Lecturas Matemáticas
Volumen **35** *(2) (2014), páginas 183–196*
ISSN 0120–1980

Algoritmo esteganográfico pseudo-asimétrico

Pseudo-asymmetric steganography algorithm

A. Soria–Lorente, R. Mecías–Hechavarría, A. A. Pérez–Espinosa & D. Rodríguez–Díaz
Universidad de Granma, Cuba

Resumen. En este artículo se presenta un nuevo algoritmo esteganográfico, vinculado al dominio espacial, el cual utiliza una clave privada y otra pública, las que permiten generar una secuencia binaria pseudoaleatoria, indicando así los píxeles de la imagen donde serán insertados los elementos de la secuencia binaria del mensaje secreto. El algoritmo propuesto, mejora en cuanto al nivel de imperceptibilidad analizado a través de los valores de PSNR, entropía relativa (Er) y coeficientes de correlación por pares de histogramas (R) del esteganograma y la imagen que sirve de cubierta, en comparación con los resultados de métodos propuestos por algunos autores.

Key words and phrases. Steganography, steganogram, cryptography.

Abstract. In this paper a new steganographic algorithm connected to the spacial domain is presented, which uses a private key and another public, that they permit generating a binary pseudo-random sequence, indicating thus the pixels of the image where the elements of the binary sequence of the secret message will be inserted. The proposed algorithm, improves to the level of imperceptibility analyzed through the values of PSNR, relative entropy (Er) and correlation coefficients for pairs of histograms (R) of the steganogram and the cover image, in comparison to the results of methods proposed by some authors.

2010 AMS Mathematics Subject Classification. 94A60, 11T71, 14G50.

1. Introducción

Con el rápido crecimiento de las tecnologías de la información y las telecomunicaciones, se han incrementado cada vez más las zonas vulnerables para

una empresa y sus datos. Todos los documentos de una empresa necesitan una protección fiable para mantener su privacidad, autenticidad, integridad y confidencialidad. 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. Por tales motivos el uso de la criptografía y la esteganografía juega un papel significativo en la sociedad para la seguridad y protección de la información.

La criptografía es la ciencia de proteger y custodiar la información digital de forma segura mediante técnicas de cifrado, la misma procede del término derivado de la palabra griega *kryptos*, que significa «escondido». El objetivo de la criptografía no es ocultar la existencia de un mensaje, sino más bien ocultar su significado, un proceso que se conoce como codificación. Para hacer que el mensaje sea ininteligible se codifica siguiendo un protocolo específico, sobre el cual se han puesto de acuerdo de antemano el emisor y el receptor a quien va dirigido. De esta forma, dicho receptor puede invertir el protocolo codificador y hacer que el mensaje sea comprensible. La ventaja de la criptografía es que si el enemigo intercepta un mensaje cifrado, éste es ilegible. Sin conocer el protocolo codificador, al enemigo le resultaría difícil, cuando no imposible, recrear el mensaje original a partir del texto cifrado [11, 14].

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 [1]. 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 [8], imagen [2, 9] y vídeo [5, 6], 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. Luego, una vez que los datos han sido ocultados, la información puede ser transferida a través de los medios de comunicación inseguros.

No hay que confundir la criptografía con la esteganografía: la primera modifica los datos para hacerlos incomprensibles, mientras que la segunda simplemente los oculta entre otros datos. A pesar del diferente enfoque de cada una, en muchas ocasiones se combinan ambas técnicas para lograr mejores resultados [7, 10, 13, 16]. 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.

Entre las técnicas más usadas en la esteganografía se encuentran las correspondientes al dominio espacial. 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 [1, 9, 12]. Otra de las técnicas dentro de la esteganografía tiene que ver con el dominio de la frecuencia, 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 [1]. Dentro de esta técnica se utilizan transformadas tales como la de Fourier, la transformada discreta de los cosenos [10, 17] y la de *wavelets* ¿óndulas?) [4, 5, 15].

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 [1, 7], el mismo utiliza dos claves, una pública y otra privada, en vez de una única clave simétrica, 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. Este nuevo algoritmo proporciona una mayor protección y seguridad de la información que transita dentro del esteganograma, puesto que además de utilizar una clave privada, la cual es intercambiable por el emisor y el receptor haciendo uso de la criptografía asimétrica, utiliza una clave pública que sin ella es inútil conseguir la información secreta del esteganograma, puesto que solamente la combinación de ambas claves proveen el resultado deseado.

En la proxima sección se expondrá la descripción de dicho algoritmo y en la siguiente se mostrarán algunos de los experimentos que sirven para validar el resultado fundamental de este artículo. Para finalizar se darán las conclusiones a las que se llegaron.

2. Descripción del algoritmo esteganográfico

Los algoritmos de llave pública, o algoritmos asimétricos, han demostrado su interés para ser empleados en redes de comunicación inseguras, su novedad fundamental con respecto a la criptografía simétrica es que las claves no son únicas, sino que forman pares.

Hasta la fecha han aparecido multitud de algoritmos asimétricos, la mayoría de los cuales son inseguros; otros son poco prácticos, bien sea porque el criptograma es considerablemente mayor que el mensaje original, o porque la longitud de la clave es enorme. Se basan en general en plantear al atacante problemas matemáticos difíciles de resolver.

En la práctica muy pocos algoritmos asimétricos son realmente útiles. El más popular, por su sencillez, es RSA [11], que ha sobrevivido a multitud de ataques.

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos si exceptuamos aquellos basados en curvas elípticas se recomiendan claves de al menos 1024 bits [11]. Además, la complejidad de cálculo que comportan estos últimos los hace considerablemente más lentos que los algoritmos de cifrado simétricos. En la práctica los métodos asimétricos se emplean únicamente para codificar la clave de sesión (simétrica) de cada mensaje o transacción particular.

En el algoritmo que más adelante se describe, se supone que tanto el emisor como el receptor poseen de antemano una misma clave privada, la cual de algún modo ha sido trasmitida haciendo uso de la criptografía asimétrica o de clave pública, específicamente el algoritmo RSA.

La dificultad del algoritmo RSA radica fundamentalmente en la complejidad que hoy en día existe para la factorización de grandes números. En particular, las claves pública y privada que utiliza dicho algoritmo, se calculan a partir de un número que se obtiene como producto de dos primos grandes. Por lo tanto, el atacante se enfrentará, si desea recuperar el mensaje secreto a partir del criptograma y la clave pública, a un problema de factorización [11].

Para generar el par de claves pública y privada en el algoritmo RSA, primeramente se deben elegir aleatoriamente dos números primos grandes, p y q y luego se debe calcular a $n = pq$. Inmediatamente, se debe elegir a un número $e \in \mathbb{Z}$ primo relativo con $\varphi(n) = (p-1)(q-1)$, tal que $1 < e < \varphi(n)$, dando lugar de este modo, a la clave pública representada mediante el par (e, n).

A continuación, mediante el algoritmo extendido de Euclides [11] se calcula el inverso de e en $\mathbb{Z}^*_{\varphi(n)} = \{1, \ldots, \varphi(n) - 1\}$, es decir, se determina el número $d \in \mathbb{Z}^*_{\varphi(n)}$, tal que $ed \equiv 1 \,(\text{mód}\, \varphi(n))$, dando lugar de este modo, a la clave privada representada mediante el par (d, n).

Ahora bien, si un emisor A desea enviar un mensaje m a un receptor B, se deben realizar los siguientes pasos:

1.- El emisor A debe conseguir la clave pública del receptor B, es decir, el par (e, n).
2.- El emisor A debe representar el mensaje m como un elemento de $\mathbb{Z}^*_n$.
3.- El emisor A debe enviar al receptor B el valor del criptograma $c \equiv m^e \,(\text{mód}\, n)$.

Luego, para recuperar el mensaje original m, el receptor B debe utilizar la clave privada (d, n) conseguida por él y proceder del siguiente modo:

$$c^d \,(\text{mód}\, n) \equiv (m^e)^d \,(\text{mód}\, n) \equiv m^{ed} \;\; (\text{mód}\, n) \equiv m.$$

2.1. Proceso de inserción.

1.- Solicitar una clave pública de 64 bits al emisor.

2.- Concatenar la clave privada y la pública del siguiente modo, formando así una nueva clave de 128 bits. El primer elemento de esta clave de 128 bits es el primer elemento de la privada y el segundo es el primero de la pública; el tercero es el segundo de la privada y el cuarto es el segundo de la pública y así sucesivamente.

3.- Calcular 15 subclaves.

3.1.- De cada uno de los 16 bytes de la clave generada en el paso 2. se elimina el octavo bit, el menos significativo. Para ello hay que realizar la siguiente permutación en la clave de 128 bits reduciéndose la misma a 112 bits.

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

El bit 1, el más significativo de la clave transformada, es el bit 84 de la clave original, el bit 2 pasa a ser el bit 77, etc....

3.2.- Dividir la clave permutada en dos mitades de 56 bits cada una, $c_1^{(1)}$ el bloque que contiene los 56 bits de mayor peso y $c_1^{(2)}$ los 56 bits restantes.

3.3.- Calcular las 15 sub-claves, comenzando a partir de $i = 1$.

3.3.1.- Rotar 1 o 2 bits a la izquierda de $c_i^{(1)}$ y $c_i^{(2)}$ para conseguir $\tilde{c}_i^{(1)}$ y $\tilde{c}_i^{(2)}$ respectivamente. El número de bits de desplazamiento está dado mediante $1 + \text{mód}\,(i-1, 2)$, $i = 1, ..., 15$. Hacer $c_{i+1}^{(1)} = \tilde{c}_i^{(1)}$ y $c_{i+1}^{(2)} = \tilde{c}_i^{(2)}$.

3.3.2.- Concatenar $\tilde{c}_i^{(1)}$ y $\tilde{c}_i^{(2)}$ y permutar el resultado mediante la siguiente compresión

52	101	57	10	47	55	32	77
112	91	62	20	105	110	25	82
35	67	95	11	49	79	84	43
30	42	80	27	9	8	75	23
85	13	48	70	22	44	68	71
92	87	3	63	99	17	37	94
88	14	109	93	1	90	74	58
102	111	24	107	59	31	73	45
65	81	98	19	69	40	51	34
33	7	97	78	15	5	61	53
64	28	4	41	50	89	83	100
104	12	29	21	54	2	38	103

De esta manera se obtiene la sub-clave C_i, que tiene una longitud de 96 bits.

3.3.3.- Regresar a 3.2.1., hasta que se haya calculado la última sub-clave C_{15}.

4.- Conseguir una secuencia binaria pseudoaleatoria cuya cantidad de bits iguales a 1 coincida con la longitud de la secuencia binaria del mensaje secreto. Para ello se deben seguir los siguientes pasos:

4.1.- Hacer $k = 1$.

4.1.1.- Aplicar la correspondiente expansión

87	94	77	77	61	46	90	62
24	29	16	8	69	41	87	10
4	14	77	83	52	70	44	86
48	14	67	42	27	39	79	5
20	1	36	30	81	27	58	11
51	9	14	19	64	37	7	43
56	68	57	57	87	38	59	95
63	74	12	7	93	91	50	60
71	87	53	33	84	2	92	5
47	77	89	27	32	3	85	78
4	77	77	5	4	96	4	76
25	77	22	73	54	45	26	82
65	77	57	15	88	80	6	5
75	66	49	23	7	7	40	18
5	28	17	77	87	57	35	27
7	5	31	55	13	34	21	72

a la secuencia binaria $C_k \oplus C_{k+1}$ extendiendo la misma a una secuencia binaria de 128 bits, donde $\oplus$ es la siguiente operación binaria ($0 \oplus 0 = 1 \oplus 1 = 0$ y $0 \oplus 1 = 1 \oplus 0 = 1$).

4.1.2.- Denotar por seq1 al resultado conseguido en 4.1.1.

4.1.3.- Extraer los bits menos significativos de cada unos de los bytes que componen la clave pública, consiguiendo de esta manera una secuencia binaria de 16 bits.

4.1.4.- Aplicar la operación del paso 4.1.1. entre cada uno de los 8 bloques de 16 bits de la secuencia de 128 bits conseguida en el paso 4.1.2. y la secuencia de 16 bits conseguida en el paso anterior. Luego, denotar la secuencia resultante de 128 bits mediante seq1.

4.2.- Mientras que la cantidad de bits iguales a 1 en la secuencia binaria seq1 sea menor a la longitud de la secuencia binaria del mensaje, proseguir.

4.2.1.- Si $k < 14$ entonces:

4.2.1.1.- Hacer $k = k + 1$.

4.2.1.2.- Aplicar la expansión del paso 4.1.1. a $C_k \oplus C_{k+1}$.

4.2.1.3.- Seguido, aplicar la operación del paso 4.1.1. entre cada uno de los 8 bloques de 16 bits de la secuencia de 128 bits conseguida en el paso anterior y la secuencia de 16 bits conseguida en el paso 4.1.3.

4.2.1.4.- Concatenar seq1 con la secuencia binaria resultante del paso anterior.

4.2.1.5.- Tomar seq1 como la secuencia binaria resultante del paso anterior.

4.2.2.- Si no se cumple la condición 4.2.1., entonces concatenar los 8 bytes intermedios de las sub-claves C_{14} y C_{15} formando así una nueva clave de 128 bits y luego a partir de la misma generar 15 sub-claves usando los pasos de 3. hasta 3.3.3.

4.2.2.1.- Luego, hacer $k = 1$.

4.2.2.2.- Aplicar los pasos 4.2.1.2. al 4.2.1.5.

4.2.2.3.- Proseguir de esta manera hasta que se cumpla la condición 4.2.

4.3.- Extraer la sub-secuencia binaria de seq1 partiendo de su primer bit, cuya cantidad de bits iguales a 1 sea exactamente la longitud de la secuencia binaria del mensaje secreto.

4.4.- Si la longitud de la secuencia binaria resultante del paso anterior no es divisible por 64, completar la misma con ceros hasta que se cumpla dicha condición.

4.5.- Tomar seq2 como la secuencia binaria resultante del paso anterior.

5.- Particionar la secuencia binaria resultante del paso 4.5. en r bloques de 64 bits. Sea s_i^j el j-ésimo elemento del i-ésimo bloque, con $i = 1, \ldots, r$, y $j = 1, \ldots, 64$.
6.- Segmentar la imagen-cubierta en bloques de $8x8$ píxeles. Cabe notar que en este artículo 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 $8x8$ píxeles equivale a 3 matrices cuadradas de orden 8. Sea M_i^j el j-ésimo elemento de la i-ésima matriz de orden 8, con $i = 1, \ldots, r$, y $j = 1, \ldots, 64$.
7.- Insertar el k-ésimo elemento de la secuencia binaria del mensaje secreto en el bit menos significativo del j-ésimo elemento M_i^j de la i-ésima matriz de orden 8, siempre y cuando el correspondiente j-ésimo elemento s_i^j del i-ésimo bloque resultante del paso 5. sea igual a 1. Aquí k no sólo representa la posición del k-ésimo elemento de la secuencia binaria del mensaje secreto, sino también, el k-ésimo elemento igual a 1 en la secuencia binaria resultante del paso 4.5.

2.2. Proceso de extracción. El proceso de extracción se realiza del siguiente modo: el receptor debe conocer la clave privada y al mismo tiempo poseer la pública, 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. donde 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.

Cabe destacar, que para el algoritmo propuesto, las claves pública y privada se toman de manera aleatoria. No obstante a esto, no se ve afectada la seguridad del esteganograma, puesto que dicho algoritmo funciona internamente como si fuese simétrico, donde ambas claves se combinan, formando una nueva clave de 128 bits, la cual se considera segura como ya se había explicado antes [11].

3. Validación del algoritmo propuesto

En esta sección se presentarán las evaluaciones y resultados del algoritmo esteganográfico propuesto y el análisis de las ventajas con respecto al algoritmo de clave privada presentado en [1]. 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 de 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

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

donde MSE está dado por el error cuadrático medio

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

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 [3], propuso una medida que cuantifica la seguridad del sistema esteganográfico llamada ϵ–seguro, la cual viene dada mediante la expresión

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

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 $\mathrm{ER}(P_C||P_E) = 0$, 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 se mide a través de un valor ϵ, para cualquier tipo de imagen [3].

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

Figura 1. Imágenes utilizadas en los experimentos; 1. Autumn, 2. Lenna, 3. Mandril, 4. Peppers; con dimensiones 1120 x 784 cada una.

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 [1]; 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.

Para el desarrollo del primer experimento se abrió la imagen Lenna en la aplicación STEGLAB 1.0. Luego, haciendo uso de cinco claves privadas diferentes se ocultó a partir del algoritmo propuesto en [1], 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 *opus magnum*, *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 propuesto en este artículo, utilizándose las mismas cinco claves privadas juntamente con cinco claves públicas diferentes, 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).

Los valores obtenidos de las magnitudes evaluadas, se muestran en la Tabla 1, mientras que en la Tabla 2 se presentan las claves utilizadas en este experimento. Como se puede observar, los valores de los PSNR obtenidos a partir del algoritmo propuesto, aumentaron para cada una de las claves públicas y privadas, con respecto al algoritmo presentado en [1], manteniendo para tal caso las mismas claves privadas, lo que evidenció un mayor grado de imperceptibilidad respecto al resultado alcanzado en [1]. 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 histograma de la imagen cubierta y el esteganograma, véase la Figura 2.

Por otra parte, los valores de la entropía relativa, para cada plano, aumentaron levemente con respecto al resultado alcanzado en [1], 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 Tabla 3, 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 Autumn y Peppers, 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 Autumn y Peppers 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.

Tabla 1. Valores de los PSNR, coeficientes de correlación y de entropía relativa para los dos algoritmos y la imagen cubierta Lenna (1120 x 784). El número 1 representa al algoritmo presentado en [1] mientras que el 2 representa al algoritmo propuesto en este artículo.

Algoritmo	PSNR	Rr	Rg	Rb	Err	Erg	Erb
✓1	80.4508	0.9999	0.9999	0.9999	0.0003	0.0002	0.0002
✓1	80.5103	0.9999	0.9999	0.9999	0.0003	0.0002	0.0002
✓1	80.5764	0.9999	0.9999	0.9999	0.0003	0.0003	0.0002
✓1	80.4734	0.9999	0.9999	0.9999	0.0004	0.0002	0.0002
✓1	80.4536	0.9999	0.9999	0.9999	0.0003	0.0003	0.0002
✓2	80.5735	0.9999	0.9999	0.9999	0.0004	0.0002	0.0002
✓2	80.5418	0.9999	0.9999	0.9999	0.0004	0.0003	0.0002
✓2	80.5909	0.9999	0.9999	0.9999	0.0004	0.0003	0.0003
✓2	80.4989	0.9999	0.9999	0.9999	0.0004	0.0004	0.0002
✓2	80.5132	0.9999	0.9999	0.9999	0.0003	0.0003	0.0002

Tabla 2. Claves privadas y públicas utilizadas en los dos algoritmos para la imagen cubierta Lenna (1120 x 784).

Algoritmo	Clave Privada	Clave Pública
✓1	Aslorent	—
✓1	OGZY:Tvy	—
✓1	Z_2{wX*a	—
✓1	;NX7L3Y$	—
✓1	”zH4YKRb	—
✓2	Aslorent	N;Fpr-Y7
✓2	OGZY:Tvy	q1RD_V3
✓2	Z_2{wX*a	gt57r5/(
✓2	;NX7L3Y$	KgaN78Yl
✓2	”zH4YKRb	_ZR]

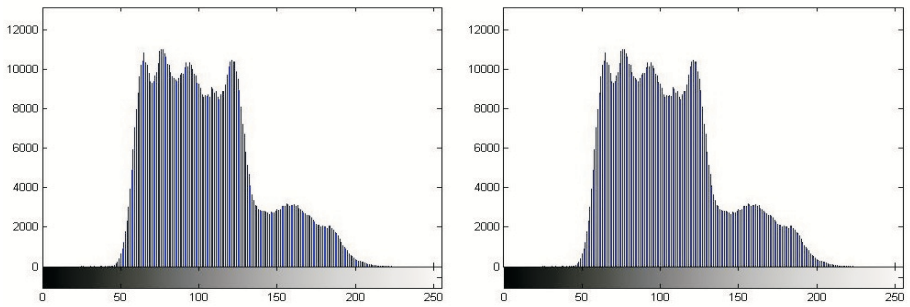

Figura 2. La imagen de la izquierda representa el histograma del tercer plano de la imagen cubierta Lenna y la imagen de la derecha representa el histograma del tercer plano del esteganograma Lenna.

Tabla 3. Valores de los PSNR, coeficientes de correlación y de entropía relativa para los dos algoritmos y las cuatro imágenes de la Figura 3. Para este experimento se utilizaron la clave privada Aslorent y la pública Ib./Bp*+.

Imágenes	PSNR	Rr	Rg	Rb	Err	Erg	Erb
✓Autumn_1	80.5735	0.9999	0.9999	0.9999	0.0005	0.0003	0.0002
✓Autumn_2	80.5793	0.9999	0.9999	0.9999	0.0003	0.0002	0.0003
✓Lenna_1	80.4508	0.9999	0.9999	0.9999	0.0003	0.0002	0.0002
✓Lenna_2	80.4961	0.9999	0.9999	0.9999	0.0004	0.0002	0.0002
✓Mandril_1	80.4621	0.9999	0.9999	0.9999	0.0002	0.0003	0.0002
✓Mandril_2	80.5103	0.9999	0.9999	0.9999	0.0003	0.0003	0.0003
✓Peppers_1	80.4621	0.9999	0.9999	0.9999	0.0001	0.0002	0.0002
✓Peppers_2	80.6789	0.9999	0.9999	0.9999	0.0001	0.0002	0.0001

4. Conclusiones

En este artículo, se ha presentado un nuevo algoritmo esteganográfico que utiliza dos claves, una pública y otra privada, 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. Además, 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.

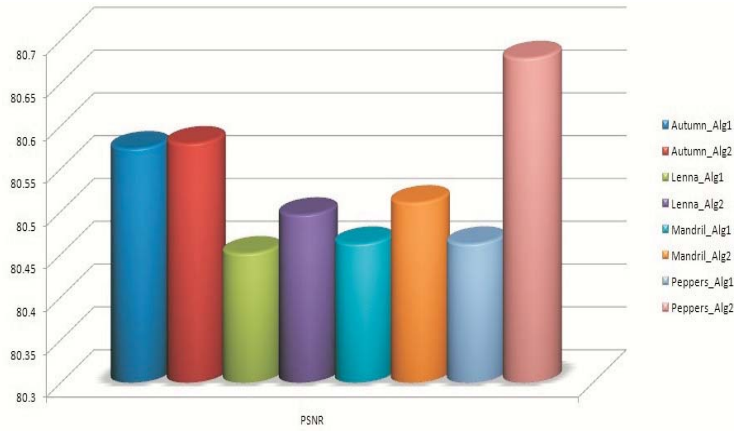

Figura 3. Gráfico comparativo de los PSNR correspondientes a las imágenes Autumn, Lenna, Mandril y Peppers con dimensiones 1120 x 784 cada una, determinados para ambos algoritmos.

Agradecimientos: Los autores expresan sus más sinceros agradecimientos a los árbitros por sus valiosas sugerencias. Agradecemos además, al proyecto ClaveMat, financiado por la unión Europea: `www.clavemat.com`.

Referencias

[1] A. Soria-Lorente, R. Manuel Sánchez & A. M. Ramírez Aberasturis, *Steganographic algorithm of private key*, Revista de investigación, G.I.E Pensamiento Matemático. **3** (2)(20139, 059–072.

[2] D. Biswasa, S. Biswasb, A. Majumdera, D. Sarkara, D. Sinhaa, A. Chowdhurya & S. K. Dasa. *Digital Image Steganography using Dithering Technique*. Procedia Technology **4** (2012), 251–255.

[3] C. Cachin. *An Information-Theoretic Model for Steganography*, Paper presented at the Proceedings of 2nd Workshop on Information Hiding, USA, 1998.

[4] B. E. Carvajal–Gámez, F. J. Gallegos–Funes & J. L. López–Bonilla. *Esteganografía para Imágenes RGB: Factor de Escalamiento*. JVR **4** (3) (2009), 66–77, 2009.

[5] B. E. Carvajal–Gámez, M. Acevedo & J. L. López–Bonilla. *Técnica Esteganográfica para ocultar un vídeo dentro de otro utilizando la Transformada Wavelet Discreta*. JVR **4** (2) (2009), 54–61.

[6] O. Cetin & A. T. Ozcerit. *A new steganography algorithm based on color histograms for data embedding into raw vídeo streams*. Computers & Security **28** (2009), 670–682.

[7] C. Chin-Chen, C. Tung-Shou Chen & C. Lou-Zo. *A steganographic method based upon JPEG and quantization table modification*. JVR **141** (2002), 123–138.

[8] S. Geetha, N. Ishwarya & N. Kamaraj. *Evolving decision tree rule based system for audio stego anomalies detection based on Hausdorff distance statistics*. Inform. Sci. **180** (2010), 2540–2559.

[9] X. Liao, Q. Wena & J. Zhan. *A steganographic method for digital images with four-pixel differencing and modified LSB substitution*. J. Vis. Commun. Image R. **22** (2011), 1–8.
[10] C. L. Liu & S. R. Liao. *High-performance JPEG steganography using complementary embedding strategy*. Pattern Recognition **41** (2008), 2945–2955.
[11] M. J. Lucena López. *Criptografía y seguridad en computadores*. Universidad de Jaén, Versión 4-0.7.51, 2008.
[12] D. Lou & C. Hu. *LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis*. Inform. Sci. **188** (2012), 346–358.
[13] W. Mei-Yi, H. Yu-Kun & L. Jia-Hong. *An iterative method of palette-based image steganography*. Pattern Recognition Letters **25** (2004), 301–309.
[14] G. Oded. *Foundations of Cryptography, Vol. 2*. Cambridge University Press. 2004.
[15] I. Orea–Flores, M.Acevedo & J. López–Bonilla. *Wavelet and Discrete Transform for Inserting Information into BMP Images*. Anziam Jour. **48** (1) (2006), 23–35.
[16] S. Songa, J. Zhangb, X. Liaoa, J. Dua & Q. Wena. *A Novel Secure Communication Protocol Combining Steganography and Cryptography*. Procedia Engineering **15** (2011), 2767–2772.
[17] K. Wonga, X. Qib & K. Tanaka. *A DCT-based (mod 4) steganographic method*. Signal Processing **87** (6) (2009), 1251–1263.

(Recibido en mayo de 2014. Aceptado para publicación en septiembre de 2014)

Anier Soria–Lorente
Aldo Pérez–Espinosa
Rubén Mecías–Hechevarría
Damayanis Rodríguez–Díaz
Departamento de Ciencias Básicas
Universidad de Granma
Bayamo, Cuba
e-mail: asorial@udg.co.cu
e-mail: aldo.perez@gr.mic.cu
e-mail: rmecias@trdcaribe.co.cu
e-mail: drodriguezd@udg.co.cu