Información Tecnológica
Vol. 25(4), 193-204 (2014)
doi: 10.4067/S0718-07642014000400021

Sistema de Imagen Secreta Compartida con Optimización de la Carga Útil

Angelina Espejel-Trujillo, Iván Castillo-Camacho, Mariko Nakano-Miyatake, Héctor Pérez-Meana
Escuela Superior de Ingeniería Mecánica y Eléctrica, Instituto Politécnico Nacional. Av. Santa Ana 1000, Col. San Francisco Culhuacán, 04430 México D.F.-México. (e-mail: angelina.et@gmail.com, blackevanus@gmail.com, mnakano@ipn.mx, hmperezm@ipn.mx)

Recibido Nov. 22, 2013; Aceptado Ene. 24, 2014; Versión final recibida Feb. 26, 2014

Resumen

En este trabajo se propone un esquema de umbral-(*k,n*) basado en el método de interpolación, donde los datos secretos son cualquier tipo de datos binarios, tales como imágenes, señales de audio, video, documentos y archivos ejecutables. El esquema propuesto usa los polinomios de Lagrange en el campo de Galois GF(2^8) para codificar y decodificar los datos secretos sin pérdidas. Los datos secretos son ocultados en *n* imágenes camuflaje. Para la decodificación, se requieren al menos *k* (≤n) imágenes camuflajes para revelar los datos secretos. Para incrementar la carga útil de los datos secretos, la interpolación de Lagrange se resuelve de manera iterativa bajo un campo *GF(2^8).* Los resultados muestran que el sistema propuesto presenta una mayor carga útil comparado con los resultados de otros métodos propuestos previamente. Además, la calidad de las imágenes camuflaje es mayor que en los algoritmos convencionales cuando la misma cantidad de datos secretos es compartida.

Palabras clave: secreto compartido, imagen secreta compartida, carga útil, interpolación de Lagrange

Improved Secret Image Sharing Scheme with Payload Optimization

Abstract

In this paper an interpolation method based on *(k,n)*-threshold secret image sharing (SIS) scheme is proposed, in which the secret data are any binary data, such as images, audio, video, document and even executable files. The proposed scheme uses Lagrange polynomial in the Galois Field *GF*(2^8) to encode and decode the secret data in a lossless manner. The shared data are hidden into *n* camouflage images. In the decoding stage, at least *k (≤n)* camouflage images are required to reveal the secret data. To increase the payload of the secret data, Lagrange interpolation is solved in an iterative manner under *GF*(2^8). The experimental results show a higher payload of the secret data compared to those of other methods previously reported. Also, the quality of the camouflage images is higher than that of the conventional algorithms when the same amount of secret data is shared.

Keywords: secret sharing, image secret sharing, payload, Lagrange interpolation

INTRODUCCIÓN

Actualmente en los grandes corporativos y empresas gubernamentales se llevan a cabo gestiones sobre información confidencial, algunas de las cuales conllevana la divulgación dela misma.Sin embargo para poder divulgar dicha información, que puede ser un secreto gubernamental o material clasificado, es necesario que varios miembros de sus juntas directivas o gabinetes estén de acuerdo en llevar a cabo esa acción. Por lo que se requiere de un sistema que comparta información de manera segura entre varios miembros de un grupo, donde se pueda a acceder a esta de manera colectiva restringiendo el acceso individual.

Para resolver estos escenarios, Shamir (1979) y Blakely (1979) propusieron un esquema eficiente conocido como Esquema de Secreto Compartido (ESC) bajo un umbral-*(k,n)*, en el cual durante la etapa de codificación, los datos secretos son segmentados en *n* piezas que son compartidos entre *n* participantes; mientras que en la etapa de decodificación al menos *k* piezas de las*n* son requeridas para recuperar la información confidencial. La seguridad de este esquema consiste en asegurar que la información secreta no pueda ser recuperada con *(k-1)* o menos piezas y que usando cualquier $l \geq k$ piezas, la información pueda ser revelada sin ninguna ambigüedad.

Basado en el ESC, los Esquemas de Imagen Secreta Compartida (EISC) fueron desarrollados para compartir una imagen secreta entre varios participantes. Estos esquemas pueden ser clasificados en tres categorías (Tsai y Col., 2009): EISC basados en Criptografía Visual (CV) (Naor y Shamir, 1995; Droste, 1996;Ateniesey Col.,1996; Espejel y Col., 2011; Espejel y Col., 2012), EISC basados en una Variante de Esquema de Secreto Compartido Visual (V-ESCV) (Chang y Col., 2000; Wu y Sun, 2010) y EISC basados en Métodos de Interpolación (Thien y Lin, 2002; Lin y Tsai, 2004; Yang y Col., 2007; Chang y Col., 2008). Por otro lado se tienen los EISC basados en Autómatas Celulares (AC) (Álvarez y Col., 2003; Álvarez y Col., 2008; Eslami y Col., 2012; Wu y Col., 2012; Jin y Wu, 2012) que pueden ser considerados como una implementación de los EISC, en los cuales la teoría de autómatas celulares es empleada para este propósito. En los EISC basados en CV propuestos por Naor y Shamir (1995), se genera un EISC bajo un umbral-*(k,n)* donde *n* imágenes llamadas *sombras,* las cuales lucen como un patrón de ruido pseudo-aleatorio, cifran una imagen secreta binaria. En los EISC basados en CVcualquier combinación de *k* sombras de las*n* sombras generadas se superponen juntas de tal forma que la imagen secreta es revelada por medio del Sistema Visual Humano (SVH), sin necesidad de operaciones computacionales. Sin embargo al lucir las sombras como ruido pseudo-aleatorio, éstas pueden considerarse sospechosas cuando son enviadas a través de las redes de comunicación. Esta limitación se mantiene incluso en los sistemas Extendidos de CV propuestos en Ateniese y Col. (1996) y Droste (1996), los cuales generan sombras visualmente reconocibles en lugar de que éstas luzcan como ruido pseudo-aleatorio. Aun con las modificaciones introducidas, la limitación persiste ya que estos esquemas son adecuados solamente para imágenes binarias, además de que la calidad de la imagen generada es muy pobre.Adicionalmente a esta limitación, la expansión del pixel en la imagen revelada presenta restriccionesinevitables para su uso práctico.

Los EISC basados en V-ESCV intentan superar las limitaciones de los EISCbasados en CV (Nakano y Col., 2011), comentadas anteriormente, usando algunos algoritmos de codificación y decodificación diferentes. Generalmente en el proceso de recuperación de los EISC algunos algoritmos de recuperación son empleados en vez del SVH y, aunque algunas limitaciones son superadas, otros inconvenientes persisten en los sistemas de EISCbasados en CV. El esquema de Chang (2000) oculta una imagen a color en dos imágenes camuflajeen las cuales la expansión de pixel no ocurre, al igual que la imagen secreta obtenida no se expande.Sin embargo el esquema está limitado a un umbral de (2,2) en vez de un *(k,n)*. En los EISCbasados en V-ESCV propuesto por Wu y Sun (2010), cualquier imagen a escala de grises es descompuesta en los 8 planos de bits donde cada plano de bit es tratado individualmente como una imagen secreta y las sombras son generadas para cada plano de bits usando un esquema convencional de CV. En el proceso de recuperación, cada plano de bits es revelado superponiendo sus respectivas sombras y finalmente la imagen en escala de grises es obtenida mediante la recomposición de los 8 planos de bits revelados. La principal limitación de este sistema es que la expansión de los pixeles es igual que la presentada en los EISC basados en CV.

En los EISC basados en AC, los cuales utilizan la teoría de autómata celular, una imagen secreta es considerada como un autómata celular bidimensional C^t. Este evoluciona en un tiempo discreto *t* mediante el cambio de estado de sus celdas (pixeles) de acuerdo a una función de transición *f*, una configuración de sus vecindades denotado por $V_{i,j}$ y los estados de sus celdas en *t-q* , donde *q={1.2…., n}*. En la etapa de recuperación *n* sombras son presentadas en orden consecutivo y se procesan con la evolución inversa para recuperar la imagen secreta. Álvarez y Col. (2003) proponen un sistema cuyas datos secretos son imágenes a color y se reparten entre *n* participantes usando la teoría de AC para generar *n* imágenes con apariencia de ruido pseudo-aleatorio, las cuales son requeridas para recuperar la imagen secreta. En (Álvarez y Col.,

2008), se presenta una mejora de este sistema, donde más de una imagen secreta es compartida. Aquí las*n* imágenes secretas son consideradas como C^{t-1}, C^{t-2},…, C^{t-n} estados de *C*. El trabajo reportado en (Eslami y Col., 2012; Wu y Col., 2012; Jin y Wu, 2012) presenta sistemas basados en AC donde imágenes naturales son usadas como imágenes camuflaje, Eslami y Col. (2012) presentan un autómata celular dimensional para procesar cada celda (pixel) de la imagen secreta. Una vez que la última evolución ha terminado, esta es insertada dentro de las imágenes camuflaje usando la técnica LSB. El método propuesto en Wu y Col. (2012) obtiene *k* planos de las imágenes secretas como C^{t-1}, C^{t-2},…, C^{t-q} estados de AC y el sistema evoluciona de acuerdo a la teoría de AC. Cuando la última evolución es obtenida, ésta es insertada en las imágenes camuflajes usando operación de módulo. Finalmente Jin y Wu (2012) emplean las características de la configuración de vecindades para generar las*n* sombras. Dado que todo el proceso es realizado a nivel de bit, el punto clave de este proceso es la operación XOR utilizada. La principal desventaja de los EISC basados en AC es que presentan muchas condiciones, tales como el orden de las imágenes camuflaje y las funciones de transición usadas durante la evolución, las cuales son requeridas para revelar las imágenes secretas. Además en esta categoría sólo se construyen esquemas con umbral *(n,n)*.

Para obtener una imagen recuperada con una alta calidad, los esquemas EISC basados en Método de Interpolación (MI) son la mejor opción. Este esquema está directamente basado en el esquema de secreto compartido de Shamir (1979) y debido a su deseable desempeño, varios esquemas basados en MI han sido propuestos en los años recientes (Thien y Lin, 2002; Lin y Tsai, 2004; Yang y Col., 2007; Chang y Col., 2008). Thien y Lin (2002) proponen un esquema de umbral *(k,n)* , en el cual un polinomio de grado *k-1* es construido usando *k* pixeles de una imagen a escala de grises. La principal desventaja de este esquema es que las sombras con apariencia de ruido son almacenadas o transmitidas, lo cual podría ser sospechoso para un tercero. En Lin y Tsai(2004), los autores proponen un esquema EISC basado en MI con un umbral *(k,n)* , el cual se combina con esteganografía LSBempleandooperaciones en módulo-251 en el polinomio de grado *k-1* para restringir los valores de las llaves, las cuales deben de estar situadas entre el rango de [0,250]. Los valores de las llaves obtenidas se insertan en las imágenes camuflaje usando esteganografía LSB. En este esquema las imágenes camuflaje son siempre 4 veces mayores que la imagen secreta, y hay un poco de pérdida en la calidad de la imagen secreta recuperada debido al truncamiento dentro del rango [0,250]. Yang y Col. (2007) proponen una mejora al método de Lin y Tsai (2004), en el cual para autenticar las imágenes camuflaje, se implementa una función Hash en vez de usar una verificación por bit de paridad como en el caso de Lin y Tsai (2004). También la operación módulo-251 es reemplazada por la operación $GF(2^8)$ para obtener una imagen revelada sin pérdidas. Sin embargo la autenticación basada en Hash ocasiona un incremento en el uso de los bits que se ocultan por lo que para compensar esto, la calidad de la imagen es sacrificada. Este método también propicia una expansión en las imágenes camuflaje. Chang y Col. (2008) proponen una mejora al algoritmo de Lin y Tsai (2004), reemplazando la autenticación del bit de paridad por el Teorema Chino del Residuo (TCR). En este algoritmo, también la operación módulo-251 es utilizada; por lo que la imagen revelada es una imagen con pérdidas.

En este trabajo, se propone un método de EISC basado en MI con un umbral *(k,n)* en el cual lacarga máxima de datos útil puede ser controlada mediante el valor *k*. Esto es, si *k* es mayor que 4, la máxima carga útil de los datos secretos puede ser tan grande como el tamaño de la imagen camuflaje, lo cual permite una eficiente y secreta transmisión de los datos. En el algoritmo propuesto, todas las operaciones se realizan dentro del Campo de Galois, $GF(2^8)$, usando un polinomio primitivo el cual garantiza que la imagen revelada sea sin pérdidas, y al mismo tiempo permite que las imágenes camuflaje tengan mayor calidad. Además, la información secreta puede ser cualquier tipo de datos, tal como documentos, audio, video e incluso un archivo ejecutable. El resto de este trabajo está organizado como sigue: Inicialmente se presenta el algoritmo propuesto. Seguidamente se proveen algunos resultados experimentales que muestran el rendimiento del algoritmo propuesto y finalmente se presenta la conclusión de este trabajo.

ESQUEMA PROPUESTO DE IMAGEN SECRETA COMPARTIDA

Como se mencionó anteriormente el EISC propuesto está basado en el esquema de secreto compartido de Shamir con un umbral *(k,n)*, en el cual la información secreta *S* se comparte entre *n* participantes y cuando al menos *k* participantes proveen sus sombras, la información secreta *S* es revelada. El umbral *(k,n)* del esquema de secreto compartido de Shamir (1979) se basa en un polinomio de grado *(k-1)* dado por:

$$F(x_i) = S + a_1 x_i + a_2 x_i^2 + \ldots + a_{k-1} x_i^{k-1}, \qquad i = 1..n \tag{1}$$

Donde *S* es la información secreta, x_i es el valor compartido para el *i-ésimo* participante P_i, el cual debe satisfacer la condición $x_i \neq x_j$ para cualquier *i≠j* y $a_1,..,a_{k-1}$ es un conjunto de coeficientes seleccionados al azar, los cuales no necesariamente se requiere en la etapa de recuperación. Una vez que todos los pares

$(x_i, F(x_i)), i = 1..n$ han sido generados, son distribuidos entre los *n* participantes. Como se mencionó anteriormente, para recuperar el mensaje secreto*S*, al menos *k* pares $(x_i, F(x_i))$ son requeridos para encontrar la solución de (1) usando el método de interpolación de Lagrange.

En el algoritmo propuesto, los datos secretos pueden ser cualquier tipo de datos digitales, incluyendo imágenes, documentos e incluso archivos ejecutables, lo que significa que los datos secretos deben ser compartidos y recuperados sin ninguna pérdida. Primeramente los datos secretos son compartidos utilizando el esquema de secreto compartido de Shamir bajo un campo *GF*(2^8) y luego cada sombra es insertada dentro de *n* imágenes camuflaje usando esteganografía LSB. Para revelar los datos secretos al menos *k* imágenes camuflaje son requeridas, las cuales se dividen en bloques de 2x2 pixeles. Seguidamente de cada bloque de cada imagen camuflajese extrae un byte, correspondiente a una sombra de un participante. Finalmente*k*bytes en totalson extraídos de *k* imágenes camuflaje y son asignados como solución $F(x_{q_l}), l = 1..k$ del polinomio dado por (1). Aplicando la interpolación de Lagrange a (1), los datos secretos son obtenidos. Las siguientes secciones proveen una descripción detallada de la etapa de codificación y decodificación del método propuesto.

Etapa de Codificación

En la etapa de codificación, el conjunto de datos secretos *S* de *L* bytes es segmentado en bloques de *k* bytes, donde cada bloque es descrito como $B_j = [s_1^j, s_2^j, \cdots s_k^j], j = 1..L/k$. Por su parte las imágenes camuflaje denotadas como $C_i, i = 1..n$, se distribuyen a cada uno de los *n*participantes. El diagrama a bloques de la etapa de codificación en el esquema propuesto se muestra en la figura 1. Aquí usando *k* bytes de cada bloque secreto, se construye un polinomio de grado *(k-1)* en el GF(2^8)el cual está dado por (2), donde *g(x)* es un polinomio primitivo en GF(2^8).

$$F(x) = (s_1 + s_2 x + s_3 x^2 + \ldots + s_k x^{k-1}) \mod g(x) \tag{2}$$

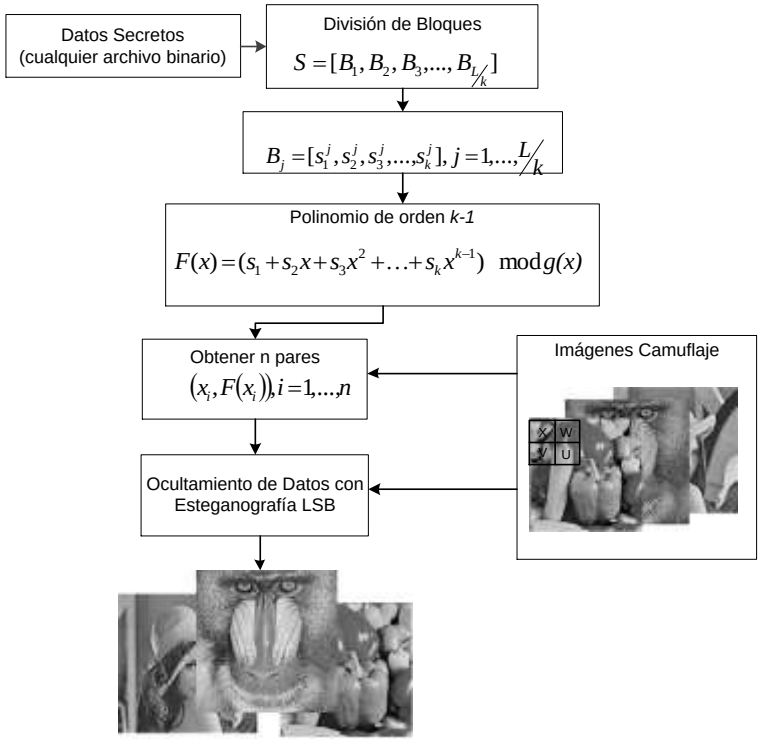

Fig. 1: Diagrama a bloques de la etapa de codificación en el esquema propuesto.

Cada imagen camuflaje es dividida en bloques de 2x2 pixeles como se muestra en la figura 2 y usando el pixel localizado en la parte superior izquierda de cada bloque, la cual es denotada por $X_{i,j}$, el polinomio dado en (2) se evalúa.

$$F(X_{i,j}) = \left(s_1 + s_2 X_{i,j} + s_3 X_{i,j}^2 + \ldots + s_k X_{i,j}^{k\ 1}\right) \bmod g(x) \tag{3}$$

Donde $X_{i,j}$ es el valor del pixel localizado en la parte superior del *j-ésimo* bloque de la *i-ésima* imagen camuflaje C_i.

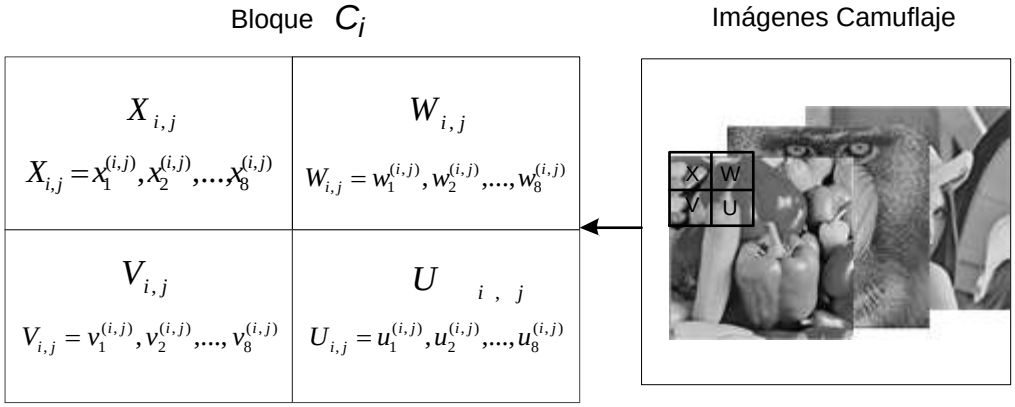

Fig. 2: Bloque de 2×2 pixeles de cada imagen camuflaje C_i. X,W,V y U son los cuatro valores de pixeles de cada bloque.

Evaluando (3) usando el valor del pixel $X_{i,j}$ de cada una de las*n* imágenes camuflaje, obtenemos *n* pares de valores para cada bloque, los cuales son $(X_{i,j}, F(X_{i,j})), i = 1,..,n, j = 1,..,m$, donde *m* es el número de bloques. La operación *GF*(2^8) garantiza una recuperación sin pérdida de los datos secretos y una alta calidad de las imágenes camuflaje. La representación binaria de los valores $F(X_{i,j})$, los cuales están dentro del rango [0, 255], se denota:

$$T_{i,j} = \left[F(X_{i,j})\right]_b = [t_1^{(i,j)}, t_2^{(i,j)}, \cdots, t_8^{(i,j)}], \quad i = 1,..,n,\ j = 1,..,m \tag{4}$$

Donde $[z]_b$ es la representación binaria del valor de un byte z. Los 8 bits de $T_{i,j}$ son divididos en tres partes y embebidos en los tres bits menos significativos $W_{i,j}$, $V_{i,j}$ y $U_{i,j}$. Esta operación se ilustra en la figura 3. De esta figura se puede observar que los tres bits menos significativos de los pixeles $W_{i,j}$ y $V_{i,j}$, los cuales son $w_6^{(i,j)}, w_7^{(i,j)}, w_8^{(i,j)}$ y $v_6^{(i,j)}, v_7^{(i,j)}, v_8^{(i,j)}$, son remplazados por $t_1^{(i,j)}, t_2^{(i,j)}, t_3^{(i,j)}$ y $t_4^{(i,j)}, t_5^{(i,j)}, t_6^{(i,j)}$, respectivamente, mientras que los dos bits menos significativos del pixel $U_{i,j}$, $u_7^{(i,j)}, u_8^{(i,j)}$ son remplazados por $t_7^{(i,j)}, t_8^{(i,j)}$. Para autenticar cada uno de los bloque de cada imagen camuflaje, un bit de paridad $p^{(i,j)}$ es obtenido de los 8 bits de $F(X_{i,j})$ y el cual es usado para remplazar $u_6^{(i,j)}$. Estos tres pixeles con los datos ocultos $\tilde{W}_{i,j}$, $\tilde{V}_{i,j}$, $\tilde{U}_{i,j}$ y el pixel $X_{i,j}$ forman un bloque en donde se ocultan los 8 bits de $F(X_{i,j})$. Esta operación se repite para cada uno de los bloques $B_j, j = 1...L/k$ del dato secreto *S* hasta que se obtienen las *n* estego-imágenes compartidas, en las cuales están ocultos los datos secretos *S*.

Etapa de decodificación

Para recuperar los datos secretos *S,* al menos *k* estego-imágenes deben presentarse. La etapa de decodificación se muestra en la figura 4. En esta etapa primeramente las estego-imágenes son divididas en bloques de 2x2 pixeles y entonces los 8 bits de datos $T_{i,j}^{'}$ y el bit de paridad $p' = \tilde{u}_6^{i,j}$ son extraídos de los tres pixeles $\tilde{W}_{i,j}$, $\tilde{V}_{i,j}$, $\tilde{U}_{i,j}$ como se presenta en (5).

$$T_{i,j}^{'} = [\tilde{w}_6^{i,j}, \tilde{w}_7^{i,j}, \tilde{w}_8^{i,j}, \tilde{v}_6^{i,j}, \tilde{v}_7^{i,j}, \tilde{v}_8^{i,j}, \tilde{u}_7^{i,j}, \tilde{u}_8^{i,j}] \tag{5}$$

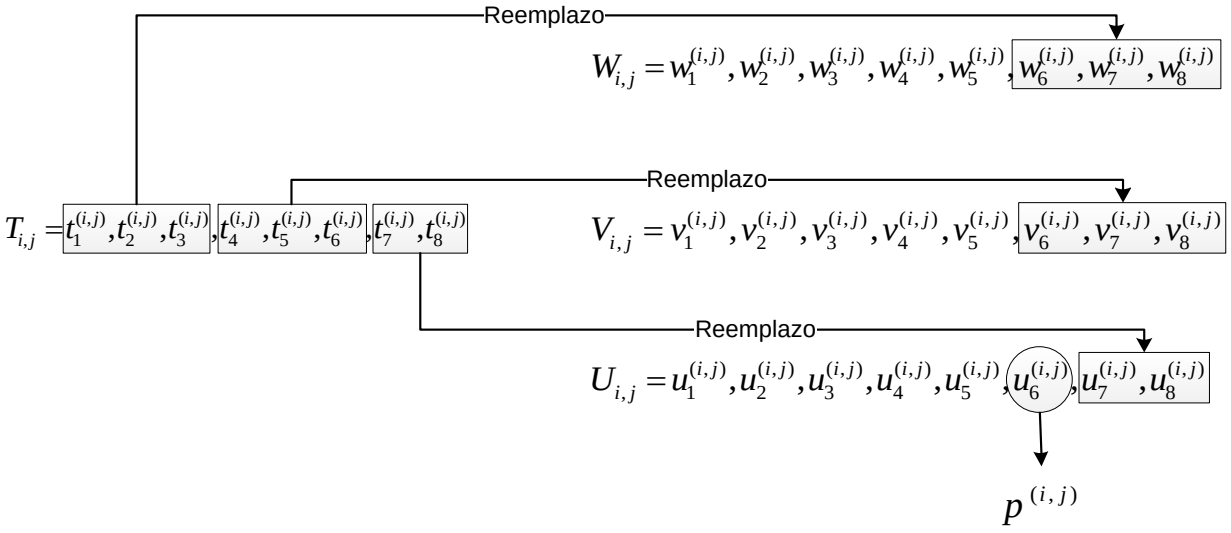

Fig. 3: Ocultamiento de datos usando esteganografía LSB

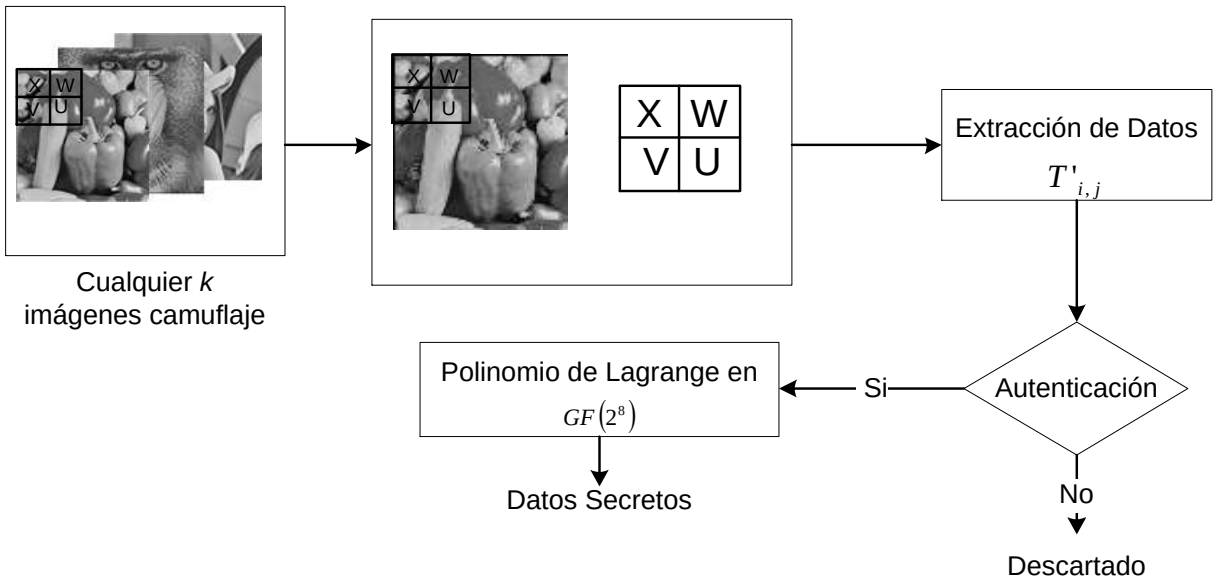

Fig. 4: Diagrama de la etapa de decodificación del algoritmo propuesto.

Después que $T'_{i,j}$ es extraído, la autenticación debe ser confirmada usando el bit de paridad extraído $p' = \tilde{u}_6^{i,j}$ y los elementos de $T'_{i,j}$. Si $p' = \tilde{p}^{i,j}$ entonces el *j-ésimo* bloque de la*i-ésima* imagen camuflaje es auténtica, en otro caso este bloque no es auténtico, donde $\tilde{p}^{i,j} = \tilde{w}_6^{i,j} \otimes \tilde{w}_7^{i,j} \otimes \tilde{w}_8^{i,j} \otimes \tilde{v}_6^{i,j} \otimes \tilde{v}_7^{i,j} \otimes \tilde{v}_8^{i,j} \otimes \tilde{u}_7^{i,j} \otimes \tilde{u}_8^{i,j}$ y $\otimes$ es la operación OR-exclusiva. Si $T'_{i,j}$ es auténtico, los datos secretos serán extraídos usando la interpolación de Lagrange, si no es auténtico $T'_{i,j}$ es descartado.

Este proceso depende fuertemente de la clase de los datos secretos, si éstos son un archivo ejecutable, una vez que se determina que uno de los bloques ha sido alterado, la estego-imagen entera a la que pertenece el bloque alterado, debe ser descartado. Mientras que si los datos secretos son, por ejemplo, una imagen, solo el bloque alterado debe ser descartado y usando los bloques calificados como auténticos se pueden reconstruir los datos secretos.

En *j-ésimo* bloque, el valor extraído $Y_{i,j}$, el cual es una representación decimal de $T'_{i,j}$, se obtiene en el rango de [0,255]. Introduciendo *k* pares $(X_{i,j}, Y_{i,j})$ dentro de la interpolación de Lagrange (3), *k* datos secretos $s_1^j, s_2^j, \cdots, s_k^j$ que fueron codificados en *j-ésimo* bloques son recuperados calculando (6)-(8). Aquí, el primer dato secreto s_1^j es obtenido por (6).

$$s_1^j = L_j(0) = \left[(-1)^{k-1} \left(\sum_{i=1}^{k} Y_{i,j} \prod_{q=1, i \neq q}^{k} \frac{X_{q,j}}{X_{i,j} - X_{q,j}} \right) \right] \bmod g(x) \tag{6}$$

Los datos secretos $s_2^j, s_3^j, \cdots, s_k^j$ son obtenidos de manera consecutiva calculando iterativamente (6) usando el valor actualizado $Y'_{i,j}$ dado por (7).

$$Y'_{i,j} = \left[\frac{Y_{i,j} - s_1^j}{X_{i,j}} \right] \bmod g(x) \tag{7}$$

$$s_r^j = \left[(-1)^{k-r} \left(\sum_{i=1}^{k-r+1} Y'_{i,j} \prod_{q=1, i \neq q}^{k-r+1} \frac{X_{q,j}}{X_{i,j} - X_{q,j}} \right) \right] \bmod g(x), \qquad r = 2, \ldots, k \tag{8}$$

En (6)-(8) es usado el mismo polinomio primitivo *g(x)* en *GF*(2^8) utilizado en (2) y (3). Todos los datos secretos son reconstruidos aplicando la operación arriba mencionada a todos los bloques.

RESULTADOS EXPERIMENTALES

En esta sección se evalúa el rendimiento del algoritmo propuesto usando varias imágenes a color y a escala de grises como imágenes camuflaje, mientras que como datos secretos son usados algunas imágenes, documentos y documentos encriptados. En toda la evaluación es usado el polinomio primitivo $g(x) = (x^8 + x^4 + x^3 + x + 1)$. El rendimiento del algoritmo propuesto es comparado con algunos de los algoritmos previamente presentados en la literatura (Lin y Tsai, 2004; Yang y Col., 2007; Chang y Col., 2008), también se compara con (Álvarezy Col., 2003) y (Wu y Col., 2012) ya que tienen el mismo propósito que el algoritmo propuesto. En todos los algoritmos mencionados arriba, se usa como dato secreto una imagen, esto es con el propósito de realizar una justa comparación, a su vez en el sistema propuesto cualquier archivo binario puede ser usado como datos secretos.

Una breve descripción de estos algoritmos está dada en la Tabla 1, en la cual PS:PC significa la proporción del número de pixeles entre la imagen secreta y la imagen camuflaje. En el esquema propuesto, *k* pixeles de la imagen secreta son ocultados en bloques de 4 pixeles de las imágenes camuflaje, denotado por *k*:4, mientras que en los esquemas de Lin y Tsai (2004) y Yang y Col. (2007), solo un pixel puede ser ocultado en cada bloque, independientemente del valor de *k* . Para Álvarez y Col. (2003)y Wu y Col. (2012), es necesario que las imágenes secretas sean del mismo tamaño que las imágenes camuflaje, e incluso en Álvarez y Col.(2003), el cual es un sistema multi-secreto, todas las imágenes secretas deben tener el mismo tamaño de las imágenes camuflaje. Lin y Tsai (2004)y Chang y Col. (2008), presentan operaciones de campos finitos basadas en módulo-251, donde se usa 251 ya que es el número primo más grande dentro del rango de pixeles de imagen [0, 255], mientras que en Álvarez y Col. (2003)y Wu y Col. (2012) se usa mod(*c*), donde $c = 2$ para imágenes binarias, $c = 2^8$ para imágenes a escala de grises, y $c = 2^{24}$ para imágenes a color. En el esquema propuesto, la codificación y decodificación se llevan a cabo dentro del campo de Galois GF(2^8), evitando así el truncamiento de los valores de los pixeles, esto permite una reconstrucción perfecta de la imagen secreta y cualquier dato secreto. Como se puede observar en la Tabla I, los métodos de Álvarez y Col. (2003) y Wu y Col. (2012) no utilizan ningún mecanismo de autenticación de las imágenes camuflaje, las cuales son patrones pseudo-aleatorios en el método de Álvarez y Col. (2003)

Tabla 1: Descripción de varios esquemas de EISC basados en MI y AC, incluido el propuesto

Esquema	PS:PC	Campo Finito	Método de Autenticación	Tipo de Camuflaje	Archivo Secreto
Lin y Tsai (2004)	1:4	mod 251	Chequeo de Paridad	Natural	Imagen
Yang y Col. (2007)	1:4	$GF(2^8)$	Hash	Natural	Imagen
Chang y Col. (2008)	*k*:4	mod 251	CRT	Natural	Imagen
Alvarez y Col. (2003)	NA	mod (*c*)	-	Seudo-aleatorio	Imagen
Wu y Col.(2012)	1:1	mod (*c*)	-	Natural	Imagen
Propuesto	*k*:4	$GF(2^8)$	Chequeo de Paridad	Natural	Imagen, text, .pdf, .xls, etc

Las figuras 5 y 6 muestran algunos ejemplos de imágenes secretas e imágenes camuflaje usadas en las evaluacionesy la figura 7 muestra una comparación entre el algoritmo propuesto y cuatro algoritmos previamente propuestos (Lin y Tsai, 2004; Yang y Col., 2007; Chang y Col., 2008; Wu y Col., 2003), acerca de la calidad de las imágenes camuflaje con datos secretos compartidos y ocultos. Aquí se usa un esquema de umbral (2,3) para evaluarlos cuatro algoritmosy el algoritmo propuesto, mientras que para algoritmo de Wu y Col.(2003),un umbral-(3,3) es usado, ya que los esquemas EISC basados en AC generan solo esquema de umbrales *(n,n).* El esquema de Álvarez y Col. (2003) no puede incluirse en esta evaluación ya que sus imágenes camuflaje no son imágenes naturales si no que son imágenes con apariencia de ruido pseudo-aleatorio. Así, como se muestra en la figura 7, el algoritmo propuesto presenta imágenes camuflaje con mejor calidad en comparación con los demás algoritmos.

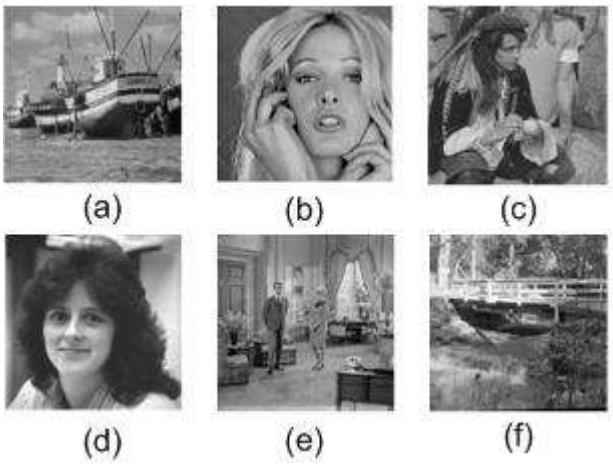

Fig. 5: Imágenes a escala de grises.(a) Imagen Secreta, (b)-(f) Imágenes Camuflaje

Fig. 6: Imágenes a color. (a) Imagen Secreta (b)-(f) Imágenes Camuflaje

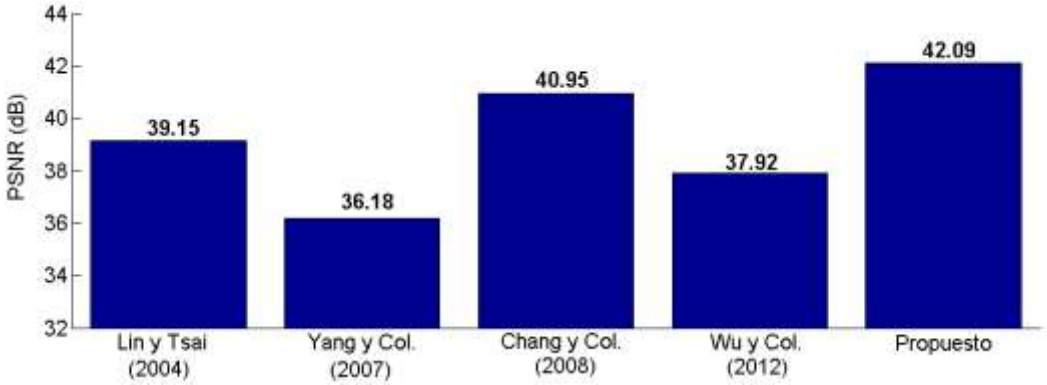

Fig. 7: Comparación de la calidad de las estego-imágenes generadas por cuatro métodos previamente presentados y el algoritmo propuesto.

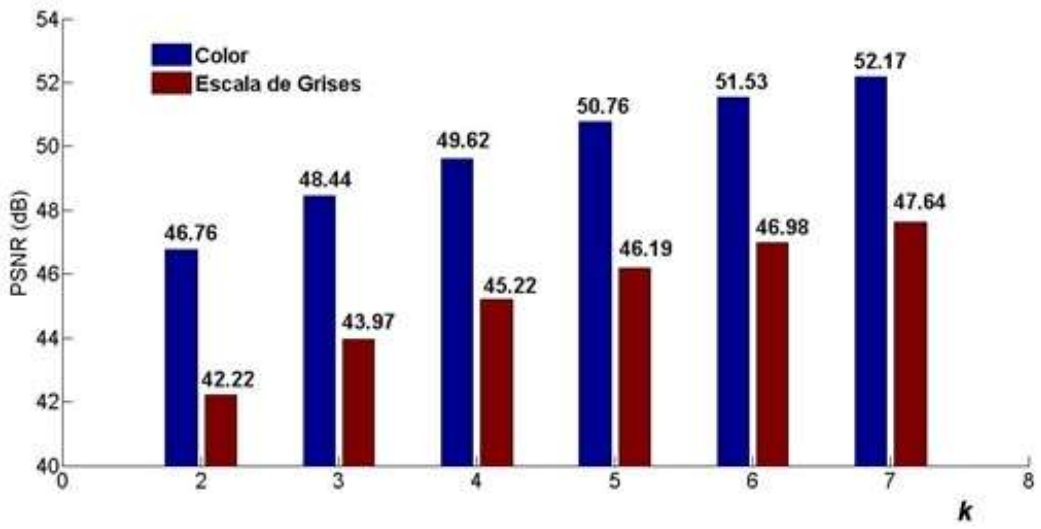

Fig. 8: Relación entre el valor *k* de esquema umbral-(*k*, 7) y la calidad de imágenes camuflaje

La figura 8 muestra la relación entre el valor *k* en un esquema de umbral-(*k*,7) y la calidad de las imágenes camuflaje cuando la imagen secreta, mostrada en la figura 5(a), fue compartida entre 7 participantes y se ocultó dentro de 7 imágenes camuflaje. Las imágenes camuflaje son: a escala de grises y a colores, algunas de ellas se presentan en las figuras 5 y 6. Como se puede observar de la figura 8, la calidad de las imágenes camuflaje es directamente proporcional al valor *k* del esquema. Obviamente después del ocultamiento, la calidad de las imágenes camuflaje a color es mejor que la calidad de las imágenes camuflaje a escala de grises, debido a la mayor capacidad de ocultamiento que tiene las primerasrespecto a las segundas.

La carga útil (payload) de los datos usados en el algoritmo con un esquema de umbral *(k,n)* esta dado por:

$$Payload\ (byte) = \frac{NPixeles \times Ncolor \times 4}{4} \tag{9}$$

donde *NPixeles*es el número de pixeles y *N color* es número de colores que continen las imágenes camuflaje. La máxima carga útil de los datos secretos denominada *Payload* en (9) es proporcional al tamaño de las imágenes camuflaje (*NPixeles*) y el valor *k*. Por ejemplo, si el algoritmo propuesto comparte información secreta en imágenes camuflaje a escala de grises con un tamaño de 100×100 pixeles bajo un esquema de umbral (4,6), La máxima carga útil de los datos secretos es igual a 10Kbyte, lo cual significa que este es del mismo tamaño de las imágenes camuflaje.

Como se mencionó anteriormente, las operaciones en $GF(2^8)$, dadas por (2)-(3) y (6)-(8), contribuyen a una recuperación sin pérdida de los datos secretos, lo cual permite al algoritmo propuesto manejar cualquier tipo de datos digítiales, tal como: documentos, imágenes, audio e inclusive archivos ejecutables y archivos encriptados como datos secretos compartidos entre *n* participantes.La figura 9 presenta el promedio de los valores PSNR de las stego-imágenes generadas por el algortimo propuesto usando un esquema de umbral-(*k*,*7*), variando el valor de *k*. En este caso los datos secretos son un documento con extension ".docx" cuyo tamaño es de 128 kbytes, el cual es la máxima carga útil que puede ofrecer un esquema de umbral-(*2*,*7*), usando el algoritmo propuesto con imágenes camuflaje a escala de grises de 512×512 pixeles. Cabe mencionar que esta máxima carga útil equivale a un documento de 5 paginas. La figura 10 muestra el promedio de los valores PSNR de las stego-imágenes generadas por algortimo propuesto usando un esquema de umbral-(*k*,*7*), variando el valor de *k*. En este caso los datos secretos son un documentocon extension ".docx" cuyo tamaño es de 382 kbytes,el cual es la máxima carga útil que puede ofrecer un esquema de umbral-(*2*,*7*), usando el algoritmo propuesto con imágenes camuflaje a color de 512×512 pixeles y esta máxima carga útil es equivalente a un documento de 10 paginas.

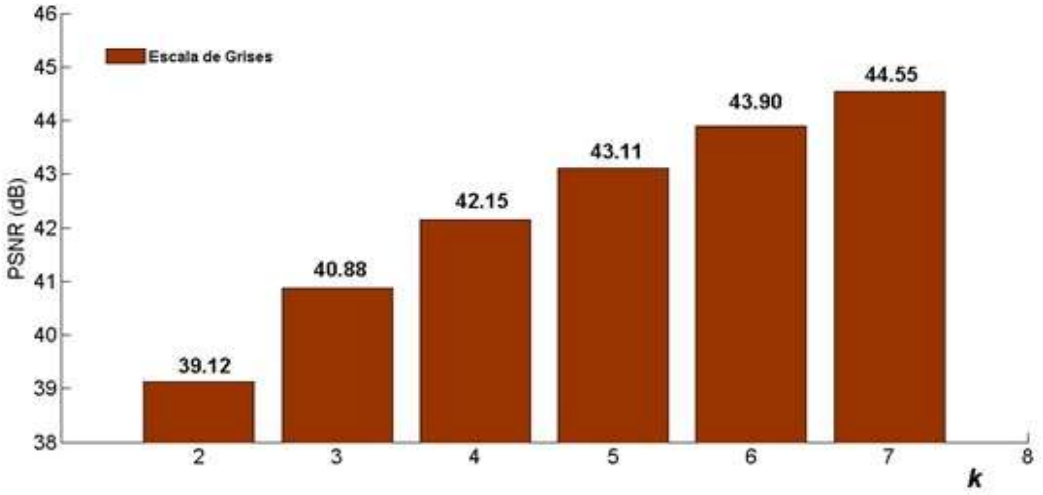

Fig. 9: Relación entre valor *k* de un esquema de umbral-(*k, 7*) y la calidad de imágenes camuflaje a escala de grises usando un documento como dato secreto.

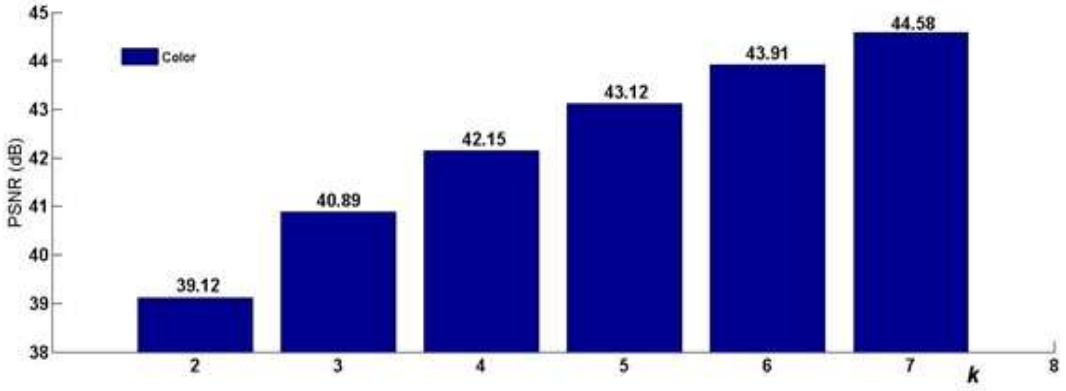

Fig. 10: Relación entre k-valores de un esquema de umbral- (k, 7) los valores PSNR con un documento como dato secreto para imágenes a color.

CONCLUSIONES

En este trabajo varios Esquemas de Imagen Secreta Compartida (EISC) han sido analizados, incluyendo los esquemas EISC basados en Autómatas Celulares (AC). Entre estos esquemas de EISC, los que están basados en MI son considerados como la mejor opción, desde varios puntos de vista, tales como la calidad de las imágenes secretas recuperadas y la flexibilidad de los esquemas; donde cualquier esquema de umbral-*(k,n)* puede ser construido. En el algoritmo propuesto de esquema de EISC basado en MI, los datos secretos no solo son imágenes digitales si no también cualquier dato binario, tales como documentos, audio, video e incluso archivos ejecutables. Hasta este punto, los datos secretos pueden ser recuperados sin pérdida debido al uso de operaciones polinomiales usadas en el proceso de codificación y decodificación dentro del campo de Galois $GF(2^8)$. Para incrementar la máxima carga útil de los datos secretos, los datos secretos compartidos corresponden a cada *k* bytes de los datos ocultos en cada bloque de 2x2 pixeles de las*n* imágenes camuflaje usando esteganografía LSB.

Los resultados de la evaluación muestran que la calidad de las imágenes camuflaje con datos secretos ocultos es mayor que la obtenida por los algoritmos presentados previamente en la literatura (Lin y Tsai, 2004; Yang y Col., 2007; Chang y Col., 2008, Wu y Col., 2012). En el esquema propuesto, la máxima carga útil de información puede ser controlada por el valor*k* del esquema de umbral *(k,n)* y el tamaño de las imágenes camuflaje. Si *k* es mayor que 4, el tamaño máximo de los datos secretos puede ser mayor que el tamaño de las imágenes camuflaje, lo cual permite una trasmisión y almacenamiento eficientes de los datos secretos. Como se mencionó anteriormente, la principal ventaja del algoritmo propuesto es la recuperación sin pérdida de los datos secretos usando operaciones en $GF(2^8)$, lo que permite que los datos secretos

puedan ser cualquier tipo de datos digitales incluyendo archivos ejecutables e incluso datos encriptados. Esta ventaja que ofrece el algoritmo propuesto hace posible una comunicación más fiable que la comunicación subliminal convencional basada en técnicas esteganográficas combinadas con algoritmos criptográficos, ya que el esquema propuesto es un esquema de secreto compartido, donde al menos *k* imágenes camuflaje son requeridas para revelar los datos secretos.

AGRADECIMIENTOS

Esta investigación fue financiada por el Consejo Nacional de Ciencia y Tecnología (CONACyT) y por el Instituto Politécnico Nacional.

REFERENCIAS

Álvarez, G., E. L. Hernández y A. Martín del Rey, *A multisecret sharing scheme for color images based on cellular automata,* Information Sciences , 178 (22), 4382-4395 (2008).

Álvarez, G., E. L. Hernández y A. Martín del Rey, *Secret color images using cellular automata with memory*. *<arXiv:cs/0312034v1> [cs.CR].* 1-17 (2003).

Ateniese, G., C. Blundo, A. De Santis y D. R. Stinson, *Extended Capability for Visual Cryptography,* Theorical Computer Science, 250(1-2), 143-161 (1996).

Blakley*, G.R., Safeguarding cryptographic keys,* AFIPS Conf. Proc. *48, 313-317 (1979).*

Chang, C.C., C.S. Tsai y T.S. Chen, *A new scheme for sharing secret color images in computer network,* In Proceedings of International Conference on Parallel and Distributed System, 21-27, Iwate, Japan, (2000).

Chang, C.C., Y.P. Hsieh y C.H. Lin, *Sharing secrets in stego-images with authentication*, Pattern Recognition, 41(10), 3130-3137 (2008).

Droste, S, *New Results on Visual Cryptography,* Lecture Notes in Computer Science, Advances in Cryptology, 1109, 401-415 (1996).

Eslami, Z., S.H. RazzaghiyJ. Zarepour, *Secret image sharing based on cellular automata and steganography*, Pattern Recognition, 43(1), 397-404 (2012).

Espejel, T. A., M. Nakano, M. Iwamoto, H.M. Pérez,*A cheating prevention EVC scheme using watermarking techniques,* Revista Facultad de Ingeniería, Univ. Antioquia, 63, 30-42, (2012).

Espejel, T. A., M. Nakano, H.M. Pérez, *Comparación entre Varios Esquemas de Criptografía Visual Extendida*, Revista Inf. Tecnol, 23(4), 105-124 (2011).

Jin, J., y Z.H. Wu, *A secret image sharing based on neighborhood configurations*, Optics and Laser Technology, 44(3), 538-548 (2012).

Lin, C.C. y W.H. Tsai, *Secret image sharing with steganography and authentication*, J. Syst. Software,73(3), 405–414 (2004).

Nakano M., E. Escamilla y H. Pérez, *Criptografía Visual basada en el esquema de umbral: Una revisión tutorial,* Revista Inf. Tecnol, 22(5), 107-120(2011).

Naor, M. y A. Shamir, *Visual cryptography*, Advances in Cryptology-Eurocrypt ’94*,* Lecture Notes in Computer Science*,* 1–12, Springer, Berlin, (1995).

Shamir, A., *How to Share a Secret,* Communications of the ACM, 22(10), 612-613 (1979).

Thien, C.C. y J.C. Lin, *Secret Image Sharing*, Computers and Graphics. 26(5), 765-770 (2002).

Tsai, D.S., G. Horng, T.H. Chen y Y.T. Huang, *A novel secret image sharing scheme for true-color images with size constraint*, Information Sciences, 179(19), 3247-3254 (2009).

Wu, X. y W. Sun,*A novel Bit Plane based Image Sharing Scheme using EVCS*, In International Conference on Information, Network and Automation (ICINA), 540-544, Guangzhou, China,(2010).

Wu, X., D. Ou, Q. Liang y W. Sun, *A user-friendly secret image sharing scheme with reversible steganography based on cellular automata*, The journal of Systems and Software, 85(8), 1852–1863 (2012).

Yang, C.N., T.S. Chen, K.H. Yu y C.C. Wang, *Improvements of image sharing with steganography and authentication*, Journal of Systems and Software, 80(7), 1070-1076 (2007).