ocultar la información, a estos medios se le conoce como contenedor o cubierta.

A pesar del diferente enfoque de cada una, en muchas ocasiones se combinan ambas técnicas para lograr mejores resultados.

Una de las técnicas más usadas dentro de la esteganografía son las que trabajan en el dominio espacial (Soria, et al., 2014; Soria, A., Manuel, R. and Ramírez, A. M. 2013), que tienden a proporcionar mayor capacidad de inserción que otros métodos. En estas técnicas 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 (Soria, et al., 2014; Soria, A., Manuel, R. and Ramírez, A. M. 2013).

Otra de las técnicas usadas es la que operan en el dominio de la frecuencia (Shahana, T. (2013; Soria, A. and Berres, S.,2017; Velasco, C., et al., 2007), asociada a los cambios de las altas y bajas frecuencias de la imagen, de tal manera, que las altas frecuencias como los bordes, las líneas y ciertos tipos de ruidos son utilizados para ocultar información (Soria, A. and Berres, S. ,2017; Soria, A., Cumbrera, R. and Fonseca, Y.A., 2016), para ello se utilizan herramientas matemáticas como la transformada discreta de los cosenos (Soria, A. and Berres, S., 2017; Velasco, C., et al., 2007) y la de wavelets (Mazumder, J. and Hemachandran, K., 2013).

Un sistema Esteganográfico está caracterizado por tres elementos fundamentales: capacidad (cantidad de información que puede ser ocultada), seguridad/invisibilidad (probabilidad de detección por un estego-analista) y robustez (cantidad de alteraciones dañinas que el medio puede soportar antes de que se pierda la información oculta). Estas características son de conocimiento en el ámbito internacional, por lo que es común que muchos países tengan como política manipular los medios digitales que viajan en sus redes, ejemplo de esto es la compresión imágenes, archivos y otros datos.

Otra de las técnicas más utilizadas por la comunidad internacional para comprimir imágenes está la compresión JPEG (Joint Photographic Experts Group), el cual constituye uno de los estándares más conocidos y utilizados para la compresión de imágenes con pérdida. Fue diseñado para comprimir imágenes, full color y en escala de grises, de escenas naturales del mundo real. Se obtienen buenos resultados al aplicarlo sobre fotografías, trabajos de arte y material similar, aunque no ocurre así con letras, dibujos simples o dibujos de líneas (Chang, C., Lin, X. and Tseng, C., 2007).

En el desarrollo de la Esteganografía varios autores han propuestos métodos esteganográficos que insertan la información en el proceso de compresión JPEG usando la matriz de cuantificación estándar obteniéndose muy buenos resultados, pero otros han buscado resultados modificando esta matriz. Uno de los primeros trabajos publicado en el tema fue el artículo (Chang, C., Lin, X. and Tseng, C. , 2007) donde los autores realizan cambios en la matriz de cuantificación y demuestran que con esto se puede tener muy buenos resultados, en (Coskun, I., Akar, F., and Cetin, O., 2013) se utilizó la matriz modificada en la media frecuencia, luego en (Soria, A., Mecías, R. Pérez, A. A. and Rodríguez, D., 2014) que utilizaba la matriz de cuantificación modificada propuesta en (Chang, C., Lin, X. and Tseng, C., 2007).

En el trabajo presentado por Centurión, A.M, Soria y Estrada, P.M., (2018) en el I Taller Nacional de Calidad Educativa, CICE, se presenta un algoritmo esteganográfico que utiliza una clave pública de 128 bits y un cuadrado mágico de 8x8, a partir de las cuales se genera una secuencia pseudoaleatoria, que indica los píxeles de la imagen donde se insertan los elementos de la secuencia binaria del mensaje secreto.

El objetivo de este trabajo es elaborar un algoritmo esteganográfico vinculado al dominio de la frecuencia, el cual utiliza una clave privada y una pública, para ocultar información en imágenes digitales, con el propósito de que la imagen no sea perceptible ante cualquier sistema de cómputo, garantizando la seguridad de la información.

POBLACIÓN Y MUESTRA

Descripción del algoritmo esteganográfico utilizando el dominio de la frecuencia.

Proceso de inserción

Entrada: Imagen cubierta (*C*), clave privada de 64 bits, clave pública de 64 bits, mensaje secreto $\boldsymbol{M} = \{m_1, \cdots, m_r\}$, donde $m_i \in \{0,1\}$ con $1 \leq i \leq L$.

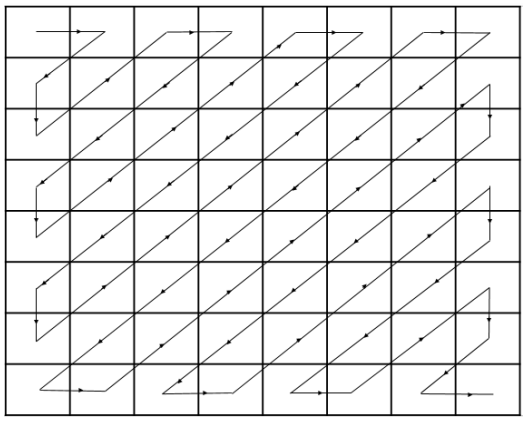
Salida: Estego imagen (*S*).

Procedimiento:

- ✓ Solicitar una clave privada y una pública de 64 bits respectivamente al emisor.
- ✓ Generar la secuencia binaria ***seqbit*** a partir de ambas claves, teniendo en cuenta el procedimiento propuesto por Soria, A y Berres, S.(2017).
- ✓ Tomar:

$$\boldsymbol{A} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 \\ 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 \\ 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 \\ 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 \\ 49 & 50 & 51 & 52 & 53 & 54 & 55 & 56 \\ 57 & 58 & 59 & 60 & 61 & 62 & 63 & 64 \end{bmatrix}$$

- ✓ Aplicar a ***A*** el escaneo en ZigZag



Para conseguir la secuencia *seqord*.

- ✓ Continuar los pasos del Algoritmo 1.

Algoritmo 1: Proceso de Inserción
r=0;
l=0;
For $1 \leq i \leq numfilas/8$ de la imagen, hacer
ui = (i-1)8+1;
uf = 8i;
For $1 \leq j \leq numcolumnas/8$ de la imagen, hacer
If *seqbit*(*r*) == *1*
vi = (seqord(j) – 1)8+1;
vf = 8j;
Matrix=DCT(*C*(*ui:uf*,*vi:vf,3*)); (DCT≡Transformada discreta de los cosenos)
Matrix=Cuantificar(Matrix) (Ver Soria, A. and Berres, S.,2017)
Aplicar el escaneo en ZigZag a Matrix para conseguir *Coeff*;

For $2 \leq k \leq 9$ hacer

l = l+1;

If *Coeff(k)<0*

Remplazar el LSB de |*Coeff(k)*| por m_l; (LSB≡Bit menos significativo)

Else

Remplazar el LSB de *Coeff(k)* por m_l;

End If

End For

Aplicar el escaneo en ZigZag a *Coeff* para conseguir Matrix;

S(*ui:uf*,*vi:vf,3*)=IDCT(Matrix); (IDCT≡Transformada Inversa de DCT)

r=r+1;

Else

r=r+1;

End If

End For

End For

Proceso de extracción:

Entrada: Estego imagen (*S*), clave privada de 64 bits, clave pública de 64 bits.

Salida: Mensaje Secreto (*M*).

Procedimiento:

- ✓ Solicitar una clave privada y una pública de 64 bits respectivamente al emisor.
- ✓ Generar la secuencia binaria *seqbit* a partir de ambas claves, teniendo en cuenta el procedimiento propuesto por Soria, A y Berres, S., (2017).
- ✓ Continuar los pasos del Algoritmo 2.

Algoritmo 2: Proceso de Extracción

r=0;

l=0;

For $1 \leq i \leq numfilas/8$ de la imagen, hacer

ui = (i-1)8+1;

uf = 8i;

For $1 \leq j \leq numcolumnas/8$ de la imagen, hacer

```
        If  seqbit(r) == 1
          vi = (seqord(j) – 1)8+1;
          vf = 8j;
          Matrix=DCT(C(ui:uf,vi:vf,3)); (DCT≡Transformada discreta de los cosenos)
          Matrix=Cuantificar(Matrix) (Ver Soria, A. and Berres, S.,2017).
          Aplicar el escaneo en ZigZag a Matrix para conseguir Coeff;
          For 2 ≤ k ≤ 9 hacer
            l = l+1;
            If Coeff(k)<0
              Extraer el LSB de |Coeff(k)| por m_l; (LSB≡Bit menos significativo)
            Else
              Extraer el LSB de Coeff(k) por m_l;
            End If
          End For
          r=r+1;
        Else
          r=r+1;
        End If
    End For
End For
```

ANÁLISIS DE LOS RESULTADOS

Para el análisis experimental se estudian 4 imágenes RGB de 24 bits de tamaño 512 x 512, ver Figura 1, y se analiza la imperceptibilidad y seguridad del sistema esteganográfico teniendo en cuenta 50 claves diferentes escogidas aleatoriamente.

Como es conocido, la eficiencia en la protección de la información mediante la esteganografía, radica precisamente en el uso de un algoritmo esteganográfico adecuado que posibilite de forma correcta la inserción de datos, donde uno de los principales factores a tener en cuenta es el nivel de imperceptibilidad, debido a que un sistema esteganográfico tiene que generar un esteganograma suficientemente inocente, ya que no debe de levantarse ninguna sospecha. Por tanto, el grado de distorsión o imperceptibilidad de un esteganograma respecto a la imagen original juega un papel fundamental (Soria Lorente, et al., 2014).

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. El PSNR está dado en unidades llamadas decibelios (dB) y se escribe de la siguiente forma (Soria Lorente, et al., 2014):

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

donde MSE está dado por el error cuadrático medio

$$\text{MSE} = \frac{1}{3mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{3}\left\|I\left(i,j,k\right) - E\left(i,j,k\right)\right\|^2,$$

siendo *I* la imagen original y *E* el esteganograma.

La seguridad de un sistema esteganográfico es evaluada tras examinar la distribución de la cubierta y del esteganograma. Cachin en 1998 (Soria Lorente, et al., 2014), propone una medida que cuantifica la seguridad del sistema esteganográfico llamada -seguro, la cual viene dada mediante la expresión

$$\text{ER}(P_C||P_E) = \sum P_C\left|\log\frac{P_C}{P_E}\right| \leq \epsilon,$$

donde P_C y P_E, son las probabilidades de 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_E. Cabe notar que, un sistema esteganográfico se llama perfectamente seguro si ER(P_C||P_E) = 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, para cualquier tipo de imagen (Soria Lorente, et al., 2014).

A continuación, se mostrarán algunos de los experimentos realizados a las imágenes RGB de 24 bits, mostradas en la Figura 1.

Como se podrá observar en lo que sigue, para el algoritmo propuesto, la imagen original y la estego imagen no muestran diferencias notorias.

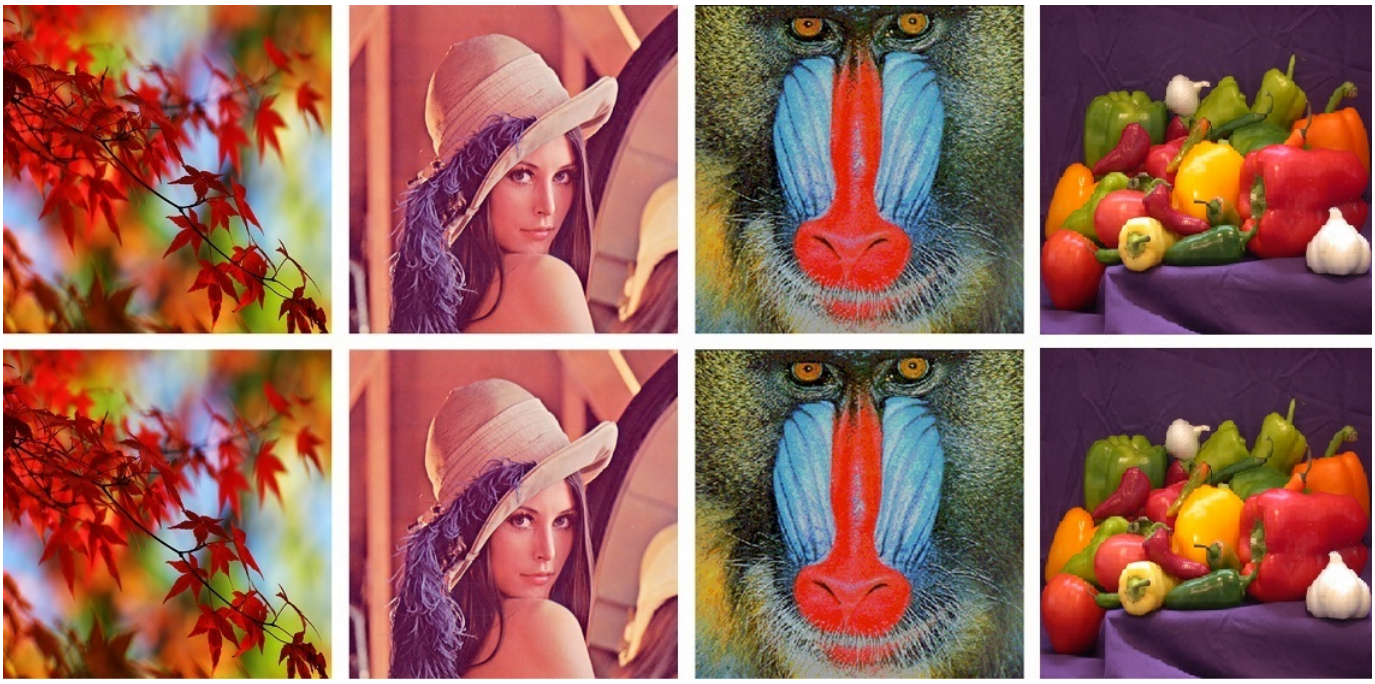


Figura 1: Imágenes antes y después de la inserción de la información secreta. Las imágenes de arriba representan las originales o cubiertas mientras que las de abajo son las estego-imágenes.

Para el desarrollo del primer experimento se utilizan 50 claves privadas de 128 bits, diferentes, escogidas al azar y se oculta a partir del algoritmo propuesto un mensaje secreto de tamaño 1551 bytes (12408 bits), obteniéndose de este modo 50 estego imágenes diferentes para cada imagen cubierta. Como se puede observar, los valores de los PSNR obtenidos a partir del algoritmo propuesto, evidencian claramente el alto grado de calidad de las estego imágenes así como el elevando nivel de imperceptibilidad, elemento fundamental en un sistema esteganográfico fuerte. De las 4 imágenes, las que mejores resultados arrojaron, en cuanto a imperceptibilidad, fueron las imágenes Leaves, Peppers y Lenna, ver Figura 2.

Por otra parte, los valores de la entropía relativa, para cada plano, aumentan levemente con respecto al resultado alcanzado en (Soria Lorente, et al., 2014), no obstante, en todos los casos, los valores obtenidos para la entropía relativa en cada uno de los planos, son cercanos a cero; por lo que se puede afirmar que el sistema esteganográfico conseguido a partir del algoritmo propuesto, es suficientemente seguro.

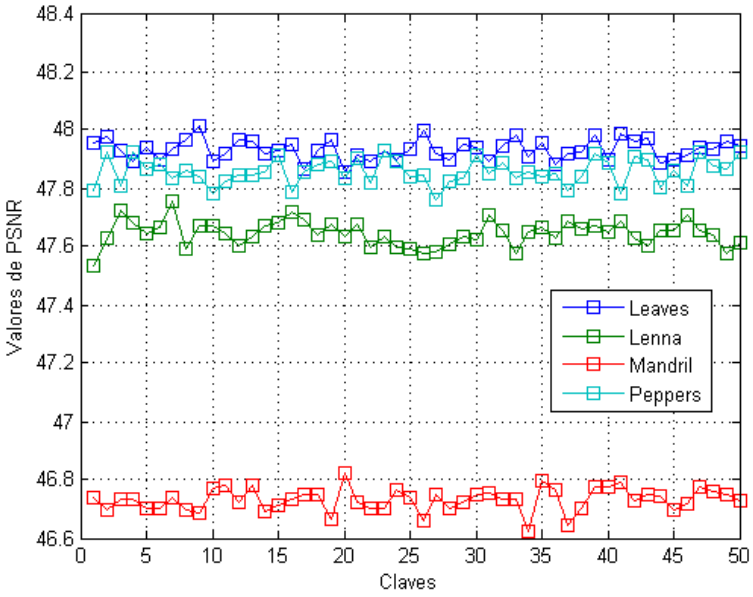


Figura 2: Gráfico comparativo de los PSNR correspondientes a las imágenes Leaves, Lenna, Mandril y Peppers, con dimensiones 512 x 512 cada una.

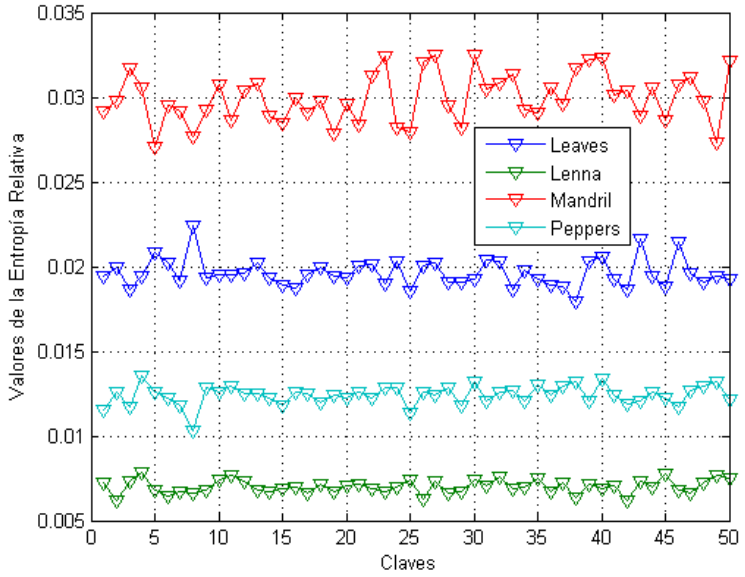


Figura 3: Gráfico comparativo de los ER correspondientes a las imágenes Leaves, Lenna, Mandril y Peppers, con dimensiones 512 x 512 cada una.

CONCLUSIONES

1. En este artículo, se propone un algoritmo esteganográfico en el dominio de la frecuencia con el propósito de insertar la información privada y secreta en las componentes de baja frecuencia de la imagen cubierta.

2. A partir del análisis experimental, los resultados vinculados a la calidad e imperceptibilidad, demuestran que entre las imágenes originales y las estego imágenes no existen diferencias significativas y mucho menos notorias frente al sistema visual humano.
3. Los valores cercanos a cero de la entropía relativa, evidencian que el sistema esteganográfico propuesto es seguro frente a agentes externos no autorizados, dando lugar a que la información sensible transite a través de los disímiles canales de comunicación sin que sea detectada.

REFERENCIAS BIBLIOGÁFICAS

Centurión, A.M., Soria, A., Estrada, P.M. (2018.) Un Algoritmo Esteganográfico vinculado a los Cuadrados Mágicos. I Taller Nacional de Calidad Educativa. CICE. Centro de Innovación y Calidad de la educación. UCI.

Chang, C., Lin, X. and Tseng, C. (2007). Reversible hiding in dct-based compressed images. Inform. Sci., 177. pp.768–2786.

Coskun, I., Akar, F., and Cetin, O. (2013). A new digital image steganography algorithm based on visible wavelength. Turk. J. Elec. Eng. & Comp. Sci., 21 . pp. 548–564.

Kumar, G. and Rana, A. (2015). Data hiding techniques in digital multimedia. International Journal of Engineering Science Invention Research and Development, I: . pp.333–337Soria, A. (2017). Implicaciones Sociales de la Criptografía y la Esteganografía.

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

Mazumder, J. and Hemachandran, K. (2013). A high capacity and secured color image steganographic technique using discrete wavelet transformation. International Journal of Computer Science and Information Technologies, 4(4). pp. 583–589Soria, A., Moreno, E.R y Centurión, A.M.(2015). Algoritmo esteganográfico pseudo-asimétrico con claves de 128 bits. XI Taller metodológico Patriótico Militar.

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

Soria, A. and Berres, S. (2017). 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 pp. 1–14.

Soria, A., Mecías, R., Pérez, A.A. and Rodríguez, D. (2014). Pseudo-asymmetric steganograph algorithmy. Lecturas Matemáticas, 35(2). pp.183–196.

Soria, A., Manuel, R. and Ramírez, A. M. (2013) Steganographic algorithm of private key. Revista de investigación, 3(2). pp.059–072.

Soria, A., Cumbrera, R. and Fonseca, Y.A. (2016). Steganographic algorithm of private key on the domain of the cosine discrete transform. Revista Cubana de Ciencias Informáticas, 10(2). pp.116–131.

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

Velasco, C., López, J., Miyatake,M., and Pérez, H. (2007). Esteganografía en una imagen digital en el dominio dct. Científica, 11). pp. 169–176.