UNIVERSIDAD NACIONAL DEL ALTIPLANO
REVISTA DE INVESTIGACIONES DE LA ESCUELA DE POSGRADO
Versión electrónica ISSN 2077 – 8686
Versión Impresa ISSN 1997-4035
ARTÍCULO ORIGINAL

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

ESTEGANOGRAFÍA EN IMÁGENES DIGITALES APLICANDO AUTÓMATAS CELULARES BIDIMENSIONALES COMO GENERADORES SEUDOALEATORIOS

ESGANOGRAPHY IN DIGITAL IMAGES APPLYING BIDIMENSIONAL CELLULAR AUTOMATICS AS SOUNDROAD GENERATORS

Iván Soria Solís[1], Carlos Castro Buleje[1], Hugo Calderón Vilca[2], Confesor Vargas Valverde[2], Samuel Pérez Quispe[2], Alejandro Apaza Tarqui[2]

[1]Universidad Nacional José María Arguedas, Facultad de Ingeniería de Sistemas, Jr. Juan Francisco Ramos N° 380, Ciudad Universitaria, Andahuaylas, Apurimac, isoria@unajma.edu.pe
[2]Universidad Nacional del Altiplano, Escuela de Posgrado. Av. Floral Nº 1153, Ciudad Universitaria, Puno, Perú.

RESÚMEN

La esteganografía permite codificar información dentro de archivos de imágenes u otros formatos aprovechando las limitaciones de los sentidos; sin embargo, existen técnicas de estegoanálisis que permiten detectar si una imagen ha sido alterada con esta técnica y a la vez existen múltiples técnicas de codificación. Por tanto, este es un campo en constante evolución. El presente estudio combina la esteganografía sobre imágenes digitales en formato PNG y en modo de color RGBA de 32 bits, utilizando la técnica del Bit Menos Significativo - LSB, con un generador de bits seudoaleatorio, implementado en base a un autómata celular bidimensional que genera secuencias de bits con apariencia de aleatoriedad. El autómata apropiado, según su regla de transición, se determinó mediante simulación para múltiples reglas por ser un modelo impredecible, las secuencias de bits generadas se evaluaron mediante las pruebas estadísticas de Relación de Señal a Ruido de Pico - PSNR y la Entropía Relativa de la estegoimagen. La entropía de las imágenes resultantes de la aplicación de ambas técnicas resultó ser similar a la entropía de las imágenes originales y en consecuencia son difícilmente detectables por las técnicas estadísticas de estegoanálisis incrementándose la seguridad de la codificación.

Palabras Clave: Autómata celular bidimensional, esteganografía, generador seudoaleatorio, LSB, PNG.

ABSTRACT

Steganography allows encoding information within image files or other formats exploiting the limitations of the senses, however, there steganalysis techniques that detect whether an image has been altered with this technique, yet there are multiple coding techniques. Therefore, this is a constantly evolving field. This study combines digital steganography of PNG images in color mode and 32-bit RGBA using the technique of LSB - LSB, a pseudo-random bit generator implemented based on a two-dimensional cellular automaton that generates sequences of bits with the appearance of randomness. The appropriate PLC by transition rule was determined by simulation for multiple rules to be an unpredictable pattern, generated bit sequences were evaluated by statistical tests Signal to Noise Pico - PSNR and the relative entropy estegoimagen. The entropy of the images resulting from the application of both techniques found to be similar to the entropy of the original images and thus are hardly detectable by statistical techniques steganalysis increase the encryption strength.

Keywords: Two-dimensional celular automaton, steganography, pseudorandom generator, LSB, PNG.

*Autor para Correspondencia: isoria@unajma.edu.pe,

UNIVERSIDAD NACIONAL DEL ALTIPLANO
REVISTA DE INVESTIGACIONES DE LA ESCUELA DE POSGRADO
Versión electrónica ISSN 2077 – 8686
Versión Impresa ISSN 1997-4035
ARTÍCULO ORIGINAL

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

INTRODUCCIÓN

Existen múltiples técnicas de ocultaciones de la información, pero estas tienen solamente un nivel de seguridad "probable", por lo que se necesita diseñar y construir nuevos métodos de ocultación de información. Los hackers están evolucionando constantemente, descubriendo nuevas técnicas de ataque y ampliando sus objetivos a nuevas tecnologías (Jhaveri, 2012).

La estenografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros llamados "portadores", de modo que no se perciba su existencia (Gutub, 2010). Es decir, se trata de ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal (Angulo, Ocampo, y Blandon, 2007).

La estenografía sobre imágenes es la técnica que trata de ocultar mensajes en archivos de imágenes por medio de un mapa de bits, cambiando el valor de algunos bits, los que menos afectan a la apariencia de la imagen (Steinmetz, Dittman, y Steinbach, 2000). Se debe tener en cuenta que el transporte de imágenes grandes por Internet puede despertar sospechas. (Angulo, Ocampo, y Blandon, 2007) por lo que se recurre a secuencias seudoaleatorias (Velasco *et al*., 2007). El estegoanálisis trata de descubrir y hacer los mensajes inútiles, por lo que pueden realizarse de varias formas (Onomza, Isah y Ochoche, 2012).

Un generador de bits seudoaleatorios es un algoritmo determinístico al que proporcionándole una sucesión binaria aleatoria de longitud k, produce una sucesión binaria que parece aleatoria (White y Hoya, 2002). Un autómata en su forma más simple es una línea unidimensional donde el color o estado cambia discretamente a través del tiempo. Los cambios son determinados en función de su estado anterior y de las celdas vecinas (Juarez, Zenill y Stephens, 2011). Tienen algunas características que pueden ser generalizadas a los autómatas n-dimensionales (Gonzales y Chaves, 2006). Las imágenes en formato PNG pueden ser de paleta indexada o estar formada por varios canales. El número de canales depende de si la imagen es en escala de grises o en color y si dispone de canal alfa o transparencia (Roelofs, 1999).

La aleatorización del mensaje antes de aplicar la técnica de la esteganografía, ha sido propuesta también en estudios previos (Kruss *et al*., 2003). Los generadores de bits basados en autómatas celulares unidimensionales se han estudiado ampliamente, pero su reversión es posible en tiempo polinomial por lo que no son seguros (Wolfram 1986). Estos pueden ser generalizados a dos dimensiones (Regnault, Schabanel y Thierry, 2009) y se puede utilizar claves para hacer este proceso más eficiente, escalable y correcto (Jakhar *et al.*, 2012). Aplicando las secuencias seudoaleatorias en la esteganografía se puede codificar de forma más eficaz y evaluar la calidad de la imagen resultante a partir de la entropía (Biswapati, y otros 2013) usando cualquiera de los métodos conocidos como LSB (Qazanfari y Safabakhsh, 2014), y en formatos con pérdida se utilizan técnicas tales como la transformada de onda entera (Thanikaiselvan, *et al.*, 2013) o una función módulo (Nagaraj, Vijayalakshmi, y Zayaraz, 2013). Las esteganografía en imágenes JPG es la más utilizada cuando se hace en formatos de imagen con pérdida (Song, Zhang, *et al.*, 2011). Los datos codificados se pueden guardar en uno o más de los canales de la imagen (Gutub, 2010) e incluso se utiliza algún canal para guardar información de otros canales que sí contienen datos codificados.

Esta investigación pretende responder a la pregunta: ¿es posible realizar esteganografía en imágenes digitales PNG con el método LSB (Bit menos significativo) aplicando autómatas celulares bidimensionales como generadores de secuencias de bits seudoaleatorias?. El objetivo

UNIVERSIDAD NACIONAL DEL ALTIPLANO
REVISTA DE INVESTIGACIONES DE LA ESCUELA DE POSGRADO
Versión electrónica ISSN 2077 – 8686
Versión Impresa ISSN 1997-4035
ARTÍCULO ORIGINAL

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

principal es implementar y analizar la esteganografía en imágenes digitales en formato PNG, utilizando la técnica del bit menos significativo y aplicando autómatas celulares bidimensionales como generadores de bits seudoaleatorios.

MATERIALES Y MÉTODOS

Para comprobar las posibilidades de los autómatas celulares bidimensionales como generadores seudoaleatorios se propuso un modelo de simulación computacional (Shannon y Johanes 1976) cuyo diseño se compone de las características siguientes:

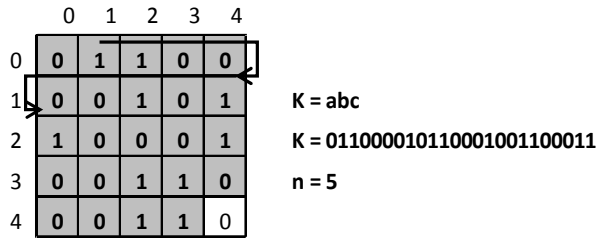

Figura 1. Látice para un autómata con clave de 24 bits

(Elaboración Propia)Una semilla o clave K

Un látice de tamaño $n \times n$ donde $n = e$ $(\sqrt{(L \quad d \quad K) * 8} + 1)$ que se inicializa con la semilla en orden de filas y columnas como se muestra en la Figura 1.

Vecindad de Moore

Regla de transición que se define asignando a cada una de las células vecinas un número correspondiente a una potencia de 2. Siendo $2^{\square}$ el valor dado a la célula central y a partir de ella a todos los vecinos en sentido horario. Lo que permite representar hasta 512 reglas. La muestra la actualización del estado de una célula para la Regla 88.

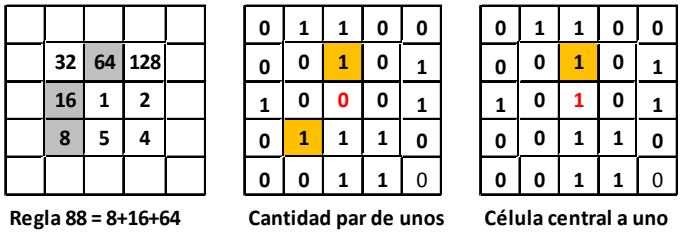

Figura 2. Actualización de los estados para la regla 88

El número total de reglas posibles a aplicar son $2^{\square} = 512$ se deben comprobar tomándose el bit correspondiente a la célula central del látice como el bit N-simo de la sucesión seudoaleatoria. Debido a que el generador se comporta como un flujo de bits indefinidamente largo se generaron $512x512 = 262144$ bits para asegurar una ventana lo bastante grande para los fines del estudio (Figura 2).

Estas secuencias deben satisfacer ciertas condiciones de aleatoriedad.

Prueba 1: Prueba de Medias

UNIVERSIDAD NACIONAL DEL ALTIPLANO
REVISTA DE INVESTIGACIONES DE LA ESCUELA DE POSGRADO
Versión electrónica ISSN 2077 – 8686
Versión Impresa ISSN 1997-4035
ARTÍCULO ORIGINAL

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

Se plantean las hipótesis de que la media $\bar{r} = 0.5$ (García, García y Cárdenas 2006). $H_0: \mu_{r_i} = 0.5$, $H_1: \mu_{r_i} \neq 0.5$

Se determina el promedio de los n elementos del conjunto r_i

$$\bar{r} = \frac{1}{n}\sum_{i=1}^{n} r_i \quad (1)$$

Los límites de aceptación superior e inferior en base a $n = 262144$ y con un nivel de aceptación de 95% con $\propto = 0.05$ para el que la probabilidad acumulada de la distribución normal estándar es $z_{\propto/2} = 0.9798$:

$$L_{\bar{r}} = \frac{1}{2} - z_{\propto/2}\left(\frac{1}{\sqrt{1\ n}}\right) \quad L_{\bar{r}} = 0.491 \quad (2)$$

$$L_{\bar{r}} = \frac{1}{2} + z_{\propto/2}\left(\frac{1}{\sqrt{1\ n}}\right) \quad L_{\bar{r}} = 0.509 \quad (3)$$

Las secuencias candidatas a seudoaleatorias que tengan una media dentro de los límites de aceptación no puede refutarse la hipótesis de que están uniformemente distribuidas. En otro caso, se descartarán por no demostrarse la uniformidad.

Prueba 2: Prueba de uniformidad. Chi-cuadrada

Se trata de una prueba de hipótesis a partir de datos, basada en un valor llamado estadístico de prueba, al cual se compara con un valor conocido como valor crítico. (García, García y Cárdenas 2006). El procedimiento general es el siguiente:

1. Obtener 30 o más datos de la variable aleatoria a analizar
2. Calcular la media y varianza de los datos.
3. Crear un histograma de $m = \sqrt{n}$ intervalos y obtener la frecuencia observada de cada intervalo O_i
4. Se determina el estadístico X_0^2 mediante la ecuación

$$X_0^2 = \sum_{i=1}^{m} \frac{(E_i - O_i)}{E_i} \quad (4)$$

Si el valor del estadístico X_0^2 es menor al valor de tablas de $X_{0.0\ ,1}^2$ entonces no se puede rechazar que le conjunto de números r_i sigue una distribución uniforme. Para el caso de estudio, por tratarse de sucesiones de 1 y 0 el valor de $X_{0.0\ ,1}^2 = 3.841$

Prueba 3: Prueba de corridas arriba y abajo

Busca determinar si un conjunto r_i es independiente para ello se plantean las hipótesis:

H_0: Los números del conjunto r_i son independientes

H_1: Los números del conjunto r_i no son independientes

Se determina el número de corridas observadas C_0. Luego se calcula el valor esperado, la varianza y el estadístico Z_0 mediante las ecuaciones:

$$\mu_{C_0} = \frac{2n-1}{3} \quad (5)$$

$$\sigma_{C_0}^2 = \frac{1\ n-2}{9} \quad (6)$$

UNIVERSIDAD NACIONAL DEL ALTIPLANO
REVISTA DE INVESTIGACIONES DE LA ESCUELA DE POSGRADO
Versión electrónica ISSN 2077 – 8686
Versión Impresa ISSN 1997-4035
ARTÍCULO ORIGINAL

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

$$Z_U = \left| \frac{C_C - \mu_{C_C}}{\sigma^2_{C_C}} \right| \quad (7)$$

Si Z_U es menor que el valor de la tabla normal estándar para $Z_{\alpha/2}$ no se puede rechazar que el conjunto de números es independiente. Para $\alpha = 0.05$, $Z_{\alpha/2} = 0.9798$

Luego de realizadas todas las pruebas se considerarán como reglas apropiadas aquellas que hayan generado todas sus secuencias de bits seudoaleatorias y que estas satisfagan las todas las pruebas realizadas. Estas reglas se utilizarán para realizar la esteganografía sobre las imágenes digitales.

Para medir la calidad de la imagen esteganográfica se utilizan medidas de calidad en relación al ruido y de desorden de los datos codificados.

Calidad (PSRN)

Se expresa en escala logarítmica y en dB. (Di Martino, y otros 2008). Para definirla se debe calcular el error cuadrático medio (M), que para dos imágenes monocromas I y K de tamaño $M \times N$ se define como:

$$M = \frac{1}{M} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \| I(i,j) - K(i,j) \|^2 \quad (7)$$

Así, el PSNR se define como:

$$P = 10 \cdot log_{10} \left(\frac{M \; I^2}{M} \right) = 20 . log_{10} \left(\frac{M \; I}{\sqrt{M}} \right) \quad (8)$$

Donde M $_I$ denota el máximo valor que puede tomar un píxel en la imagen. Cuando éstos se representan usando B bits por muestra, M $X_I = 2^B - 1$.

Para una imagen en formato RGB, la definición del P es la misma, pero el M se calcula como la media aritmética de los M s de los tres colores (Red, Green y Blue).

Los valores típicos que adopta este parámetro están entre 30 y 50 dB, siendo mayor cuanto mejor es la codificación.

Seguridad

Para probar la seguridad en el resultado de la imagen esteganográfica, se calculará la entropía de la imagen original y se comparará con la entropía de la imagen codificada. Para el cálculo de la entropía se utiliza la fórmula

$$H(X) = \sum_{i=1}^{n} p(x_i) \cdot log_2 \left(\frac{1}{p(x_i)} \right) \quad (9)$$

Esta se calcula para la imagen original y la imagen codificada para comparar la diferencia. Si la diferencia es cercana a cero, el sistema es seguro. (Wang *et al.*, 2002)

RESULTADOS Y DISCUSIÓN

El primer objetivo fue comprobar el comportamiento del autómata con diversas configuraciones. Teniendo en cuenta la longitud en bits de la clave, se calculó el número de iteraciones y el tiempo para generar una secuencia de 262144 bits, que se resume en la Tabla 1. En un procesador Intel Core i5 se comprueba que el tiempo de procesamiento crece proporcionalmente al número de iteraciones. El tiempo necesario para evolucionar el autómata se hace grande a medida que crece el tamaño de la clave y la cantidad de estados a evolucionar. Esto puede parecer ineficiente, pero

UNIVERSIDAD NACIONAL DEL ALTIPLANO
REVISTA DE INVESTIGACIONES DE LA ESCUELA DE POSGRADO
Versión electrónica ISSN 2077 – 8686
Versión Impresa ISSN 1997-4035
ARTÍCULO ORIGINAL

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

también es garantía de que la inversión del proceso es computacionalmente prohibitiva, lo cual es ideal para el objetivo que se busca en la seguridad del modelo planteado. (Jakhar *et al.*, 2012), consiguieron una orden de complejidad lineal, pero en autómatas celulares de una sola dimensión, más simples, sin considerar claves de tamaño variable como el esquema que se plantea y pone a prueba en este estudio.

En el esquema planteado en el presente estudio a mayor longitud de la clave el tiempo de procesamiento crece con un orden de complejidad $O(n^k)$ donde k es una constante. En la Figura 3, se muestran los tiempos de corrida para las claves comprobadas en la simulación.

Tabla 1. Resultado de las corridas del autómata

Longitud de clave	Iteraciones	Tiempo de procesamiento (en segundos)
8	2097152	2.228574991
25	6553600	8.220809937
81	21233664	28.32302094
144	37748736	62.47616196

Figura 3. Tiempo de corrida según longitud de clave

Una de las características relevantes para comprobar que el modelo propuesto es viable, fue comprobar que con el espacio de claves posibles el autómata no cayera en estados degenerados con únicamente ceros o únicamente unos. Esta situación es posible solo si la clave o semilla tiene predominancia de estos bits. Esta situación es difícil de producir por que la clave es ingresada primero en formato de caracteres ASCCII y es la representación en binario de estos que se utiliza como semilla en el látice.

Un caso donde existe poca población de bits con valor de 1 en el estado inicial se comprobó con la clave "@@@@" que debido a que el valor ASCCII de "@" es 64 o en binario 01000000 tiene escasos bits 1. El estado inicial y la secuencia de bits resultante en la evolución 128 de un autómata con esta configuración se muestra en la Figura 4, la regla aplicada es también un regla trivial (Regla 64)

UNIVERSIDAD NACIONAL DEL ALTIPLANO
REVISTA DE INVESTIGACIONES DE LA ESCUELA DE POSGRADO
Versión electrónica ISSN 2077 – 8686
Versión Impresa ISSN 1997-4035
ARTÍCULO ORIGINAL

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

a)

```
0 1 0 0 0 0
0 0 0 1 0 0
0 0 0 0 0 1
0 0 0 0 0 0
0 1 0 0 0 0
0 0 0 0 0 0
```

b)

```
1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0,
1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0,
1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0,
1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0,
1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0,
1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0,
1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0,
1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0
```

Figura 4. a) Estado inicial para la clave "@@@@". b) Secuencia de bits generada de longitud 128

Se puede apreciar a simple la generación de una secuencia evidentemente periódica. Esto se pone en evidencia luego con las pruebas de uniformidad e independencia y esta clave no satisface las condiciones de seudoaleatoriedad (Figura 4).

Análisis de las secuencias de bits seudoaleatorias

Luego de realizadas las corridas para las 255 reglas con cuatro tamaños representativos de claves se aplicaron las pruebas siguientes:

- P1: Prueba de Medias
- P2: Prueba Chi-cuadrado
- P3: Prueba de corridas

Las reglas que pasaron todas las pruebas con todas las configuraciones y claves se muestran en la Tabla 2. Se puede apreciar que ninguno de ellos pasó la prueba con la clave de 8 bits; y que a pesar de pasar con éxito las pruebas P1 y P2 que son pruebas de uniformidad, no logran pasar la prueba P3 que es la prueba de independencia. Esta situación se puede interpretar como la situación mostrada en la Figura 4 donde los bits generados se alternan pero de manera periódica.

Tabla 2. Reglas que pasaron las pruebas de uniformidad e independencia

Regla	Clave	P1	P2	P3
2	1	0.5001	0.0002	1.8749
	123	0.4999	0.0002	0.3747
	123456789	0.5001	0.0002	0.625
	Fibonacci_112358	0.5	0	0.9379
32	1	0.5	0	1.8749
	123	0.5001	0.0002	0.3747
	123456789	0.5	0	0.625
	Fibonacci_112358	0.4999	0.0002	0.9376
87	1	0.5	0	1.8749
	123	0.5001	0.0002	0.3747
	123456789	0.4999	0.0002	0.8032
	Fibonacci_112358	0.4999	0.0002	0.9371

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

117	1	0.5001	0.0002	1.8749
	123	0.4999	0.0002	0.3747
	123456789	0.4999	0.0002	0.6247
	Fibonacci_112358	0.5001	0.0002	0.9375
181	1	0.5	0	1.8753
	123	0.5001	0.0002	0.3747
	123456789	0.5	0	0.2672
	Fibonacci_112358	0.4999	0.0002	0.0002
196	1	0.5001	0.0002	1.8749
	123	0.5	0	0.3747
	123456789	0.4999	0.001	0.8039
	Fibonacci_112358	0.4999	0.001	0.0005
234	1	0.5	0	1.8753
	123	0.4999	0.0002	0.3752
	123456789	0.4999	0.0002	0.625
	Fibonacci_112358	0.4999	0.0002	0.0002
425	1	0.5	0	1.8753
	123	0.5	0	0.3752
	123456789	0.4999	0.0002	0.6247
	Fibonacci_112358	0.5001	0.0002	0.0002

Debido a que ninguna de las reglas superó la prueba de independencia P3 para la clave “1” de 8 bits se considera como reglas satisfactorias a las que pasaron las pruebas con las otras tres claves.

Aplicación de la esteganografía

Según lo propuesto en la metodología, se aplicó la esteganografía sobre 5 imágenes portadoras, elegidas por tener características distintas de color; complejidad que podrían afectar el resultado. Las imágenes elegidas tienen un tamaño de 128x128 bits, en formato PNG y con profundidad de color de 32 bits.

La técnica de LSB (bit menos significativo) permite reemplazar los bits menos significativos de cada canal de color, para el formato PNG en modo RGBA se pueden utilizar 4 canales por pixel. A más bits codificados por canal, también la pérdida de información y calidad de la imagen portadora se hace más notoria. En la figura 5 se aprecian los resultados de codificar un mensaje utilizando los bits LSB desde 1 hasta 8 bits. La pérdida es apreciable visualmente desde la codificación con 3 bits LSB. A medida que se utilizan más bits aparece ruido aleatorio que se puede percibir a simple vista.

En la imagen, se hace muy notorio en las zonas con un solo color predominante y en zonas con cambios suaves de color degradados. Esto se debe a que el ojo humano es más hábil detectando transiciones leves de color que cambios bruscos y con alto contraste.

UNIVERSIDAD NACIONAL DEL ALTIPLANO
REVISTA DE INVESTIGACIONES DE LA ESCUELA DE POSGRADO
Versión electrónica ISSN 2077 – 8686
Versión Impresa ISSN 1997-4035
ARTÍCULO ORIGINAL

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

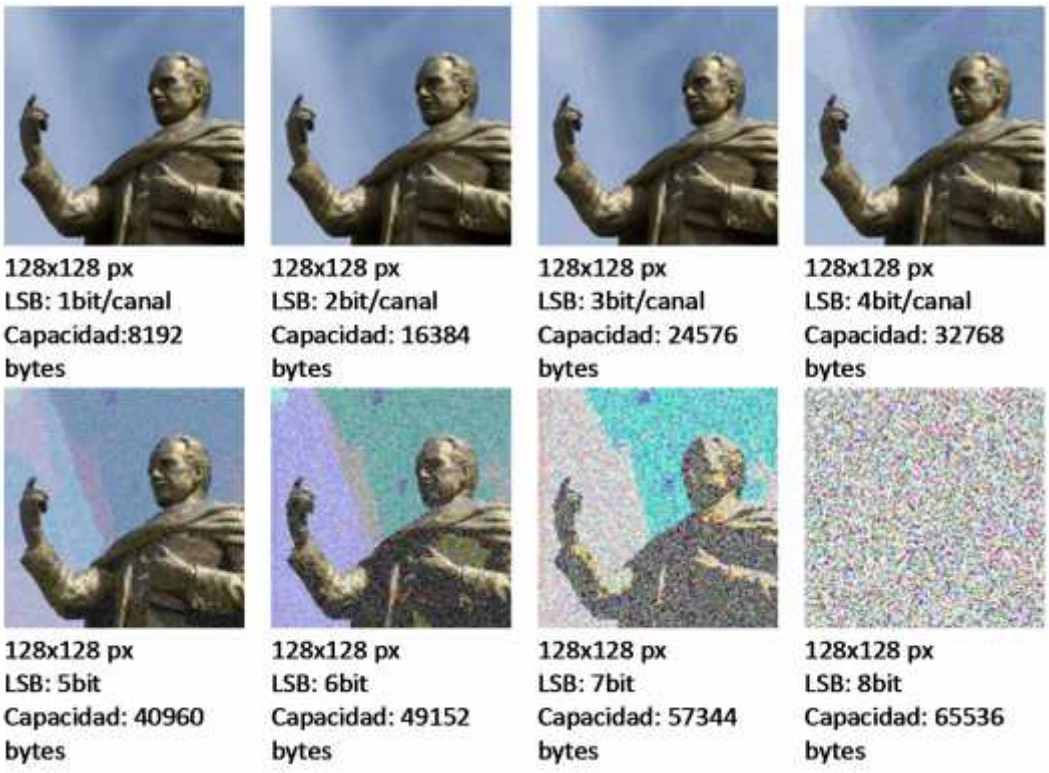

Figura 5. Capacidad de codificación de acuerdo a la cantidad de bits LSB

Los valores obtenidos para LSB de entre 1 a 8 bits para las imágenes de la muestra se presentan en la figura 5. Donde se puede apreciar que para valores de LSB menores o iguales a 4 bits, la calidad es buena para todas las imágenes.

Tabla 3. Valores de PSNR obtenidos para todas las imágenes

LSB	abeja.png	arguedas.png	bombilla.png	lenna.png	nieve.png
1	51.13342326	51.16529238	51.23650962	51.15570707	51.11612619
2	43.61560672	43.75046051	43.30066068	43.76195628	43.64235301
3	37.08905906	37.24125484	36.62774403	37.25414624	37.21336464
4	30.79678656	30.97054971	30.06637051	30.98696464	31.11931371
5	24.69153112	25.05821941	23.70699551	24.83756267	24.84423205
6	18.67979321	18.89067941	17.50581986	18.90187436	18.61245212
7	12.52113968	12.95245161	11.34142365	12.96699826	12.41760989
8	6.459759106	7.21943609	5.203180069	7.320903525	5.797859733

La disminución del PSNR es muy similar entre todas las imágenes estudiadas. Lo que evidencia que no depende de las propiedades o características inherentes a la imagen, sino que es un comportamiento normal y predecible en todos los casos (Biswapati *et al.*, 2013). consiguieron valores de PSNR de 62, lo cual es u resultado de alta calidad, pero utilizando solamente un bit por pixel de color en el canal verde; esto hace que la capacidad de codificación sea menor, es decir que se puede codificar mensajes mucho más cortos con la calidad esperada. En el presente

UNIVERSIDAD NACIONAL DEL ALTIPLANO
REVISTA DE INVESTIGACIONES DE LA ESCUELA DE POSGRADO
Versión electrónica ISSN 2077 – 8686
Versión Impresa ISSN 1997-4035
ARTÍCULO ORIGINAL

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

estudio también no se consigue un PSNR mayor a 60 pero se utilizan los cuatro canales: rojo, verde, azul, alfa. Lo cual otorga una capacidad de inserción cuatro veces superior aunque a costa de una menor calidad en la imagen esteganográfica resultante (Tabla 3).

Si se compara con los resultados obtenidos en (Nagaraj *et al.*, 2013), con valores de PSNR cercanos a 40 usando un solo bit menos significativo, los resultados obtenidos son mejores porque se ha conseguido valores de PSNR mayores a 40 no solo con un bit LSB sino con hasta 2 bits menos significativos, por lo que el esquema propuesto es de mejor calidad con el doble de datos codificados.

De forma similar a Gutub (2010), que aprovecha todos los canales en imágenes con profundidad de pixel de 24 bits RGB, aunque su métrica para evaluar la calidad del resultado es la desviación estándar, por lo que no puede ser comparada con el PSNR que mide el ruido. La desviación estándar es una medida adecuada de calidad, solo si se tiene a disposición la imagen original para comparar. En el presente estudio asumimos que la imagen original se encuentra a buen recaudo y el acceso a la misma es difícil, sino imposible para el atacante.

Para comprobar la seguridad de las imágenes esteganográficas resultantes se compara el valor de su entropía relativa con la entropía de la imagen en original. Aunque el original no debería estar disponible para un atacante, siempre existe la posibilidad de que sea obtenido por este. Para un sistema totalmente seguro esta diferencia se acerca a cero. Observamos que esta situación solamente ocurre con valores de LSB bajos y la diferencia va creciendo linealmente conforme se incrementa el valor de LSB. En algunas imágenes crece más rápidamente pero siempre en forma lineal.

Tabla 4. Entropía relativa para todas las imágenes

LSB	Lenna	Nieve	bombilla	arguedas	abeja
1	0.011643021	0.0236561	0.00242517	0.00961643	0.00726897
2	0.021590917	0.0430478	0.00554716	0.01805963	0.01337248
3	0.029884548	0.07063423	0.01344795	0.02491537	0.01865454
4	0.037546895	0.08766526	0.02323984	0.03044968	0.02266997
5	0.043315499	0.1189989	0.03094747	0.03516558	0.02623149
6	0.046587765	0.14013413	0.03781506	0.03773872	0.0292234
7	0.050840531	0.16576441	0.04270735	0.03726777	0.03233229
8	0.051014261	0.17604638	0.04477249	0.03845346	0.0333697

Se observa también que a menor valor de LSB la entropía relativa se acerca más a cero, pero incluso con un LSB tan alto como 8 bits, todavía es bastante pequeña. Esto prueba que el método implementado produce imágenes esteganográficas seguras que simulan el ruido natural y no dan evidencia de que contienen información (Tabla 4).

CONCLUSIONES

Los autómatas celulares bidimensionales también son buenos generadores de secuencias seudoaleatorias, pero su costo en tiempo de computación es más elevado que el de los autómatas

UNIVERSIDAD NACIONAL DEL ALTIPLANO
REVISTA DE INVESTIGACIONES DE LA ESCUELA DE POSGRADO
Versión electrónica ISSN 2077 – 8686
Versión Impresa ISSN 1997-4035
ARTÍCULO ORIGINAL

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

lineales. Las configuraciones estudiadas emplean un tiempo bastante grande de procesamiento por imagen. Esta es una característica que es deseable disminuir.

Son pocos los autómatas con una regla que les permita evolucionar de forma suficientemente caótica para generar secuencias de bits seudoaleatorias, las reglas estudiadas se pueden utilizar en otras configuraciones para analizar sus resultados ya que por la naturaleza impredecible de los autómatas celulares no se puede asegurar que el comportamiento descrito en ellos en este estudio es adecuado bajo todas las circunstancias. Las imágenes portadoras generadas por el método propuesto en combinación con las secuencias seudoaleatorias, generan imágenes de buena calidad con un PSNR alto, pero, solo para LSB mayores a 4 bits. Los mejores resultados sin embargo se obtienen utilizando un LSB de 1 bit. Con un LSB menor se puede codificar menos información por cada imagen portadora; la decisión de utilizar un número determinado de bits, depende de la cantidad de información a codificar y la calidad de imagen esperada.

La esteganografía que codifica mensajes cifrados con apariencia de aleatoriedad generada por un autómata celular bidimensional es segura, si se utiliza un número de bits LSB menor que dos. Para un LSB más alto un atacante puede sospechar la presencia de un mensaje oculto.

LITERATURA CITADA

Agreste, S., Andaloro, G., Prestipino, D. y Puccio, L. (2007). An image adaptative, wavelet-based watermarking of digital images. Journal of computational and applied mathematics(210), 13-21.

Angulo, C., Ocampo, S. y Blandon, L. (2007). Una mirada a la esteganografía. Scientia Et Technica, 13(37), 421-426.

Areitio, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. España: Editorial Paraninfo.

Biswapati, J., Debasis, G., Kumar, S. y Pal, P. (2013). Imagen steganogrphy basen on cellular atuomata.

Cattaneo, G., Formenti, E. Margara, L. y Mauri, G. (1999). On the dynamicla behavior of chotic cellular automata. Theoretical Computer Science(217), 31-51.

Di Martino, F., Loia, V., Perfilieva, I. y Sessa, S. (2008). An image coding/decoding method based on direct and inverse fuzzy transforms. International Journal of Approximate Reasoning(48), 110-131.

Fúster-Sabater, A. y Caballero-Gil, P. (2009). Synthesis of cryptographic interleaved sequences by means of linear cellular automata. Applied Mathematics Letters, 22(10), 1518–1524. http://doi.org/10.1016/j.aml.2009.03.018

García, E., García, E. y Cárdenas, L. (2006). Simulación y Análisis de Sistemas con Promodel. México: Prentice Hall.

Gonzales, L. y Chaves, F. (2006). Estudio de las cadenas pseudoaleatorias generadas por los autómatas celulares unidimensionales de dos estados, implementación y aplicaciones a la criptografía. (U. I. Santander, Recopilador)

Gutub, A. (2010). Pixel indicator technique for RGB image steganography. Journal of Emerging Technologies in Web Intelligence, 2(1), 56–64.

Haynes, L. (2011). Using Image Steganography to Establish Covert Communication Channels. International Journal of Computer Science and Information Security, 9(9), 1–7.

Jakhar, J., Dey, P., Dutta, M. y Bhattacharyya, K. (2012). CellTCS:A Secure Threshold Cryptography Scheme based on Non-linear Hybrid Cellular Automata. Procedia Technology, 6, 947–953. http://doi.org/10.1016/j.protcy.2012.10.115

Jhaveri, P. (2012). Dos attacks in mobile ad hoc networks:. Proceedings of the 2012 2nd International Conference on Advanced (págs. 535–541). IEEE Computer.

Juarez, G., Zenill, H. y Stevens, R. (2011). Sistemas Complejos Como Modelos de Computacion. Luniver Press.

Jyoti, D. (2012). CellTCS:A Secure Threshold Cryptography Scheme based on Non-linear Hybrid Cellular Automata. Procedia Technology 6 , 947 – 953 .

Kruss, P., Scace, C., Heyman, M. y Mundy, M. (2003). A survey of steganography techniques form image files. Advanced Security Research Journal.

Mohamed, K. (2014). A parallel block-based encryption schema for digital images using reversible cellular automata. Engineering Science and Technology, 85-94.

Nagaraj, V., Vijayalakshmi, V. y Zayaraz, G. (2013). Color Image Steganography based on Pixel Value Modification Method Using Modulus Function. IERI Procedia. http://doi.org/10.1016/j.ieri.2013.11.004

Onomza, V., Isah, A. y Ochoche, A. (2012). Steganography and its applications in information dessimilation on the Web using images as security embeddement: a wavelet approach. International Journal of Computer and Information Technology, 1(2).

Vol. 6, No.1, pp. 66-77, Enero/Marzo, 2017
Recibido 16/05/2017
Aceptado 21/07/2017
Publicado 07/08/2017
DOI: http://dx.doi.org/10.26788/riepg.2017.28

Qazanfari, K. y Safabakhsh, R. (2014). A new steganography method which preserves histogram: Generalization of LSB++. Information Sciences, 277, 90–101. http://doi.org/10.1016/j.ins.2014.02.007

Regnault, D., Schabanel, N. y Thierry, E. (2009). Progresses in the analysis of stochastic 2D cellular automata: A study of asynchronus 2D minority. Theoretical Computer Science (410), 4844-4855.

Roelofs, G. (1999). PNG: The Definitive Guide.

Shannon, R. y Johanes, J. (1976). "Systems simulation: the art and science. IEEE Transactions on Systems, Man and Cybernetics, 6(10), 723-724.

Song, S., Zhang, J., Liao, D, J. y Wen, Q. (2011). A novel secure communication protocol combining steganography and cryptography. In Procedia Engineering. http://doi.org/10.1016/j.proeng.2011.08.521

Steinmetz, R., Dittman, J. y Steinbach, M. (2000). Information Hidin Techniques for Steganography and Digital Watermarking. Katzenbeisser.

Thanikaiselvan, V., Arulmozhivarman, P., Subashanthini, S. y Amirtharajan, R. (2013). A graph theory practice on transformed image: A random image steganography. The Scientific World Journal, 2013.

Velasco, C., López, J., Nakano, M. y Pérez, H. (2007). Esteganografía en una imagen ditial en el dominio DCT. Científica, 11(4), 169-176.

Wang, J., D, Y., Chang, C. y Thouin, P. (2002). Relative entropy based methods form image thresholding. IEEE International Conference on Image Processing, 2, 265-268.

White Hoya, S. (2002). Aplicaciones de los autómatas celulares a los criposistemas de cifrado de flujo.

Wolfram, S. (1986). Random sequence generation by cellular automata. Advances in Applied Mathematics.