Original

Un algoritmo esteganográfico vinculado a los cuadrados mágicos

A steganographic algorithm linked to magic squares

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, Cuba,
asorial@udg.co.cu
Lic. Eduardo Moreno Roque, Profesor Asistente, Universidad de Granma, Cuba,
emorenor@udg.co.cu
Recibido: 12/10/2019 Aceptado: 13/11/2019

Resumen

El presente trabajo corresponde a la introducción de un novedoso algoritmo en la preparación de los estudiantes de la maestría, Matemática Aplicada de la Universidad de la Habana, correspondiente con el curso de Postgrado, “Esteganografía y Aplicaciones” , además a los miembros de MININT de la provincia de Guantánamo, se presenta un novedoso algoritmo esteganográfico vinculado al dominio espacial, el cual utiliza una clave privada de 128 bits juntamente con los cuadrados mágicos, con el propósito de ocultar información altamente clasificada, de forma tal, que la imagen resultante tras la inserción no sea perceptible ante cualquier sistema electrónico de monitoreo. El algoritmo propuesto, mejora en cuanto al nivel de imperceptibilidad analizado a través de los valores de PSNR; además, el mismo brinda un estego-sistema cuasi-perfecto y seguro reflejado en los valores conseguidos para la entropía relativa (Er).

Palabras clave: esteganografía; cuadrados mágicos; algoritmo asimétrico.

Abstract

The present work corresponds to the introduction of a new algorithm in the preparation of the students of the master's degree, Applied Mathematics of the University of Havana, corresponding to the Postgraduate course, "Steganography and Applications", in addition to the

MININT members of In the province of Guantanamo, a novel steganographic algorithm linked to the spatial domain is presented, which uses a 128-bit private key together with the magic squares, with the purpose of hiding highly classified information, so that the resulting image after the insertion is not noticeable to any electronic monitoring system. The proposed algorithm improves in the level of imperceptibility analyzed through the PSNR values; In addition, it provides a quasi-perfect and safe system-stego system reflected in the values achieved for relative entropy (Er). Put the summary in English

Keywords: steganography; magic squares; asymmetric algorithm

Introducción

La información es un recurso esencial, dado que cualquier información relevante para potenciar el desarrollo del país, conformar estados de opinión, o para conocer los puntos vulnerables del enemigo; se consideran de interés para la seguridad nacional (Soria, A., 2017; Soria, A., Moreno, E.R. y Centurión, A.M., 2015).

Hoy en día, la seguridad de la información es una preocupación constante por todos los usuarios de la red, y los piratas informáticos constituyen una amenaza para dicha seguridad, es por ello que para la transmisión de datos a través de los diferentes canales se necesitan técnicas de encriptación fuertes con el objetivo de garantizar la seguridad deseada (Sena, M.I. and Siva, A.P., 2016). Lo anterior llega a ser un asunto de vital importancia debido al incremento de Internet, existiendo la necesidad de alcanzar, por todos los medios, una protección adecuada de la información, evitando su uso, modificación, grabación o destrucción por usuarios no autorizados, o personas mal intencionadas (Soria, A., 2017; Soria, A., Moreno, E.R. y Centurión, A.M., 2015).

Una de las tecnologías de información y comunicación (TIC) que ha recibido la mayor atención en el último tiempo es Internet, que es más que una plataforma tecnológica para el intercambio de información. Más específicamente, consiste en una tecno-estructura cultural comunicativa, que permite la re-significación de las experiencias, del conocimiento y de las prácticas de interacción humana (Cabrera, J., 2004).

La Internet aparte de ser un medio de comunicación eficiente es también una herramienta para que la información se vuelva vulnerable a cualquier ataque. Sin embargo, la gran cantidad de

información transmitida permite ver un escenario en donde surge la necesidad de crear sofisticadas técnicas para proteger la información (Soria Lorente, et al., 2014).

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 los métodos y procedimientos que garanticen la protección de la información, con elevados índices de invulnerabilidad. El campo de las nuevas tecnologías de la información y las comunicaciones, proporciona un espacio apropiado para diseñar y elaborar sistemas que posibiliten una seguridad de la información (Soria, A., Moreno, E.R. y Centurión, A.M., 2015).

En la actualidad, todas las comunicaciones electrónicas están siendo continua y automáticamente monitoreadas por sistemas inteligentes que tienen un enorme poder de cómputo. En particular, toda trasmisión de texto cifrado va a llamar la atención de alguno de estos sistemas, y seguramente va a ser analizada. Resulta entonces interesante poder transmitir cierta información, usando medios electrónicos, que no llamen la “atención” de los sistemas automáticos de vigilancia, y que ofrezcan el nivel de servicio (privacidad, confidencialidad, autenticidad e integridad) ofrecidos por la esteganografía moderna (Soria, A., 2017; Soria, A., Moreno, E.R. y Centurión, A.M., 2015).

La esteganografía constituye un conjunto de técnicas las cuales permiten ocultar o camuflar cualquier tipo de datos dentro de información considerada como válida (Soria, A., 2017; Soria, A., Moreno, E.R. y Centurión, A.M., 2015; Biswasa, S. et al., 2012). Además, la misma permite burlar la vigilancia electrónica en el Internet, o simplemente que terceras personas no tengan acceso a información no autorizada. La esteganografía utiliza medios digitales, tales como archivos de texto, audio, imagen (Soria, A., 2017; Soria, A., Moreno, E.R. y Centurión, A.M., 2015; Biswasa, S. et al., 2012; Liao, X., Wena, Q. andZhang, J., 2011) y video (Soria, A., Moreno, E.R. y Centurión, A.M., 2015; Carvajal, B. E. et al., 2009; Cetin, O. and Ozcerit, A. T., 2009), que son utilizados como el archivo de transporte para ocultar la información, a este medio se le conoce como contenedor o cubierta.

Cuando el mensaje secreto es ocultado en una cubierta mediante una técnica esteganográfica se obtiene un esteganograma que contendrá el mensaje oculto dentro de dicha cubierta.

La esteganografía se ha convertido en la técnica más segura y confiable en el mundo de las comunicaciones, se enfrenta con tres retos diferentes: imperceptibilidad, robustez y capacidad. La Imperceptibilidad se refiere a encubrir los datos de modo tal que no puedan ser detectados, la robustez se encarga de impedir se puedan recuperar los datos secretos, así como no puedan ser capaces de detectar la existencia de estos (Biswajita, D. et al., 2016; Dunbar B., 2002) y la capacidad permite incorporar datos sin inconvenientes (Biswajita, D. et al., 2016; Artz D., 2001). Aunque los tres están estrechamente relacionados, ninguno debe obstaculizar al otro (Biswajita, D. et al., 2016).

Las razones para el uso de la esteganografía pueden ser muy variadas pero pueden aparecer porque no existe soporte para encriptar los datos o porque existe una autoridad que no permite el paso de cierta información. Así, la información transita en los ficheros sin que nadie sepa lo que realmente transporta en su interior.

El presente artículo tiene como propósito aplicar un algoritmo esteganográfico vinculado a los cuadrados mágicos para ocultar información altamente clasificada, de forma tal, que la imagen tras la inserción no sea perceptible ante cualquier sistema electrónico de monitoreo.

Los cuadrados mágicos son ordenaciones de números en celdas formando un cuadrado, de tal modo que la suma de cada una de sus filas, de cada una de sus columnas y de cada una de sus diagonales dé el mismo resultado. Usualmente los números empleados para rellenar las casillas son consecutivos, de 1 a n^2, siendo n el número de columnas y filas del cuadrado mágico. El mérito y gracia del juego está en su insospechada dificultad. Al sumar los números de cualquier renglón, cualquier columna o cualquiera de las dos diagonales el resultado es el mismo, a este número se le llama constante mágica.

Por ser tres los pares de filas (n/2), la suma será: $M_n = \frac{n(n^2+1)}{2}$, cantidad que se denomina constante mágica.

Orden *n*	3	4	5	6	7	**8**	9	10	11	12	13
$M_2(n)$	15	34	65	111	175	**260**	369	505	671	870	1105

En términos generales, se trata de una construcción formada por un cuadrado dividido en un número igual de casillas por lado, que contienen números naturales consecutivos, comenzando

por el 1, ordenados de tal forma que la suma de los números que aparecen en las casillas de cada una de las líneas horizontales es constante e igual a la suma de las casillas verticales, así como a la de las dos diagonales principales. Dicha suma recibe el nombre de suma mágica o constante mágica y se representa habitualmente por Mn. Los cuadrados mágicos se distinguen por su número de orden (n), que viene dado por el número de casillas por lado. Generalmente se emplean los primeros números enteros que corresponden a n^2, siendo la suma de estos números: n^2 (n^2+ 1) / 2. La suma de todas las filas, todas las columnas y las dos diagonales principales será: Mn =n (n^2+1) / 2 (Comes, M y Comes, R., 2004).

Por su importancia se utiliza un cuadrado mágico de 8x8, en el cual se acomodan todos los números del 1al 64 de manera que la constante mágica sea 260.

En general, los métodos en el dominio espacial tienden a proporcionar mayor capacidad de inserción que los métodos en el dominio de la frecuencia. Precisamente, este artículo presenta un nuevo algoritmo esteganográfico en el dominio espacial. A diferencia de otros trabajos (Soria, A., 2017), el mismo utiliza una clave privada de 128 bits, a partir de la cual se genera una secuencia pseudoaleatoria, que luego indica aquellos píxeles de la imagen donde serán insertados los elementos de la secuencia binaria del mensaje secreto, utilizando un cuadrado mágico de 8x8.

Este nuevo algoritmo proporciona una mayor protección y seguridad de la información que transita dentro del esteganograma, puesto que utiliza una clave privada, la cual es intercambiable por el emisor y el receptor haciendo uso de los cuadrados mágicos, puesto que solamente la combinación de la clave y del cuadrado mágico proveen el resultado deseado.

Se pretende mostrar los principales impactos provocados por la aplicación de un algoritmo esteganográfico vinculado a los cuadrados mágicos para la seguridad y protección de la información. A partir de la insuficiente seguridad y privacidad de la información al transitar a través de disímiles canales en la red.

Es por ello que se elabora un algoritmo esteganográfico vinculado a los cuadrados mágicos para ocultar información dentro de imágenes y así garantizar la seguridad y privacidad de la información al transitar a través de disímiles canales en la red.

Se logra la solución a un problema práctico que permite la seguridad y privacidad de la información y que puede ser utilizado con fines secretos para la Seguridad Nacional, como la que demanda la situación político-militar que vive hoy Cuba.

Población y muestra

El trabajo que se presenta fue elaborado para los estudiantes de la maestría, Matemática Aplicada de la Universidad de la Habana, correspondiente con el curso de Postgrado, "Esteganografía y Aplicaciones" , además a los miembros de MININT de la provincia de Guantánamo.

Materiales y Métodos

Teórico:

- Análisis y síntesis para la determinación de los fundamentos teóricos y metodológicos.
- Hipótesis-Deducción para el planteamiento de hipótesis. Deducciones de conclusiones a partir de conocimientos previos. Verificación

Empírico, la Observación Científica

Estadístico, la utilización del MatLab ® 7.14

Análisis y discusión

Descripción del algoritmo esteganográfico utilizando cuadrados mágicos.

Proceso de inserción

1.- Solicitar una clave privada de 128 bits al emisor.

2.- Segmentar la imagen-cubierta en bloques de 8*8 píxeles. Cabe notar que se trabajará con imágenes RGB de 24 bits, las cuales por cada píxel tienen 3 bytes, es decir, un byte para cada plano, por tal motivo, un bloque de 8*8 píxeles y equivale a 3 matrices cuadradas de orden 8. Sea M_j^i, donde i el j-ésimo elemento de la i-ésima matriz de orden 8, con i = 1;…; r, y j = 1;….; 64.

3.- Utilizar el cuadrado mágico de 8x8, que al tener dos propiedades muy importantes, una de ella es que al sumar los números de cualquier renglón, cualquier columna o cualquiera de las dos diagonales el resultado es el mismo, por ser tres los pares de filas (n/2), la suma será: $M_n = \frac{n(n^2+1)}{2}$, y la otra es que todos los números tienen una secuencia pseudoaleatoria), se desconoce cuáles son los números de cada celda.

84	**77**	**95**	**102**	**75**	**48**	**128**	**7**
42	**43**	**19**	**109**	**112**	**59**	**8**	**123**

14	**115**	**2**	**4**	**83**	**11**	**50**	**63**
80	**101**	**119**	**41**	**92**	**120**	**121**	**17**
122	**62**	**30**	**94**	**71**	**117**	**124**	**93**
88	**40**	**114**	**33**	**74**	**97**	**52**	**22**
108	**27**	**24**	**68**	**110**	**113**	**78**	**73**
28	**23**	**70**	**5**	**87**	**67**	**34**	**105**
45	**9**	**65**	**21**	**79**	**10**	**99**	**53**
32	**13**	**104**	**29**	**35**	**51**	**64**	**81**
49	**100**	**90**	**47**	**55**	**69**	**127**	**125**
57	**25**	**44**	**98**	**60**	**91**	**15**	**39**
38	**111**	**58**	**20**	**61**	**12**	**37**	**54**
107	**82**	**31**	**89**	**103**	**1**	**85**	**3**

Denotar por N_j , el j -ésimo elemento del siguiente cuadrado mágico y por p_j, el j -ésimo elemento de la secuencia binaria de la clave secreta, siendo j = 1;…; 128.

4.- Insertar el *k*-ésimo elemento de la secuencia binaria del mensaje secreto en el bit menos significativo del *j*-ésimo elemento $M_i^{N_j}$ de la *i*-ésima matriz de orden 8, siempre y cuando el correspondiente N_j-ésimo elemento pn_j de la secuencia binaria de la clave secreta sea igual a 1.

Proceso de extracción

El proceso de extracción se realiza del siguiente modo: el receptor debe conocer la clave privada y al mismo tiempo debe poseer el cuadrado mágico, mediante las cuales el emisor ocultó el mensaje secreto en la imagen original, además de la longitud de la secuencia binaria de dicho mensaje. Luego, se debe efectuar el mismo procedimiento realizado en el proceso de inserción, salvo en el paso 7, en el que se debe extraer el bit menos significativo del *j*-ésimo elemento M_i^j de la *i*-ésima matriz de orden 8 del esteganograma, siempre y cuando el correspondiente *j*-ésimo elemento s_i^j del *i*-ésimo bloque resultante del paso 5 sea igual a 1.

Validación del algoritmo propuesto

Para el análisis experimental se estudiaron 5 imágenes RGB de 24 bits, se escogieron 50 claves de 128 bits diferentes al azar.

En esta sección se presentarán las evaluaciones y resultados del algoritmo esteganográfico propuesto y el análisis de las ventajas con respecto a otros algoritmos de clave privada

presentado en (Soria, A., 2017). Para ello se implementó la aplicación en MatLab ® 7.14 (MathWorks, 2012), STEGLAB 1.0 (no registrado), la que permite calcular las magnitudes que más adelante se expondrán.

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 levantarse ninguna sospecha. Por tanto, el grado de distorsión o imperceptibilidad de un esteganograma respecto a la imagen original juega un papel fundamental.

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

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

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), propuso una medida que cuantifica la seguridad del sistema esteganográfico llamada -seguro, la cual viene dada mediante la expresión

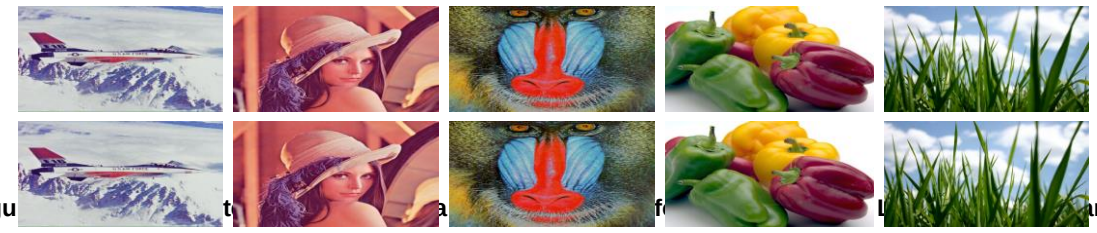
$$\text{ER}(P_C||P_E) = \sum P_C \left|\log\frac{P_C}{P_E}\right| \leq \epsilon,$$

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, expuestos en la Figura 1.

Como se podrá observar en lo que sigue, para el algoritmo propuesto, la imagen original y el esteganograma no muestran diferencias notorias. Además, el nivel de imperceptibilidad de los esteganogramas generados a partir de dicho algoritmo, mejora cuantitativamente respecto al conseguido en (Soria, A., 2017); y esto es comprobable, a través de los correspondientes PSNR, así como mediante los coeficientes de correlación por pares de histogramas del esteganograma y la imagen que sirve de cubierta, determinados en cada uno de los experimentos realizados.



Figu t a f L rriba representan las originales o cubiertas mientras que las de abajo son las estego-imágenes.

Para el desarrollo del primer experimento se abrió la imagen Lenna en la aplicación STEGLAB 1.0. Luego, haciendo uso de cinco claves privadas de 128 bits, diferentes, se ocultó a partir del algoritmo propuesto en (Soria, A., 2017), el siguiente mensaje secreto “Gauss fue un niño prodigio, a pesar de su condición de ser de una familia campesina de padres analfabetos; de él existen muchas anécdotas acerca de su asombrosa precocidad.

Hizo sus primeros grandes descubrimientos mientras era apenas un adolescente en el bachillerato y completó su magnum opus, Disquisitiones arithmeticae a los veintiún años (1798), aunque fue publicado en 1801”, obteniéndose de este modo cinco esteganogramas diferentes. Posteriormente, utilizando la misma imagen, se insertó el mensaje secreto haciendo uso del algoritmo, utilizándose nuevas claves privadas juntamente con cinco cuadrados mágicos diferentes de 128 bits, obteniéndose de este modo cinco nuevos esteganogramas, para los

cuales se calcularon los PSNR, los coeficientes de correlación por pares histograma (Rr,Rg,Rb) y la entropía relativa(Err,Erg,Erb).

Como se puede observar, los valores de los PSNR obtenidos a partir del algoritmo propuesto, aumentaron para cada una de las claves privadas y cuadrados mágicos, con respecto al algoritmo presentado en (Soria, A., 2017), lo que evidenció un mayor grado de imperceptibilidad respecto al resultado alcanzado en (Soria, A., 2017); además, los valores de los coeficientes de correlación en cada uno de los planos son muy cercanos a uno, lo cual se corresponde con los valores de los PSNR así como con la incuestionable semejanza existente entre los histogramas de la imagen cubierta y el esteganograma, véase la Figura 2. De las cinco imágenes las que mejores resultados obtuvieron en cuanto a imperceptibilidad y seguridad fueron la Mandril y Lenna, seguido de View.

Por otra parte, los valores de la entropía relativa, para cada plano, aumentaron levemente con respecto al resultado alcanzado en (Soria, A., 2017), 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.

En el segundo experimento, se utilizó la misma aplicación y se calcularon las magnitudes del experimento anterior para las cuatro imágenes de la Figura 1, cada una con dimensiones 1120 x 784.

En la Figura 2, se muestran los valores de las magnitudes calculadas. Para cada una de las imágenes utilizadas se observó un incremento de los PSNR de acuerdo con el modelo propuesto, mucho más acentuado en las imágenes Mandril y Lenna, véase la Figura 3, lo cual puede estar relacionado con la diferente ubicación de la información secreta cuando se usó la clave privada, es decir, en los esteganogramas de Mandril y Lenna quedó ocultado el mensaje secreto con un mayor grado de imperceptibilidad con respecto al resto, por lo que quedó demostrado que existe cierta influencia de las cubiertas en este proceso.

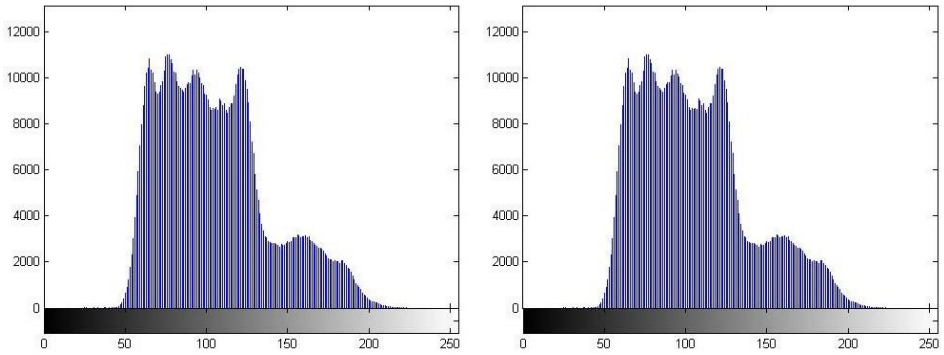


Figura 2: La imagen de la izquierda representa el histograma del tercer plano de la imagen cubierta Lenna y la imagen de la derecha representa el histograma del tercer plano del esteganograma Lenna.

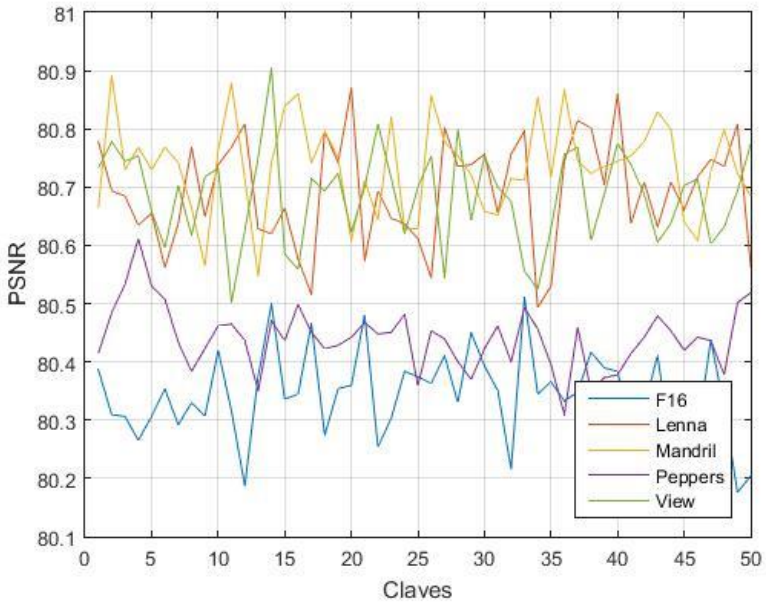


Figura 3: Gráfico comparativo de los PSNR, Lenna, Mandril, Peppers y View con dimensiones 1120 x 784 cada una, determinados para ambos algoritmos.

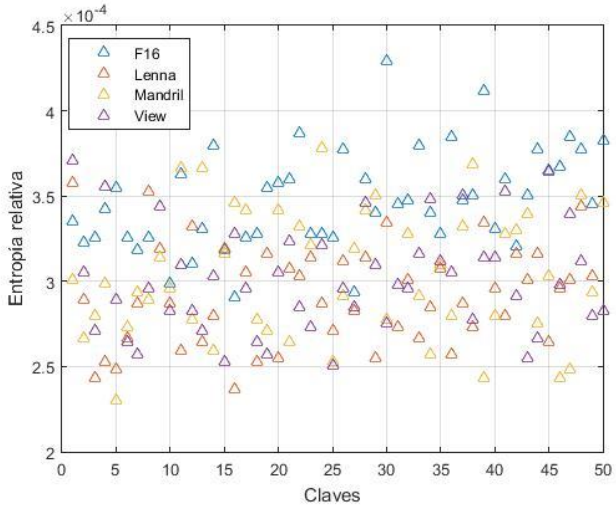


Figura 4: Gráfico comparativo de los PSNR, Lenna, Mandril, y View con dimensiones 1120 x 784 cada una, determinados para ambos algoritmos.

Impacto:

De los resultados del algoritmo el impacto logrado es metodológico, pues el mismo se inserta en la disciplina de PPD como un instrumento que puede ser utilizado en la preparación de los estudiantes para casos excepcionales de la Defensa, así como en la preparación de los estudiantes de la maestría Matemática Aplicada donde se se imparta Esteganografía, además a los miembros de MININT.

Conclusiones

En este trabajo se ha presentado un nuevo 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 luego indica aquellos píxeles de la imagen donde serán insertados los elementos de la secuencia binaria del mensaje secreto.

De acuerdo con los análisis de PSNR, de histogramas y de los valores de los coeficientes de correlación por pares, quedó demostrado que no existen anomalías detectables a simple vista, en el esteganograma con respecto a la cubierta.

Los valores obtenidos para la entropía relativa en cada uno de los planos, revelan que el sistema esteganográfico conseguido a partir del algoritmo propuesto, es suficientemente seguro.

Sirve de herramienta para la preparación de los estudiantes de maestrías de Matemática Aplicada donde se imparta Esteganografía, además se inserta en la disciplina de Preparación

para la Defensa como un instrumento que puede ser utilizado en la preparación de los estudiantes para casos excepcionales de la Defensa.

Referencias Bibliográficas

A. Soria Lorente. ”Implicaciones Sociales de la Criptografía y la Esteganografía “, 2017.

A. Soria Lorente, E.R Moreno Roque y A.M. Centurión Fajardo. “Algoritmo esteganográfico pseudo-asimétrico con claves de 128 bits”. XI Taller metodológico Patriótico Militar, 2015.

A. Soria Lorente, R. Mecías Hechavarría, A.A. Pérez Espinosa D. Rodríguez Díaz “Algoritmo esteganográfico pseudo-asimétrico (Pseudo-asymmetric steganography algorithm)”. Lecturas Matemáticas, vol. 35 (2) pp. 183–196, 2014.

1. D. Biswasa, S. Biswasb, A. Majumdera, D. Sarkara, D. Sinhaa, A. Chowdhurya, S. K. Dasa, “Digital Image Steganography using Dithering Technique”, Procedia Technology, Vol. 4, pp. 251–255, 2012.
2. Mercè Comes y Rosa Comes. “Los cuadrados mágicos matemáticos en andalus. el tratado de Azarquiel”. Universidad de Barcelona, 2004.
3. Cabrera, José. Navigators and castaways in cyberspace: psychosocial experience and cultural practices in school children’s appropriation of the Internet”. En: m. bonilla; g. cliché (eds.). Internet and Society in Latin America and the Caribbean, pp. 21-86. [Versión electrónica]. Ontario: Southbound / IDRC Books. Fecha de consulta: 30/03/07, 2004.
4. Biswajita Datta, Upasana Mukherjee, Samir Kumar Bandyopadhyay.” LSB Layer Independent Robust Steganography using Binary Addition” Procedia Computer Science 85, pp. 425 – 432, 2016.
5. Dunbar B. Steganographic techniques and their use in an Open-Systems environment. SANS Institute; January 2002.
6. Artz D. Digital Steganography: Hiding Data within Data. IEEE Internet Computing Journal; June 2001

7. X. Liao, Q. Wena& J. Zhang, A steganographic method for digital images with fourpixel differencing and modified LSB substitution, J. Vis. Commun. Image R., Vol. 22 , pp. 1–8, 2011.

B. E. Carvajal-Gámez, M. Acevedo & J. L. López-Bonilla, Técnica Esteganográfica para ocultar un video dentro de otro utilizando la Transformada Wavelet Discreta, JVR, Vol. 4, No. 2, pp. 54–61, 2009.

8. O. Cetin and A. T. Ozcerit, A new steganography algorithm based on color histograms for data embedding into raw video streams, Computers & Security, Vol. 28, pp. 670 – 682, 2009.

9. Sena Reddy, M.I,. Siva Kumar, A.P, “Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm”, Procedia Computer Science 85, pp. 62 – 69, 2016