Información Tecnológica
Vol. 23(4), 105-124 (2012)
doi: 10.4067/S0718-07642012000400013

Comparación entre Varios Esquemas de Criptografía Visual Extendida

Angelina Espejel, Mariko Nakano y Héctor Pérez
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, mnakano@ipn.mx, hmperez@ipn.mx)

Recibido Sep. 12, 2011; Aceptado Nov. 17, 2011; Versión final recibida Ene. 31, 2012

Resumen

En este trabajo se realiza una descripción y comparación de tres algoritmos de Criptografía Visual Extendida. Actualmente estos métodos son frecuentemente utilizados como base para el desarrollo de esquemas más complejos. Se obtienen resultados de la superposición de las sombras, expansión de pixeles, la calidad de la imagen resultante y las sombras, así como el número de imágenes que pueden cifrar. En un esquema convencional de criptografía visual una imagen secreta es cifrada mediante un conjunto de imágenes con apariencia de ruido pseudo-aleatorio y son repartidas a cada participante del esquema; para obtener la imagen secreta se debe superponer las imágenes recibidas. En la criptografía visual extendida las sombras son visualmente reconocibles. Se concluye que los tres métodos tienen ventajas sobre los otros dependiendo de la aplicación

Palabras clave: criptografía visual, criptografía visual extendida, esquema de secreto compartido

Comparison between various visual extended cryptography algorithms

Abstract

A description and comparison of three visual extended cryptography algorithms is presented. Currently these methods are often used as a basis for developing more complex schemes. Results related to overlapping shades, pixel expansion, quality of images and shades, and the number of coded images are obtained. In conventional visual cryptography a secret image is encrypted into a set of images that look like random-noise and are distributed to each participant of the scheme. To obtain the secret image the images received must be super-imposed. .In the extended visual cryptography the shades are visually recognizable images. It is concluded that the three methods present particular advantages depending on the application.

Keywords: visual cryptography, extended visual cryptography, secret sharing scheme.

INTRODUCCIÓN

La criptografía visual (CV) introducida en 1994 por Naor y Shamir (1994), nace del concepto del esquema de secreto compartido (Shamir, 1979), solo que en este caso aplicado a imágenes digitales. En dicho esquema, se considera una imagen digital como información secreta, la cual se desea compartir con un grupo de participantes. Dicha imagen secreta es cifrada dentro de un conjunto de imágenes con apariencia de ruido pseudo-aleatorio llamadas sombras, las cuales son repartidas a cada uno de los participantes, de tal forma que la imagen secreta puede ser revelada si un número mínimo k de sombras son superpuestas, de esta manera la información secreta es obtenida mediante el sistema visual humano (SVH). Esto permite recuperar la información secreta sin requerir equipos de cómputo de alto rendimiento como en otros esquemas criptográficos, tal es el caso de Muñoz y Rodríguez (2006), donde el cifrado de una imagen está basada en la reflexión y superposición de la intensidad de la luz, sin embargo difiere ampliamente de la CV ya que dichos algoritmos, basados en la teoría óptica, requieren de un algoritmo computacional para el descifrado de las imágenes, además de que no se basan en el esquema de secreto compartido. Las características de la CV han estimulado la investigación en este campo dando como resultado el surgimiento de la Criptografía Visual Extendida (CVE), la cual mantiene las propiedades del esquema anterior al tiempo que reemplaza las sombras pseudo-aleatorias por sombras visualmente reconocibles (VR). En la Fig. 1 se aprecian ejemplos de sombras VR.

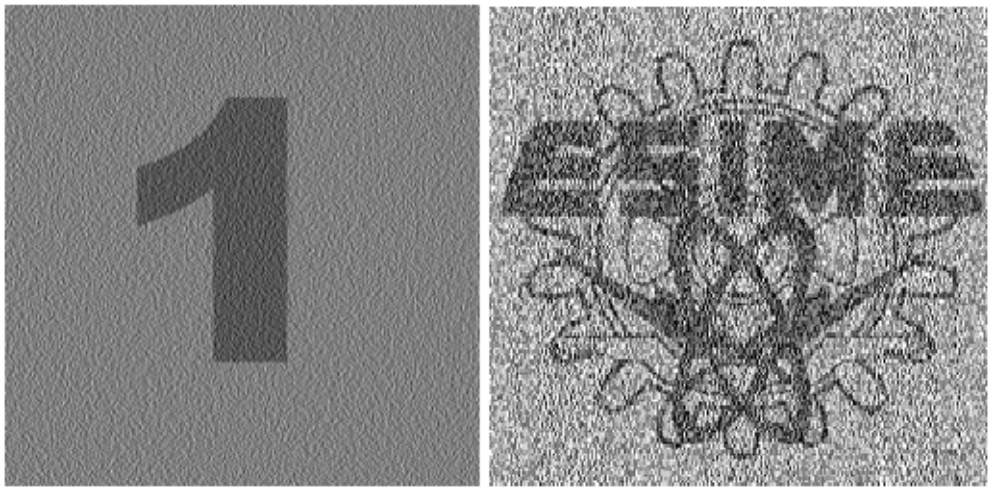


Fig. 1: Sombras Visualmente Reconocible

Con el fin de generar las sombras VR en CVE, se debe considerar tanto el color del pixel de la imagen secreta como el color del pixel de las imágenes de las sombras, por lo que el color de los pixeles de las n sombras está dado por c_i , donde $c_i \in \{1, 0\}$, $i = \{1, ..., n\}$. Esto se debe a que no solamente se cifra la imagen secreta, sino que también se asegura que las sombras VR luzcan como imágenes inocentes, lo cual complica el esquema de CVE, debido a la cantidad de pixeles que hay que representar tanto en las sombras VR como en la superposición de las mismas.

Ateniese et al. (1996a) proponen un sistema de CVE basado en estructuras de acceso general, en donde una imagen binaria es cifrada y solo se puede descifrar mediante un grupo de combinaciones de sombras definidas por el usuario llamado conjunto calificado, el cual debe satisfacer ciertas condiciones. Por otro lado se define un conjunto prohibido el cual contiene un grupo de combinaciones de sombras mediante las cuales no se puede tener acceso a dicha imagen. Droste (1996) ofrece un método de cifrado multisecreto, es decir, que se puede cifrar más de una imagen secreta en el mismo esquema. En este se define un grupo de combinaciones de sombras VR, donde cada combinación revela una imagen secreta diferente. Dicho esquema

ofrece una gran ventaja ya que más de una imagen binaria puede ser cifrada. Wang et al., (2009) propone el cifrado de una imagen binaria secreta dentro de un conjunto de sombras utilizando un umbral (k,n), el cual es generado por medio de la concatenación de matrices de CV con una matriz adicional, la cual guarda las propiedades de las imágenes de las sombras, de manera que al ser revelada la imagen secreta satisfaga las condiciones de seguridad y contraste.

Existen algunos trabajos que utilizan técnicas de halftoning para la construcción de sombras VR. La idea principal de estos métodos es modificar algunos pixeles de la imagen halftone reemplazando estos con los datos de la matriz base de CV convencional, así se asegura que las sombras son imágenes VR y al superponer estas sombras se revele la imagen secreta. En el método de Zhou et al. (2006), una imagen de sombra es transformada a dos imágenes halftone las cuales son completarías entre sí. Cada una de estas imágenes se dividen en celdas y se ubican dos pixeles que almacenaran la información de la imagen secreta. Aunque este método maneja imágenes halftone y estructuras de acceso general, requiere de imágenes complementarias, por lo que cada participante debe tener más de una sombra, de esta forma el nivel de seguridad se ve afectado. Además debido al uso de celdas, la expansión de los pixeles se incrementa, ya que la codificación de los mismos se hace dentro de cada celda, por lo que dicha celda debe ser mayor al número de subpixeles, provocando que se tenga una mayor expansión, los cual podría limitar el uso práctico de este método. En la publicación de Wang Z. et al. (2009) se proponen tres métodos como solución a las desventajas que se presentan en Zhou et al. (2006). En el primer método se propone construir las sombras después de convertir las imágenes a imágenes halftone, sin embargo siguen utilizando el concepto de imágenes complementarias. En su segundo método se utilizan pixeles auxiliares negros para cubrir la información visual de las sombras y eliminar el uso de imágenes complementarias. El tercer método modifica la sombra halftone e importa pixeles negros extra para la información visual de la sombra. Sin embargo en los últimos dos métodos se siguen utilizando celdas halftone, con lo cual la expansión de los pixeles es proporcional al tamaño de la celda. Además cualquiera de los tres métodos propuestos no permite una generalización del esquema. El algoritmo propuesto por Liu y Wu (2011), primeramente convierte las imágenes de nivel de gris en imágenes halftone usando el método de dithering, manipulando dicha matriz para generar la sombra de cada imagen. El tamaño de la matriz de dithering es la expansión real de este esquema. La calidad de las sombras construidas bajo este esquema es superior a la de los esquemas anteriores basados en halftone, debiéndose seleccionar imágenes de nivel de gris para las sombras de una manera cuidadosa, es decir deben ser claras, de lo contrario debido al proceso al que son sometidas estas pueden producir sombras muy oscuras.

Un trabajo basado en planos de bits es el de Wu y Sun (2010a), donde una imagen secreta en escala de grises se divide en planos de 8 bits, después utilizando matrices de CVE previamente generadas, se codifica cada pixel secreto en cada uno de los planos de bits, es decir cada plano de bit es tomado como si fuera una imagen binaria individual. Al terminar, se unen los 8 bits generando de esta forma las sombras. Sin embargo al decodificar la imagen secreta es necesario que cada una de las sombras se dividan en planos de 8 bits y que se superpongan por separado y se vuelvan a unir, es decir se requiere de un algoritmo computacional para revelar la información secreta, lo cual va en contra de los principios de la CV que no requiere de ningún algoritmo de cómputo para descifrar la información. De los mismos autores de este método, otro novedoso sistema de CVE es presentado en (Wu y Sun, 2010b), donde el esquema genera una sola sombra, la cual se copia y se superpone con un movimiento de traslación, con lo que la imagen secreta es revelada. El movimiento de traslación tiene que ser en un punto determinado. Aunque este sistema es novedoso debido al uso de una sola sombra, no cumple con el concepto de secreto compartido, principio en el que se basa la CV.

Algunos trabajos donde se generan esquemas de CVE utilizando imágenes a color han sido propuestos, sin embargo estos aun no representan una contribución de alto impacto, ya que siguen siendo métodos con muchas limitaciones. Por ejemplo Chen et al. (2010) proponen un método que cifra dos imágenes secretas a color bajo un umbral (2,2), las sombras son a color. Se realiza una superposición normal para obtener la primera imagen secreta, mientras que para la segunda se requiere transponer la sombra 1 sobre la sombra 2. Una de las principales

desventajas es que se limita a un umbral (2,2) con lo que no presenta una forma generalizada del esquema, y la expansión de los pixeles siempre es de m=9. Otra propuesta con imágenes a color es la de Kang et al. (2009), en donde las matrices base de un sistema de CV son utilizadas, en dichas matrices son insertados pixeles de información visual (VIP), cuya posición debe satisfacer ciertas condiciones, si estas no son cumplidas, los VIP deben reubicarse hasta tener la posición óptima, ya que estos pixeles serán sustituidos por los valores de los pixeles de las imágenes de las sombras, y a la vez codifican al pixel secreto en los tres canales de colores. Finalmente mejoran la calidad de la imagen utilizando el método de Halftone basado en el método de difusión de error. Sin embargo aunque se trata de un esquema de color para CVE, el método no utiliza imágenes secretas a color convencionales, ni hay una generalización del esquema. Por otro lado aunque el método funciona para escala de grises, al aplicarlo a colores las sombras se ven muy oscuras teniendo así un contraste pobre en la imagen resultante. Las mismas desventajas se tienen para la propuesta de Kang et al. (2011), ya que presenta el mismo método de manera màs extendida y obtiene una mejora en la calidad de la imagen resultante, sin embargo sigue teniendo los mismos inconvenientes que su antecesor. Por lo que en cuanto a sistemas de color, aun se tiene un camino que recorrer.

Considerando la literatura anterior, en este artículo se analizan los tres métodos de generación de esquemas de CVE más sobresalientes, dado que presentan aportes verdaderamente significativos, esto se demuestra con el hecho de que actualmente los algoritmos que se desarrollan para imágenes a color o escala de grises utilizan como base estos algoritmos, dichos métodos son: el método de Wang (Wang et al., 2009), el método de Ateniese (Ateniese et al., 1996), y el método de Droste (Droste, 1996). De estos tres métodos se analizan y presentan sus principales características, propiedades y el algoritmo de implementación además de algunos ejemplos, con lo que se definen de una manera más clara sus ventajas y desventajas. De esta manera, la comparación realizada entre estos métodos proporciona al lector algunos de los criterios que le permitan definir cuál es el método más conveniente de acuerdo a las necesidades del mismo. Todas las imágenes utilizadas en este artículo fueron generadas por los autores del mismo, así como las sombras y sus respectivos resultados de superposición.

Las secciones que componen el presente artículo se presentan a continuación: en la Sección “Método de Wang” se describe y analiza el método propuesto por Wang et al. (2009), en la Sección “Método de Ateniese et al.,” se proporciona una descripción y análisis del método propuesto por Ateniese et al. (1996), en la Sección “Método de Droste” se describe y analiza el método propuesto por Droste (1996). En la sección “Comparación de los tres métodos de CVE” se comparan los tres métodos mencionados anteriormente enfatizando las ventajas y desventajas de cada uno de ellos, así como sus características más relevantes. Finalmente se concluye el artículo en “Conclusiones”.

METODO DE WANG

Wang et al. (2009) propone un esquema de CVE basado en el Lema 3 de Droste (1996), donde se tiene que un par de matrices base S_0 y S_1 para un umbral (k,n), construidas bajo un esquema de CV (Naor y Shamir, 1994), al ser concatenadas con cualquier matriz booleana R de dimensiones $k \times l$, dan como resultado las matrices base B_0 y B_1 que construyen un esquema de CVE. En un umbral (k,n), las sombras son generadas de tal forma que al superponer más de k sombras se puede obtener la imagen secreta, sin embargo $(k-1)$ sombras no pueden revelar la imagen secreta, garantizando de esta forma la seguridad del esquema. Por lo que las matrices base S_0 y S_1, que serán utilizadas para generar un esquema de CVE conservan esas mismas propiedades. Por consiguiente Wang et al. (2009) proponen la construcción de una matriz R denominada A_{Binary}.

Algoritmo

El algoritmo de Wang se ilustra en el diagrama de bloques que se muestra en la Fig. 2:

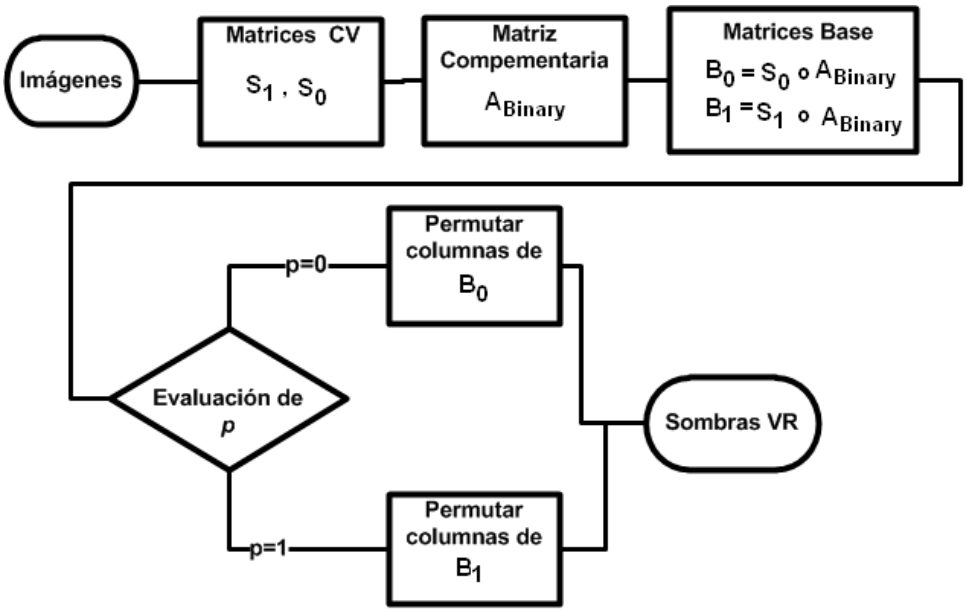


Fig. 2: Diagrama a bloques del Algoritmo de Wang

En la Fig. 2, se muestra que en primera instancia se deben construir las matrices base S_0 y S_1 de CV y la matriz A_{Binary}. Posteriormente las matrices base de CVE son obtenidas mediante la concatenación de S_0, S_1 con A_{Binary}. Cuando un pixel de la imagen secreta es seleccionado para cifrarlo, se evalúa, si el pixel secreto es de color blanco ($p = 0$), las columnas de la matriz B_0 son permutadas para la construcción de las sombras VR, sin en cambio si el pixel secreto es negro ($p = 1$), entonces las columnas de la matriz B_1 son permutadas. Al término del proceso se obtienen las sombras VR.

Construcción de matrices base

Para un umbral (k, n) de un esquema de CVE en el que una imagen secreta se cifra, una matriz adicional A_{Binary} debe generarse para construir las matrices bases de CVE. La matriz A_{Binary} tiene por consiguiente dimensiones $n \times m_0$, donde n es el número de participantes y sombras VR que se van a generar mientras que m_0 es el número de columnas que se obtienen mediante (1).

$$m_0 \geq \left\lceil \frac{n}{k-1} \right\rceil \qquad (1)$$

Algunos valores de los elementos de la matriz A_{Binary} varían dependiendo del color de los pixeles de las sombras y el resto de los elementos se fijan con valor de 1. Los elementos con valores variables se denotan con '*'. La matriz A_{Binary} tiene que satisfacer las dos condiciones siguientes.

1.- Cada fila de A_{Binary} tiene solo un '*'.
2.- El número de '*' en cada columna es a lo mucho $(k-1)$.

Contraste y Seguridad

Para garantizar la seguridad de este esquema, es necesario que se cumpla la condición (2).

$$H\left(V^{k}_{B_0}\right) = H\left(V^{k}_{B_1}\right) \quad (2)$$

Donde H es el peso de Hamming del vector resultante V cuando las matrices B_0 y B_1 son restringidas a k filas, de tal forma que no es posible saber de qué matriz provienen los subpixeles que representan a los pixeles secretos. La expansión de las matrices base m_{B_p} se obtiene mediante (3).

$$m_{B_p} = m_{S_p} + m_{A_{Binary}}, \qquad p = \{1,0\} \quad (3)$$

Donde m_{S_p} es la expansión de los pixeles de las matrices base de un esquema de CV y $m_{A_{Binary}}$ es la expansión de los pixeles de la matriz A_{Binary}. En cuanto a la diferencia relativa para este esquema, se denota por α_B y está dada por (4), donde α_{S_p} es la diferencia relativa de las matrices base del esquema de CV.

$$\alpha_B = \alpha_{S_p} \times m_{S_p}/m_{A_{Binary}}, \qquad p = \{1,0\} \quad (4)$$

Supóngase que se tiene un umbral $(3,4)$ con las imágenes binarias de la Fig. 3, donde la imagen secreta es (a).

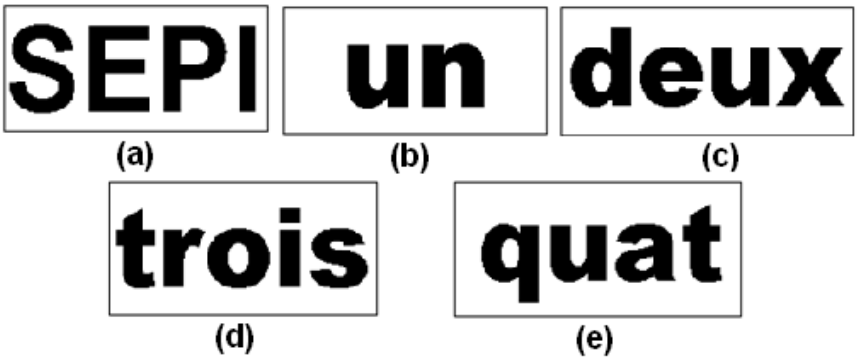


Fig. 3: (a) Imagen secreta. (b), (c), (d) y (e) Imágenes de sombras.

El primer paso del algoritmo de Wang et al. (2009), se refiere a la construcción de las matrices base S_0 y S_1. Dado que para este ejemplo se tiene $k = 3$, es recomendable construir las matrices base de CV utilizando el algoritmo para generar un umbral $(3,n)$, propuesto por Naor y Shamir (1994), o bien siguiendo el tutorial presentado por Nakano et al. (2011), donde $n = 4$, para este caso. Con lo que se obtendrán las matrices para un umbral $(3,4)$, donde m_S es la expansión en pixeles, que para este caso es $m_S = 6$ y $n = 4$, tal y como se muestra en (5).

$S_0 =$ ▯ EMBED Equation.3 ▯▯▯ $S_1 =$ ▯ EMBED Equation.3 ▯▯▯ (5)

En (5), la matriz S_0 representa los pixeles blancos y la matriz S_1 representa los pixeles negros de la imagen secreta. La segunda etapa del algoritmo es la construcción de la matriz A_{Binary}. Dado que se tiene $n = 4$ y $k = 3$ se obtiene una $m_0 = 2$ mediante (1), por lo que se obtiene una matriz A_{Binary} como se muestra en (6).

$$A_{Binary} = \begin{bmatrix} * & 1 \\ * & 1 \\ 1 & * \\ 1 & * \end{bmatrix} \quad (6)$$

En (6), $* \in \{1, 0\}$ representa el color del pixel de la sombra a la que corresponde dicha fila de la matriz A_{Binary}. De esta forma, en cada iteración i la matriz A_{Binary} cambiará en función de los valores de los pixeles de las imágenes de las sombras. El siguiente paso en el algoritmo, es el de la construcción de las matrices base B_0 y B_1 las cuales permitirán la construcción del esquema de CVE. Para ello es necesario concatenar las matrices obtenidas en (5) con la matriz obtenida en (6), de esta forma se obtienen las matrices base que se muestran en (7).

$B_0 =$ EMBED Equation.3 $\qquad B_1 =$ EMBED Equation.3 (7)

En (7), la matriz que representa los pixeles blancos es B_0 y la matriz que representa los pixeles negros es B_1. Aplicando (3) y (4) se obtiene una expansión de pixeles $m_{B_P} = 8$ y una diferencia relativa $\alpha_B = 1/8$. Una vez obtenidas estas matrices, solo resta seleccionar una de ellas en cada iteración dependiendo del color del pixel de la imagen secreta y los valores de los pixeles de las imágenes de las sombras que serán sustituidos, para así después permutar las columnas de la matriz elegida y construir las sombras VR. Las sombras VR obtenidas se muestran en la Fig. 4.

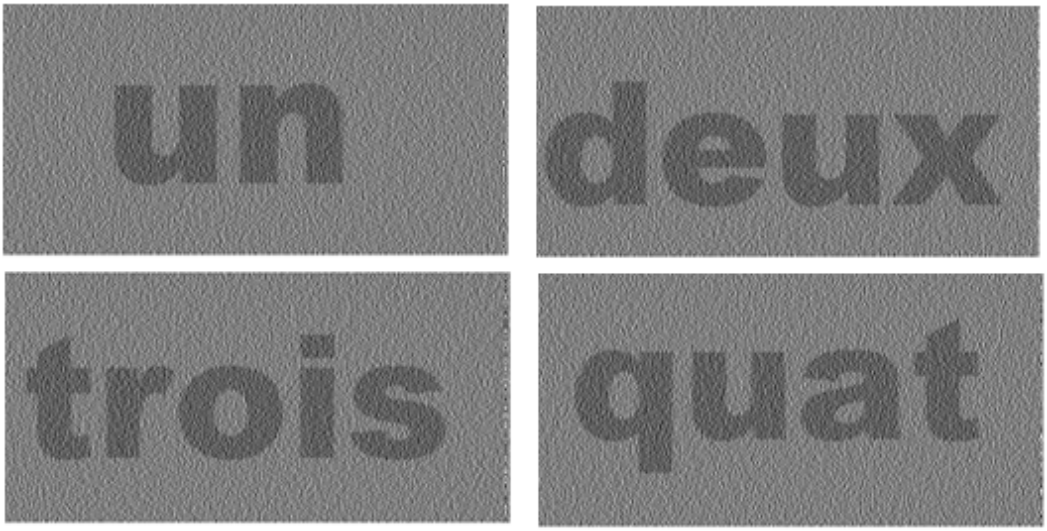


Fig. 4: Sombras VR para un umbral (3,4) de un esquema de CVE.

El resultado de la superposición de las sombras VR denotado por Δ es el que se muestra en la Fig. 5.

Fig. 5: Superposición de sombras VR para un umbral $(3,4)$. (a) $\Delta_{\{1,2,3,4\}}$, (b) $\Delta_{\{1,2,3\}}$.

Supóngase que se requiere cifrar un pixel blanco y uno negro de la imagen secreta, y que se tienen los siguientes colores de pixeles de las imágenes de las sombras: negro, blanco, negro y blanco, lo que equivale a tener el siguiente vector: $[1\ 0\ 1\ 0]$. Al sustituir estos valores en las posiciones de las matrices de (7) donde se tenga $*$, estas quedan como en (8).

$$B_0 = \text{EMBED Equation.3} \cdot \text{EMBED Equation.3} \qquad B_1 = \text{EMBED Equation.3} \tag{8}$$

Si las matrices (8) son restringidas a $k-1$ filas se obtienen las siguientes matrices:

$$A_0 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad A_1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \tag{9}$$

Los pesos de Hamming para las matrices de (9) están dados por $H(A_0) = 6$ y $H(A_1) = 6$ por lo que satisfacen la condición dada en (2). Por lo que la seguridad está garantizada tal y como se puede observar en la Fig. 6.

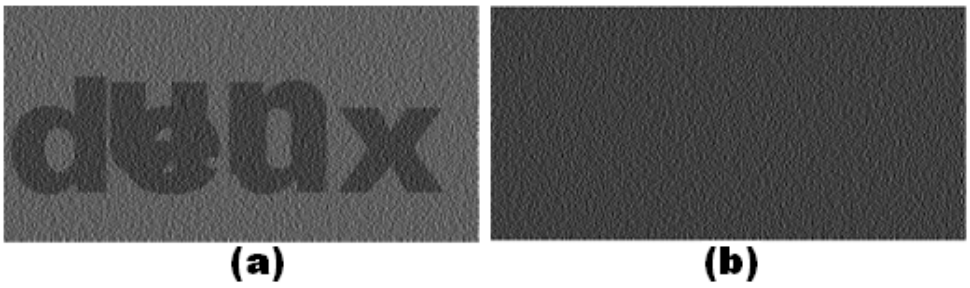


Fig. 6: Superposición de $(k-1)$ sombras VR para un umbral $(3,4)$ de un esquema de CVE donde (a) $\Delta_{\{1,2\}}$ y (b) $\Delta_{\{2,3\}}$.

METODO DE ATENIESE

Ateniese et al. (1996a) propone la construcción de un esquema de CVE basado en acceso general denominado como (Δ_Q, Δ_F)-CVE y la teoría de hipergrafo. En este método las estructuras de acceso general determinan que subconjuntos de participantes Δ_Q pueden revelar la imagen

secreta y cuáles Δ_F tienen acceso restringido, mientras que la teoría de hipergrafo es utilizada para resolver el problema de coloramiento cuando se lleva a cabo la construcción de las sombras VR.

Un hipergrafo es un conjunto de grafos definido como $H = (X, E)$, donde X es un conjunto de vértices y E es un conjunto de aristas. Utilizando las definiciones de hipergrafo en términos de criptografía visual se tiene que: $X = P$ y $E = \Delta_O$, donde *P* es el conjunto de los participantes y Δ_O es conjunto mínimo calificado que se define como $\Delta_o = \{A \in \Delta_Q : A' \notin \Delta_F \text{ for all } A' \subset A\}$.

Con lo que el problema (Δ_Q, Δ_F)-CVE, se convierte en un problema de grafo (P, Δ_O). Dicho problema es denominado "coloramiento-q", de tal forma que se busca asignar un color a cada vértice donde ninguna arista e_j tiene en sus vértices el mismo color. En tal caso se debe obtener una función de mapeo φ tal que $\varphi: X \rightarrow \{1, 2, \ldots, q\}$, donde q es el número de colores.

Algoritmo

En la Fig. 7 se muestra el diagrama a bloques del algoritmo de Ateniese:

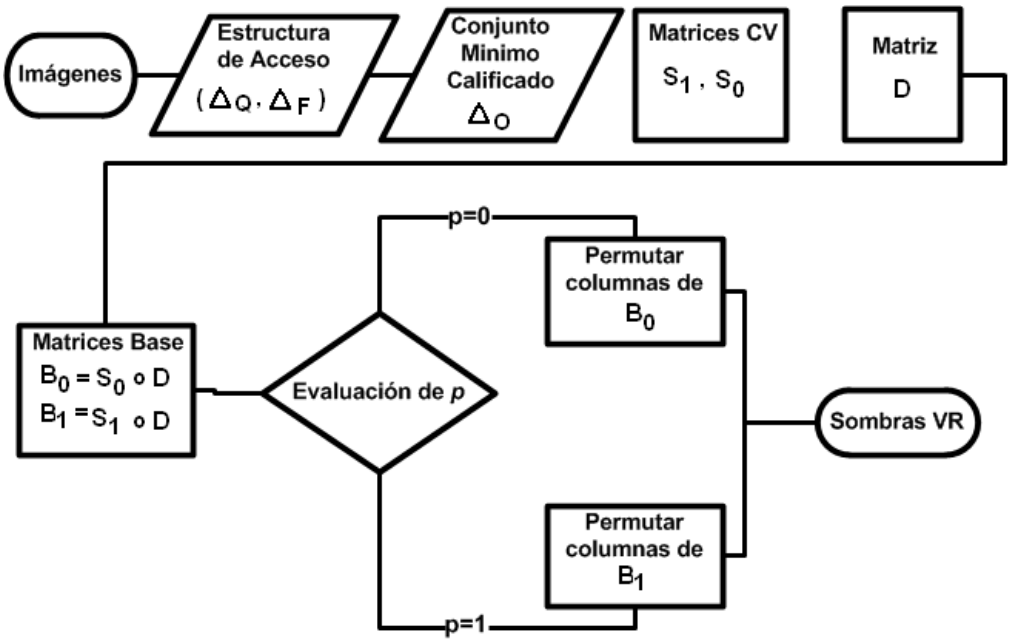


Fig. 7: Diagrama a bloques del Algoritmo de Ateniese

En el Algoritmo de Ateniese, se define una estructura de acceso, a partir de la cual se obtendrá el conjunto mínimo calificado (Ateniese et al., 1996). Una vez obtenido dicho conjunto, se procede a construir las matrices base S_0 y S_1 de CV (Naor y Shamir, 1994), y la matriz D , de tal forma que estas serán concatenadas para obtener las matrices base de CVE: B_0 y B_1 . Finalmente tiene lugar la evaluación del color de los pixeles de la imagen secreta, de tal forma que en cada iteración se selecciona una de las matrices base para permutar las columnas de dicha matriz y construir las sombras con los subpixeles dados en cada fila de la matriz.

Construcción de matrices base

Para la construcción de las matrices base: B_0 y B_1, se requiere de dos matrices previamente construidas: las matrices base S_0 y S_1 de un esquema de CV y la matriz D . Las matrices S_0 y S_1

son construidas mediante CV basado en Ateniese et al. (1996b). La matriz D es una matriz cuyos valores dependerán de los colores de los pixeles de las imágenes inocentes y de la función φ del hipergráfo. La matriz D tiene dimensiones $n \times q$ y se construye de la siguiente forma:

Para $i = 1$ hasta n
Si $c_i = b$ entonces $D(i,:) = 1$
Otro caso $D(i,:) = 1$, $D(i,\varphi(j)) = 0$
Fin

Donde c_i representa el color del pixel de la i-esima imagen de sombra y (w,b) son los colores blanco y negro, respectivamente. Una vez obtenidas las matrices S_0, S_1 y D, se procede a construir las matrices base del esquema: $B_c^{c_1,\ldots,c_n}$, bajo la condición (10), donde c es el color del pixel secreto y c_i representa el color del pixel de la i-esima imagen de sombra.

$$B_c^{c_1,\ldots,c_n} = \begin{cases} S_0 \circ D^{c_1,\ldots,c_n} & \text{si } c = w \\ S_1 \circ D^{c_1,\ldots,c_n} & \text{si } c = b \end{cases} \quad (10)$$

Contraste y Seguridad

Para que un esquema de CVE construido por el método de Ateniese et al. (1996a) sea seguro y presente un buen contraste debe satisfacer las siguientes propiedades: Sean $B_w^{c_1,\ldots,c_n}$ y $B_b^{c_1,\ldots,c_n}$ un par de colecciones de matrices booleanas donde $c_1,\ldots,c_n \in (b,w)$:

1. Cualquier combinación de participantes tal que $X \in \Delta_Q$ puede revelar la imagen secreta.

Cuando el pixel de la imagen secreta es blanco: $M \in B_w^{c_1,\ldots,c_n}$

$$h(OR(M_X)) \leq t_X - \alpha(m) \cdot m \quad (11)$$

Cuando el pixel de la imagen secreta es negro: $M \in B_b^{c_1,\ldots,c_n}$

$$h(OR(M_X)) \geq t_X \quad (12)$$

donde $h(X)$ es el peso de Hamming, $\alpha(m)$ es la diferencia relativa y t_X el umbral de contraste.

2. Ninguna combinación de participantes tal que $X \in \Delta_F$ puede revelar la imagen secreta. Si $X = \{i_1, i_2, \ldots, i_p\} \in \Delta_F$ entonces al permutar las columnas de las matrices base, estas deben ser indistinguibles entre sí, es decir, no se debe saber de dónde provienen los subpixeles.

$$B_w^{c_2,\dots,c_n}(X,:) = B_b^{c_2,\dots,c_n}(X,:) \tag{13}$$

3. Las sombras son sombras VR. La región blanca de las sombras VR tienen menos 1's que las regiones negras, esto es : Si $c_1 = blanco$ y $c_1 = negro$ entonces $h\left(B_w^{c_2,\dots,c_n}(1,:)\right) < h\left(B_b^{c_2,\dots,c_n}(1,:)\right)$ Si $c_1 = c_1$ entonces $h\left(B_w^{c_2,\dots,c_n}(1,:)\right) = h\left(B_b^{c_2,\dots,c_n}(1,:)\right)$.

Las propiedades 1 y 2 garantizan la seguridad del esquema, mientras que la tercera propiedad asegura el contraste de la imagen secreta en la superposición.

Se tiene un conjunto de participantes $P = \{1,2\}$, con sus respectivos conjuntos calificado y prohibido: $\Delta_Q = \{\{1,2\}\}$ y $\Delta_F = \{\{1\},\{2\}\}$ respectivamente. Finalmente el conjunto mínimo calificado se define como $\Delta_0 = \{\{1,2\}\}$. Se tienen las imágenes binarias de la Fig. 8 para la construcción del esquema.

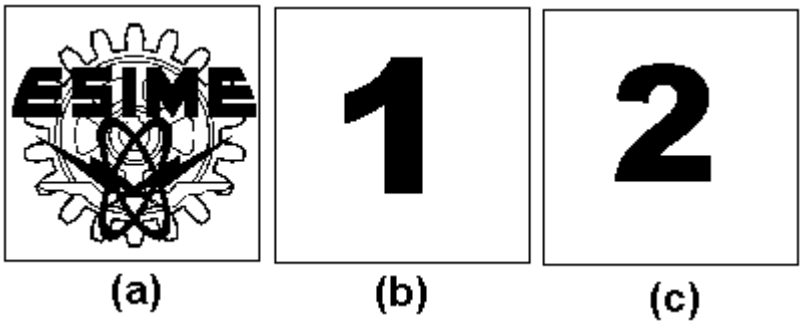


Fig. 8: (a) Imagen secreta, (b) y (c) Imágenes inocentes para sombras.

Se construyen las matrices base S_0 y S_1 usando Naor y Shamir (1994), por lo que se obtienen las siguientes matrices:

$$S_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{14}$$

Después se construye la matriz D usando una función de mapeo $y = \varphi(x)$ que asigna un participante $x \in \{1,2\}$ a un de dos colores $y \in \{1,2\}$. Un ejemplo de la función de mapeo $\varphi(x)$ es $\varphi(1) = 1, \varphi(2) = 2$. Aplicando la regla de la construcción de la matriz D con diferentes combinaciones de c_1, c_2, se puede obtener la matriz D como se muestra en tabla 1.

Tabla 1: Construcción de la matriz $\mathbf{D}$ (ejemplo)

c_1	c_2	Procesos	Matriz *D*
w	w	$D(1,\varphi(1)) = D(1,1) = 0,\ \ D(1,\varphi(2)) = D(1,2) = 0$. Los demás elementos son 1	$D^{ww} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
w	b	$D(1,\varphi(1)) = D(1,1) = 0$. Los demás elementos son 1	$D^{wb} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
b	w	$D(1,\varphi(2)) = D(1,2) = 0$. Los demás elementos son 1	$D^{bw} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$
b	b	Todos los elementos son 1	$D^{bb} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

Finalmente se concatenan las matrices base de CV y la matriz $\mathbf{D}$, por lo que se obtiene (15).

$$
\begin{aligned}
B_w^{ww} &= \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \circ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} & B_b^{ww} &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \\
B_w^{wb} &= \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \circ \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} & B_b^{wb} &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \\
B_w^{bw} &= \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \circ \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} & B_b^{bw} &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \\
B_w^{bb} &= \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \circ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} & B_b^{bb} &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}
\end{aligned}
\qquad (15)
$$

Las matrices dadas por (15) tienen una expansión $\mathbf{m = 4}$ y una diferencia relativa de $\alpha(m) = \frac{1}{4}$, por lo que si utilizamos (11) en las matrices de la columna izquierda en (15), obtenemos un peso de Hamming $\mathbf{h = 3}$, mientras que utilizando (12) en las matrices de la columna derecha en (15) se obtiene $\mathbf{h = 4}$, con lo que las condiciones (11) y (12) quedan satisfechas. En la Fig. 9 se presentan las sombras obtenidas por medio de este método y el resultado de la superposición.

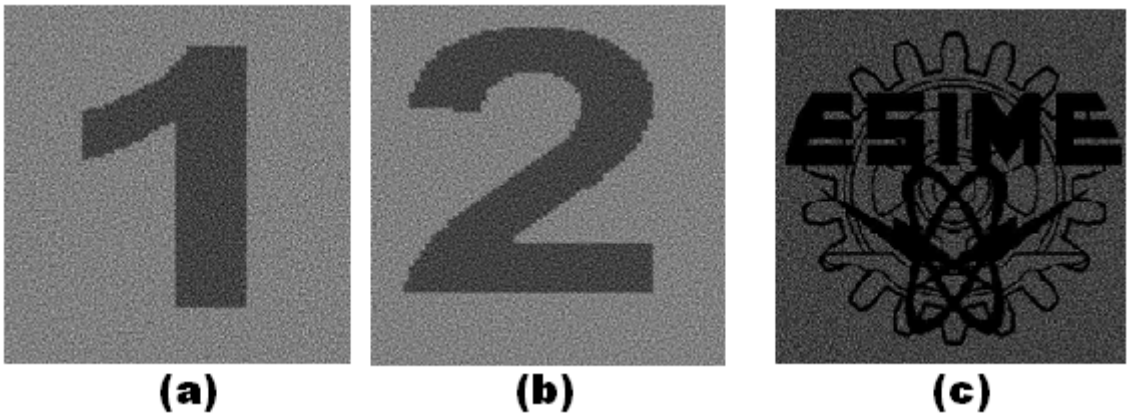


Fig. 9: (a) y (b) sombras VR, (c) $\Delta_{a,b}$.

En cuanto a la seguridad, si restringimos las matrices B_w^{ww} y B_b^{ww} de (15), a una sola fila se obtiene que:

$$B_w^{ww} = [1\ 0\ 1\ 0] = B_b^{ww} = [0\ 1\ 1\ 0] \tag{16}$$

Las matrices en (16) tienen los mismos elementos y las mismas frecuencias por lo que son indistinguibles entre sí, con lo que la condición (13) se satisface al no saber de qué matriz provienen los subpixeles.

METODO DE DROSTE

A diferencia de los dos métodos anteriormente expuestos, Droste (1996) propone un esquema de CVE multisecreto, con lo que $(2^n - 1) - n$ imágenes pueden ser cifradas, dicho método por tanto no está basado en ningún algoritmo de CV.

En el método de Droste (1996) se tiene un conjunto de participantes $P = \{1, \ldots, n\}$ y un subconjunto $Z \subseteq P$ que define todas las combinaciones de $\{1, \ldots, n\}$ que van a revelar las imágenes secretas. Si se tuviera $n = 3$, se tiene que $P = \{1,2,3\}$, se tienen entonces 3 participantes, por lo que las combinaciones que se pueden generar con este grupo de participantes están definidas por $Z = \{\{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. Donde en Z los subconjuntos que solo contengan un elemento como: $\{1\}, \{2\}, \{3\}$ representan las sombras VR, mientras que los subconjuntos que contengan dos o más elementos, representan la superposición $\Delta_{\{i_1, \ldots, i_q\}}$ de las *q* sombras VR de dichos elementos donde $1 < q \leq n$, es decir las combinaciones entre las sombras de cada participante.

Debido a que Droste (1996) permite cifrar más de una imagen secreta, la cantidad de pixeles a considerar aumenta considerablemente, ya que se tienen $2^{|Z|}$ diferentes combinaciones de pixeles blancos y negros, donde $|Z|$ es el número de elementos de Z, por lo que para estas $2^{|Z|}$ combinaciones se requieren de $2^{|Z|}$ matrices base. Cada una de las matrices base serán

denotadas por B^D, donde B es la matriz base y D es un índice tal que $D \subseteq Z$. Dicho índice es necesario para manipular las $2^{|Z|}$ combinaciones, y tiene las siguientes propiedades:

$$\text{Si } \{i_1, \ldots, i_q\} \in D \quad \text{entonces } \Delta_{\{i_1,\ldots,i_q\}} = 1$$
$$\text{Si } \{i_1, \ldots, i_q\} \notin D \quad \text{entonces } \Delta_{\{i_1,\ldots,i_q\}} = 0 \qquad (17)$$

En (17), si uno de los subconjuntos de Z no se encuentra en el subconjunto D o índice D, la superposición de dicho subconjunto tendrá valor de 0, es decir se representará como blanco, mas si en cambio, si dicho subconjunto sí se encuentra dentro del índice D, la superposición será representada como negro con el valor 1.

Algoritmo

La Fig. 10 muestra el diagrama a bloques del método de Droste.

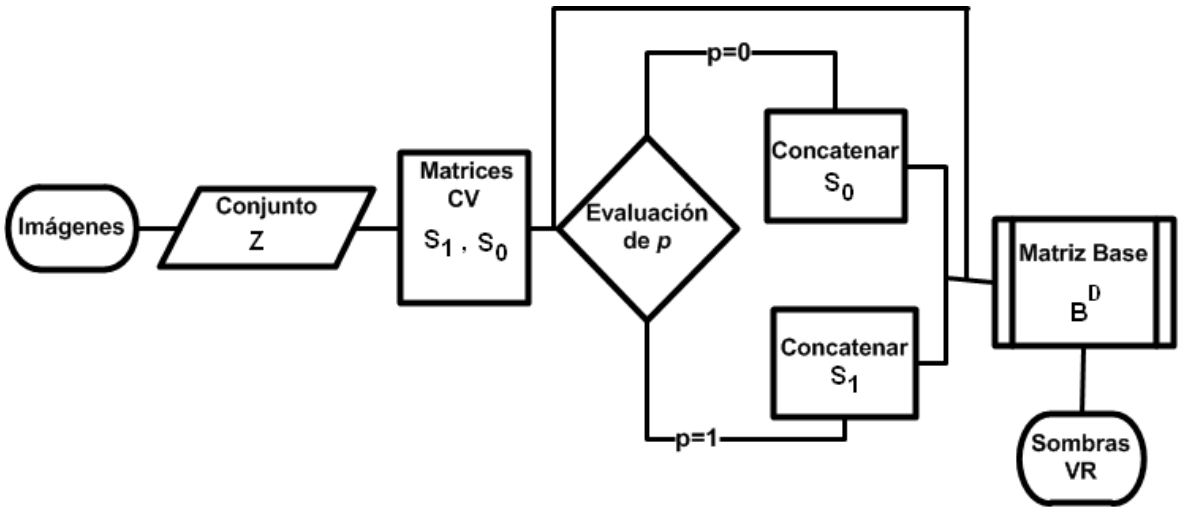


Fig. 10: Diagrama a bloques del Algoritmo de Droste

Primeramente se define el conjunto de combinaciones de sombras que van a revelar una imagen secreta, recordando que cada combinación puede revelar una imagen secreta diferente. En base a estas combinaciones se definen las matrices base para el color blanco y negro de cada una de las combinaciones de las sombras. Dependiendo de la evaluación de los pixeles se seleccionan las matrices correspondientes para cada color y se concatenan para construir la matriz base B^D, para cada iteración hay una matriz B^D diferente. Finalmente se obtienen las sombras.

Construcción de matrices base

En Droste (1996), para representar los valores “1” y “0” en las superposiciones $A_{\{i_1,\dots,i_q\}}$ se construyen matrices base S_0 y S_1 de un umbral (k, n) de un esquema de CV, para ello se utilizan las construcciones propuestas por Naor y Shamir (1994). El umbral que se requiera para generar cada una de las matrices dependerá del número de sombras que tenga el subconjunto al cual van a representar y del valor de la superposición, por lo que antes de generar las matrices B^D, es necesario definir las matrices S_0 y S_1 de CV para cada uno de los subconjuntos, por lo que por cada subconjunto habrá una matriz S_0 y S_1, para representar los valores “1” y “0”. La matriz B^D es diferente en cada iteración, y esta se construye concatenando las matrices base de cada uno de los subconjuntos en base al índice D. En el ejemplo se puede apreciar mejor como es que se obtiene la colección de matrices B^D.

Contraste y Seguridad

La expansión m de las matrices base B^D, depende del número de combinaciones que se hayan designado para dicho esquema, ya que entre más combinaciones de sombras VR haya, más subpixeles serán necesarios para representarlas, m se obtiene con la ecuación (18).

$$m = \sum_{q=1}^{n} 2^{q-1} \cdot b_q \qquad (18)$$

Las matrices base B^D deben de cumplir las siguientes condiciones dadas por Droste (1996) para que se garantice el contraste y la seguridad.

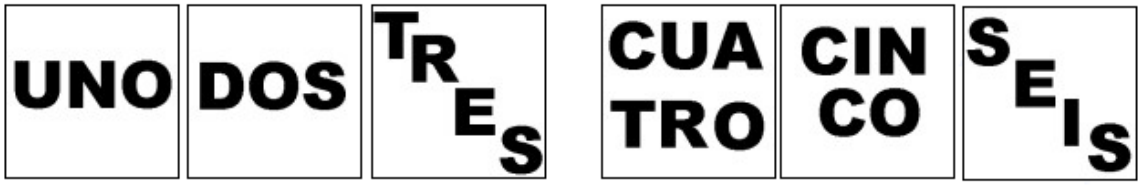
1. Para todo $\{i_1,\dots,i_q\} \subseteq Z$ hay una $d\{i_1,\dots,i_q\}$ tal que el peso de Hamming para la operación OR de las filas $\{i_1,\dots,i_q\}$ sea al menos $d\{i_1,\dots,i_q\}$ para todas las matrices B^D donde $\{i_1,\dots,i_q\} \subseteq D$.

2. Para todo $\{i_1,\dots,i_q\} \subseteq Z$ hay una $\alpha\{i_1,\dots,i_q\}$ tal que el peso de Hamming para el OR de las filas $\{i_1,\dots,i_q\}$ sea al menos $d\{i_1,\dots,i_q\} - \alpha\{i_1,\dots,i_q\} \cdot m$ para todas las matrices B^D donde $\{i_1,\dots,i_q\} \not\subseteq D$.

3. Para todo $\{i_1,\dots,i_q\} \subseteq \{1,\dots,n\}$, las restricciones de las matrices B^D a $\{i_1,\dots,i_q\}$ filas, contienen los mismos elementos con las mismas frecuencias para todo D.

Las dos primeras propiedades aseguran el contraste de la imagen y la tercera propiedad asegura la seguridad del esquema.

Se tiene un conjunto de participantes $P = \{1,2,3\}$ donde se definen las combinaciones dadas por $Z = \{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\}$, nótese que en este caso no se están utilizando todas las combinaciones que existen para este conjunto de participantes. Utilizando $(2^n - 1) - n$, se sabe que se pueden cifrar máximo 4 imágenes, sin embargo dado el conjunto de combinaciones Z, solo se cifran 3 imágenes. Las imágenes secretas y las imágenes de las sombras para construir este esquema se muestran en la Fig. 11.



(a) (b)

Fig. 11: (a) Imágenes Inocentes (b)Imágenes Secretas

Siguiendo el algoritmo de la Fig. 10 se definen las matrices base para cada uno de los subconjuntos de Z, tal y como se muestra en la Tabla 2.

Tabla 2: Matrices base para los subconjuntos de Z

Z	{1}	{2}	{3}	{1, 2}	{1, 3}
$\{i_1,\ldots,i_q\} \in D$ $\Delta_{\{i_1,\ldots,i_q\}} = 1$	$\begin{bmatrix}1\\1\\1\end{bmatrix}$	$\begin{bmatrix}1\\1\\1\end{bmatrix}$	$\begin{bmatrix}1\\1\\1\end{bmatrix}$	$\begin{bmatrix}1&0\\0&1\\1&1\end{bmatrix}$	$\begin{bmatrix}1&0\\1&1\\0&1\end{bmatrix}$
$\{i_1,\ldots,i_q\} \in D$ $\Delta_{\{i_1,\ldots,i_q\}} = 0$	$\begin{bmatrix}0\\1\\1\end{bmatrix}$	$\begin{bmatrix}1\\0\\1\end{bmatrix}$	$\begin{bmatrix}1\\1\\0\end{bmatrix}$	$\begin{bmatrix}0&1\\0&1\\1&1\end{bmatrix}$	$\begin{bmatrix}0&1\\1&1\\0&1\end{bmatrix}$

Suponiendo que se tiene un índice $D = \{\{1\},\{1,3\}\}$ se obtiene la matriz (19), que corresponde a dicho índice, concatenando las matrices de la Tabla 2.

$$B^{(\{1\},\{1,3\})} = \begin{bmatrix}1\\1\\1\end{bmatrix} \circ \begin{bmatrix}1\\0\\1\end{bmatrix} \circ \begin{bmatrix}1\\1\\0\end{bmatrix} \circ \begin{bmatrix}0&1\\0&1\\1&1\end{bmatrix} \circ \begin{bmatrix}1&0\\1&1\\0&1\end{bmatrix} \circ \begin{bmatrix}0&1\\1&1\\0&1\end{bmatrix} \quad (19)$$

La matriz que se obtiene en (19) es una matriz base con una expansión $m = 9$. Solo resta permutar las columnas de cada una de las $2^{|Z|}$ matrices base, que corresponden a cada uno de

los $2^{|Z|}$ índices y construir las sombras. Para este ejemplo, las sombras obtenidas se muestran en la Fig. 12.

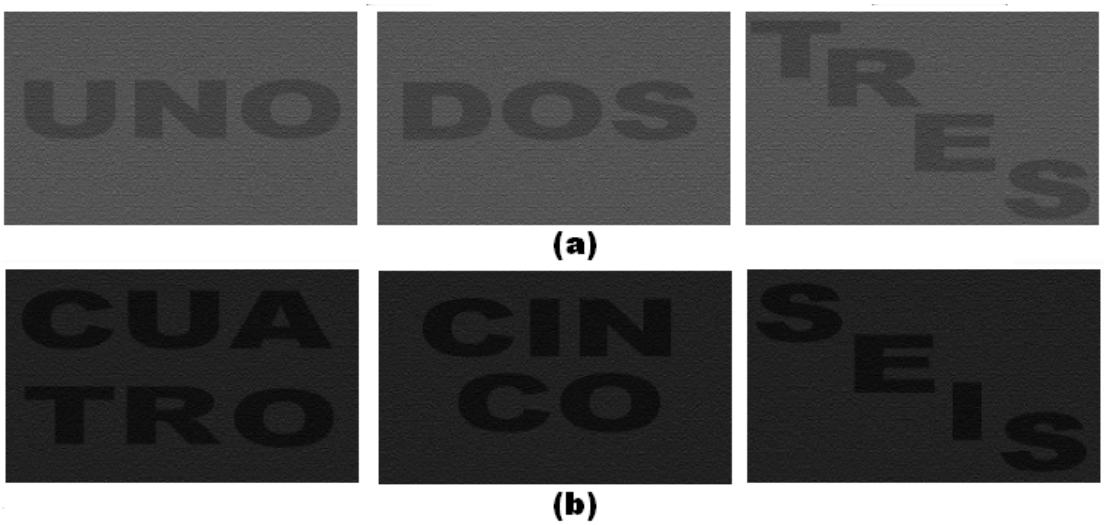


Fig. 12: (a) Sombras VR (b)Superposiciones: $\Delta_{\{1,2\}}$, $\Delta_{\{1,3\}}$ y $\Delta_{\{2,3\}}$ respectivamente.

COMPARACION DE LOS TRES METODOS DE CVE

Para poder comparar los tres métodos desde el punto de vista de la calidad de la imagen revelada e imágenes de sombra se empleó la relación señal a ruido pico (PSNR), sin embargo debido a que la expansión imposibilita un cálculo directo del PSNR y los tres métodos operan de manera distinta se tomaron las siguientes consideraciones. Para calcular el PSNR las imágenes originales fueron manipuladas debido a la expansión introducida por la CVE en las imágenes resultantes. Debido a que la construcción de los tres métodos difiere ampliamente uno del otro, para realizar una comparación adecuada entre los tres métodos, se ha elegido un umbral (3,3); por lo que para el caso de Ateniese, se define un único conjunto calificado, el cual es: {1,2,3}, y para el caso de Droste, a pesar de que es multisecreto, se cifra solamente una imagen secreta en la combinación de sombras {1,2,3}. De esta forma los tres métodos generan 3 sombras las cuales son requeridas para recuperar una sola imagen secreta. La tabla 3 muestra la comparación de los tres métodos usando varias imágenes de prueba, una de las cuales se muestra en la Fig. 3.

Tabla 3: Tabla comparativa de expansión, calidad de imágenes y sombras obtenidas en cada método.

	Wang	Ateniese	Droste
Expansión de pixel (m)	6	4	7
Contraste	1/3	1/2	1/4
Calidad de la imagen revelada	1.91 dB	2.96 dB	1.79 dB

Calidad de las sombras	3.34 dB	4.22 dB	2.94 dB

En la tabla 3 se puede observar que el método de Ateniese presenta la menor expansión en las imágenes resultantes en comparación con el método de Droste y Wang, ya que tiene una expansión de m=4, por lo que las dimensiones de las imágenes resultantes son solo el doble de la imagen original. En lo que respecta al PSNR, en el caso de la imagen resultante, Ateniese presenta el PSNR más alto con 2.96 dB, al igual que las sombras generadas por dicho método, las cuales tienen el PSNR más alto en comparación con el obtenido de las sombras generadas por los otros dos métodos. Por otro lado Wang presenta un PSNR menor que Ateniese, tanto para la imagen secreta resultante como para las sombras, al igual que presenta una mayor expansión en las imágenes que genera con m=6, sin embargo en comparación con el método de Droste, tiene mejores resultados en cuanto la calidad de las imágenes se refiere, por lo que Droste es el método que presenta una mayor expansión y menor calidad de las imágenes, ya que presenta el PSNR más bajo, sin embargo Droste es un método multisecreto, y aunque presenta un PSNR bajo, para este caso donde solo se cifra una imagen, la expansión tiene un cambio poco significativo como cuando cifra más de una imagen, como ya se puede observar en la Fig. 12, donde cifra tres imágenes secretas y su m=9, mientras que para el caso de la tabla 3, la m=7 con solo una imagen secreta cifrada.

A continuación se presentan los puntos clave de cada uno de los métodos anteriormente expuestos.

Como se observa en la tabla 4, si se desea cifrar más de una imagen secreta, la mejor opción que se propone utilizar es el método de Droste, ya que es el único método que propone un esquema de CVE multisecreto, y aunque presenta una desfavorable expansión de pixeles al incrementar el número de combinaciones de participantes, esta puede optimizarse usando el método de Klein y Wessler (2007). Por otro lado, a pesar de tener un bajo PSNR, como se pudo observar en la tabla 3, esto es debido a que el método está desarrollado para cifrar varias imágenes secretas de tal forma que tenga una expansión mínima, por lo que cuando una sola imagen es cifrada puede mostrar ese tipo de puntos desfavorables.

Tabla 4: Comparación de métodos de CVE

	Wang	*Ateniese*	*Droste*
Número máximo de imágenes secretas	1	1	$(2^n - 1) - n$
Método Basado	(k, n)-CV	Estructuras de Acceso general	Concatenación de matrices (n, n)-CV
Optimización	Reducción de m en matrices base CV	Reducción de m en matrices base CV El mejor hipergrafo	Reducción de m por (Klein y Wessler, 2007)
Ventajas	Implementación en base a cualquier umbral (k, n)	Capacidad de definir conjuntos Δ_Q y Δ_F	Esquema de CVE multi-secreto
Desventajas	Limitado a una imagen secreta.	Limitado a una imagen secreta. Complejidad alta debido al algoritmo de	Aumento considerable de m si se usan todas las combinaciones para ocultar imagen secreta

		coloramiento-q (NP-Duro).	

Si se desea cifrar solo una imagen secreta o utilizar un umbral (k,n) se puede utilizar el método de Wang, puesto que presenta una implementación bastante versátil al construirse a partir de cualquier umbral (k,n) de CV, aunque la expansión es mucho mayor que en la del método de Ateniese, esta podría optimizarse reduciendo el factor m de las matrices CV. Y de acuerdo a la tabla 3, los niveles de PSNR que se obtuvieron si bien están por debajo de los obtenidos por Ateniese, se aproximan bastante.

Si se desea cifrar una imagen y definir más específicamente que conjunto de participantes tiene acceso a ella, se sugiere utilizar el método de Ateniese, ya que es bastante versátil en definir una estructura que permite delimitar el acceso a la imagen de una manera segura, y presenta además el factor m más bajo con respecto a los otros dos métodos y un PSNR mayor, como se muestra en la tabla 3, sin embargo su implementación es bastante compleja debido al coloramiento-q, y como ya se menciona solo puede cifrar una imagen al igual que el método de Wang.

CONCLUSIONES

En este artículo se presentaron tres de los más sobresalientes métodos de Criptografía Visual Extendida (CVE), donde las sombras de todos los participantes son imágenes visualmente reconocibles (VR), además de satisfacer todas las propiedades de CV. A lo largo del artículo se presenta el algoritmo, la construcción de matrices base, la condición de contraste y seguridad. Así mismo se proporciona un ejemplo de cada uno de los tres métodos. Finalmente se realizó una comparación entre los tres métodos desde el punto de vista de ventajas y desventajas, proporcionando al lector algunos criterios que le permitan definir cuál es el método más conveniente a las necesidades del mismo, al igual que también se presenta una tabla comparativa donde se resaltan los resultados que se obtienen en cuanto a expansión y calidad de las sombras e imágenes decodificadas se refiere. De esta comparación se concluye que el método de Ateniese es el método que ofrece la mejor calidad de sombras e imágenes resultantes con una expansión mínima. Mientras que si se desea cifrar más de una imagen secreta, obviamente el mejor método es Droste, ya que es el único método que presenta esa opción y con una expansión similar al de Wang cuando este cifra una sola imagen. Por otro lado Wang puede ser usado si lo que se busca es cifrar una imagen con un umbral (k,n), ya que presenta un PSNR satisfactorio en sus imágenes resultantes.

REFERENCIAS

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).

Ateniese, G., C. Blundo, A. De Santis and D. R. Stinson, *Visual cryptography for general access structures*, Inform. Computation, 129(2), 86-106 (1996).

Chen Q., X. Lv, M. Zhang y Y. Chu, *An Extended Color Visual Cryptography Scheme with Multiple Secrets Hidden*, International Conference on Computational and Information Sciences (ICCIS), 521-524, Chengdu-China, 17 al19 de Diciembre (2010).

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

Kang I., Arce G.R. y Heung-Kyu L., *Color extended visual cryptography using error diffusion*, IEEE International Conference on Acoustics, Speech and Signal Processing, 1473-1476, Taipei-Taiwan, 19 al 24 de Abril (2009)

Kang I., Arce G.R. y Heung-Kyu L., *Color Extended Visual Cryptography Using Error Diffusion*, IEEE Transactions on Image Processing, 20(1), 132-145 (2011).

Klein A. y M. Wessler, *Extended Visual Cryptography Schemes,* Inform. Compt. 205(5), 716-732 (2007).

Liu F. y C. Wu, *Embedded Extended Visual Cryptography Schemes*, IEEE Transactions on Information Forensics and Security, 6(2), 307-322 (2011).

Muñoz J.A., Rodriguez R., *Image encryption based on phase encoding by means of a fringe pattern and computational algorithms*, Revista Mexicana de Física, 52(1), 53–63 (2006)

Nakano M., E. Escamilla y H. Pérez, *Criptografía Visual basada en el esquema de umbral: Una revisión tutorial,* a aparecer en Información Tecnológica, 22(5), (2011).

Naor M. y A. Shamir, *Visual Cryptography,* Advances in Cryptography-Eurocrypt'94, 1-12 (1994).

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

Wang D., F. Yi y X. Li, *On general construction for extended visual cryptography schemes,* Proceedings of Pattern Recognition*,* 42(11), 3071-3082 (2009)

Wang Z., Arce G.R. y Di Crescenzo G., *Halftone Visual Cryptography Via Error Diffusion*, IEEE Transactions on Information Forensics and Security, 4(3), 383-396 (2009).

Wu X. y W. Sun, *A novel bit plane based image sharing scheme using EVCS*, International Conference on Information Networking and Automation , 1, 540-544 , Kunming-China , 18 al 19 de Octubre (2010).

Wu X. y W. Sun, *A novel extended visual cryptography scheme using one shared image*, IEEE International Conference on Information Theory and Information Security (ICITIS), 216-220, Beijing-China, 17 al 19 de Diciembre (2010).

Zhou Z., Arce G.R. y Di Crescenzo G., *Halftone Visual Cryptography*, IEEE Transactions on Image Processing, 15(8), 2441-2453 (2006).