A cheating prevention EVC scheme using watermarking techniques

Esquema ECV con prevención de fraude usando técnicas de marca de agua

Angelina Espejel Trujillo[1], *Mariko Nakano Miyatake*[*1], *Mitsugu Iwamoto*[2], *Hector Perez Meana*[1]

[1]Mechanical and Electrical Engineering School. National Polytechnic Institute of Mexico. Av. Santa Ana 1000 Col. San Francisco Culhuacan, C.P. 04430. Mexico D.F, México.

[2]Department of Information and Communication Engineering. The University of Electro-Communications. Chofugaoka 1-5-1, Chofu City. Tokyo, Japan.

(Recibido el 4 de marzo de 2011. Aceptado el 23 de mayo de 2012)

Abstract

Visual Cryptography (VC), proposed by Naor and Shamir in 1994, is a variation of the conventional secret sharing scheme. In VC, instead of a numerical secret key, a secret image is shared among participants in the form of images called shares. Each participant possesses his own share which cannot reveal the secret image being alone, making it necessary to stack more than one share of a qualified participant in order to reveal the secret image. Thus in VC the stacking of shares is equivalent to the decryption process, where neither extra computations nor previous knowledge are required to reveal the secret image. Until now some important VC schemes, such as the *(k,n)*-VC scheme, the general access structure for VC and the extended VC (EVC), have been proposed. Unfortunately all schemes can be cheated, if one or more participants try to generate their fake shares to force the revealed secret image to be a faked one. In this paper, we propose a cheating prevention VC scheme, in which the shares can be identified and authenticated using the EVC scheme and watermarking techniques. In the proposed VC scheme, the share of each participant can be identified by its meaningful appearance instead of noise-like image used in the conventional VC scheme. For the purpose of authentication of each share two binary watermark images are encrypted using shift operation. Before the secret image is revealed, the validation of the shares must be carried out, extracting two watermark images. If they can be extracted correctly, the revealed secret image is considered as authentic;

[*] Autor de correspondencia: telefax: + 52 + 55 + 562 058, correo electrónico: mnakano@ipn.mx. (M. Nakano)

otherwise it is determined as a faked one. The simulation results show the desirable performance of the proposed EVC scheme.

---------- *Keywords:* Visual cryptography, extended visual cryptography, cheating prevention, watermarking

Resumen

La Criptografía Visual (CV), propuesta por Naor y Shamir en 1994, es una variación del esquema de secreto compartido convencional. En la CV, en lugar de una llave secreta, se comparte una información visual, tal como una imagen, entre los participantes en una forma de imágenes llamadas sombras. Cada participante posee su propia sombra, de la cual no se puede revelar el secreto, sin embargo realizando la superposición de sombras de participantes calificados, el secreto se puede revelar siendo perceptible por el sistema visual humano. En la CV la superposición de sombras es equivalente al proceso de descifrado, por lo tanto no requiere ninguna carga computacional extra ni ningún conocimiento previo para revelar la imagen secreta. Hasta ahora algunos esquemas importantes de CV, tales como el esquema CV-*(k,n)*, las estructuras de acceso general para CV y el esquema extendido CV (ECV), han sido propuestos. Desafortunadamente todos los esquemas se pueden engañar fácilmente, si uno o algunos participantes tratan de generar sombras falsas para que una imagen falsa se revele como la imagen secreta. En este artículo se propone un esquema de CV que previene este engaño, en el cual la sombra de cada participante se identifica y autentica usando el esquema de ECV y técnicas de marca de agua. En el esquema propuesto la sombra de cada participante se puede identificar por su significado, en lugar de ser una imagen de tipo ruido sin significado, que se usa en un esquema convencional de CV. Para la autenticación de cada sombra, dos imágenes binarias de marca de agua son cifradas usando la operación de corrimiento. Antes de revelar la imagen secreta, la validación de las sombras debe llevarse a cabo, extrayendo ambas imágenes de marca de agua. Si las imágenes de marca de agua extraídas son correctas, la imagen secreta revelada se considera como auténtica, en caso contrario esta se determina como falsa. Los resultados obtenidos por simulación computacional muestran el deseable funcionamiento del esquema propuesto.

--------- *Palabras clave:* Criptografía visual, criptografía visual extendido, prevención de fraude, marca de agua

Introduction

Visual Cryptography (VC) scheme introduced by Naor and Shamir [1] is a novel cryptographic method which is also called Visual Secret Sharing scheme, because it can be regarded as a realization of the secret sharing scheme [2], however in this case the secret is a visual message instead of a numerical key. Basically VC has two important features: the first one is its perfect secrecy, and the second one is its decryption method, where neither complex decryption algorithms nor the aid of computers is required [1]. Only human visual system is used to identify the secret from the stacked shares of some qualified participants. Therefore, VC is a very convenient method for protecting secrets when computers or other decryption devices are not available.

Until now, some important VC schemes have been proposed. For instance, after the Naor-Shamir (*k,n*)-threshold VC scheme [1], the general access structures for VC [3] and the extended VC (EVC) schemes were proposed by [4, 5], which contributed considerably to the developments of many VC schemes. Recently the VC has attracted the researcher's attention due to its possible applications, such as client authentication in network banking systems [6] and personal identification systems combining VC and biometric techniques, such as fingerprints and face patterns [7]. However all previously mentioned VC schemes can be cheated by one or more dishonest participants [8, 9], who can modify their shares to force the revealed image to be their faked version. Therefore the development of efficient cheating prevention techniques for VC scheme is an essential issue. Recently some cheating prevention algorithms have been proposed. In some of them an additional information, such as an additional share, is introduced for authentication purpose [8, 9], while in other proposals, watermarking techniques are introduced for this purpose [10]. However, all of these proposals still present some security weakness.

This paper proposes a new EVC scheme to improve the VC scheme with cheating prevention mechanism proposed by Luo et al. [10], in which a watermarking technique is introduced to the basic (*2,2*)-VC scheme in order to authenticate the shares [10]. The proposed scheme, unlike [10], is based on the EVC scheme, in which the share of each participant is a meaningful innocent looking image, instead of the conventional noise-like image. It allows identifying the share of each participant, avoiding also simple cheating. Furthermore in the proposed scheme, a secret image together with two watermark patterns is encrypted into two shares. This is equivalent to encrypt three secret images, where two of them can be used for authentication of the third share. Then it provides more strict cheating prevention than the Luo's scheme [10]. The proposed scheme is evaluated by computer simulations, which show that the proposed scheme satisfies the security and contrast conditions of the EVC scheme, and also the desirable performance as a cheating prevention mechanism.

The rest of the paper is organized as follows. Firstly, three important VC schemes [1, 3-5] are described briefly and their security flaws pointed out in [8, 9] are presented. Also Lou et al.'s scheme is shown as a solution to this cheating problem. Next, the proposed EVC algorithm is described in detail, followed by experimental results. Finally, the conclusions of this paper are provided.

Related works

Visual cryptography schemes

Visual Cryptography (VC) scheme proposed by [1], is a variant of the (*k,n*)-threshold scheme [2], in which more than *k* out of *n* participants can reveal the secret image by stacking their shares, although (*k-1*) participants cannot reveal the secret image. In this scheme, each pixel of the secret image is expanded into *m* sub-pixels composed by black and white pixels, where *m* is called the pixel expansion. These expansions are determined by two basis matrices, which are generated to satisfy the security and contrast conditions. The basis matrices for *n* participants with a pixel expansion *m* are given by

$$C^0 = \begin{bmatrix} c_{11}^0 & c_{12}^0 & \cdots & c_{1m}^0 \\ c_{21}^0 & c_{22}^0 & \cdots & c_{2m}^0 \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1}^0 & c_{n2}^0 & \cdots & c_{nm}^0 \end{bmatrix} \in \{1,0\}^{n\times m}, \quad \mathrm{C}^1 = \begin{bmatrix} c_{11}^1 & c_{12}^1 & \cdots & c_{1m}^1 \\ c_{21}^1 & c_{22}^1 & \cdots & c_{2m}^1 \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1}^1 & c_{n2}^1 & \cdots & c_{nm}^1 \end{bmatrix} \in \{1,0\}^{n\times m} \qquad (1)$$

If a pixel of the secret image is 'white', C^0 is selected otherwise C^1 is selected. To encrypt each pixel of the secret image, the columns of the selected matrix are permuted randomly, and then each row of the selected matrix is used to generate the sub-pixels of each share. Thus each element of the basis matrices c^b_{ij} represents the *j*-th sub-pixel of the *i*-th share, where $b \in \{0,1\}$. The stacking operation used in the VC scheme is a bit OR operation shown by figure 1(a); while figure 1(b-d) shows an example of (*2,3*)-threshold scheme. The grayness of a decrypted image depends on the number of black and white sub-pixels used for encryption of each pixel of the secret image. To control the grayness of stacked the shares of any *k* participants $[i_1, i_2, \cdots, i_k]$, the OR operation of the row vectors corresponding to $[i_1, i_2, \cdots, i_k]$ of the basis matrices must satisfy (2) and (3).

$$Hw\left[OR\left(V^0_{i_1}, V^0_{i_2}, \cdots, V^0_{i_k}\right)\right] < d_v - \alpha m, \qquad (2)$$

$$Hw\left[OR\left(V^1_{i_1}, V^1_{i_2}, \cdots, V^1_{i_k}\right)\right] \geq d_v, \qquad (3)$$

where *Hw* [*X*] is Hamming weight of vector *X*, $V^b_{i_q}$ is *iq*-th row of the basis matrix C^b, with b={0,1}, and $1 \leq d_v \leq m$ is a threshold, *m* is the pixel expansion and *α* represents the relative difference between a white and black in the stacked shares. Therefore *α* is required as large as possible, while the pixel expansion *m* is required as small as possible. Thus (2) and (3) determine the contrast conditions of VC, for example in figure 1, *m*=3 and *α*=1/3 are assigned. Additionally for any subset, $\{i_1, \cdots, i_q\} \subset \{1, \cdots, n\}, q < k \leq n$, must be satisfied the security condition given by

$$Hw\left[OR\left(V^0_{i_1}, \cdots, V^0_{i_q}\right)\right] = Hw\left[OR\left(V^1_{i_1}, \cdots, V^1_{i_q}\right)\right], \quad (4)$$

which means that any subset of *q*<*k* participants cannot reveal the secret image.

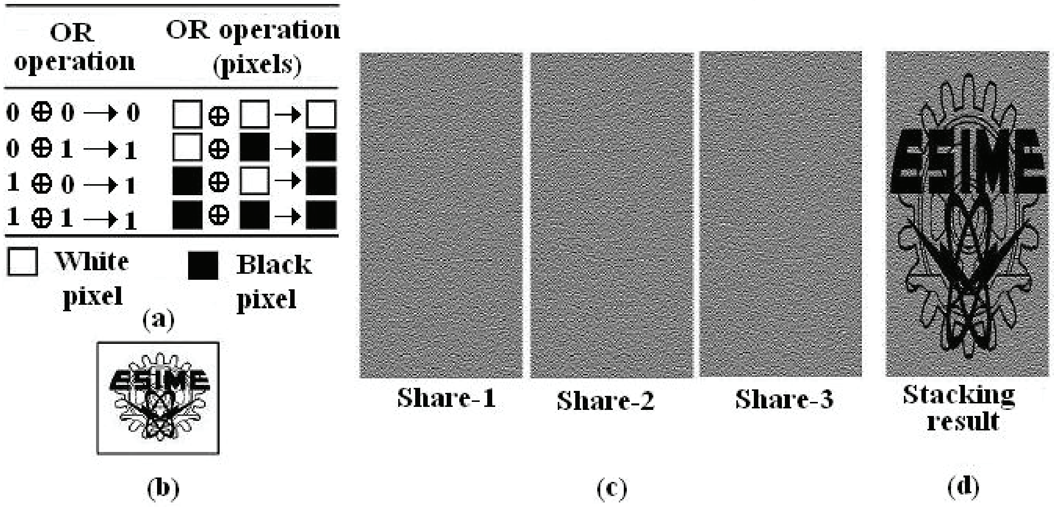

Figure 1 An example of (*2,3*)-VCS. (a) Bit OR operation, (b) Secret image, (c) Shares of three participants and (d) stacking results of two or three shares

The general access structure proposed by [3] is a general version of (*k,n*)-threshold scheme [1], in which a family of participants called qualified sets Γ_q and a family of participants called forbidden sets Γ_f can be assigned. Any subset $\{i_{1,}\ i_{2,}\ \ldots\ i_{q1,}\} \in \Gamma_q$ can reveal the secret image, by stacking their shares, while any subset $\{j_{1,} j_{2,}\ \ldots\ j_{q2,}\} \in \Gamma_f$ cannot reveal the secret, though their shares are stacked. Then the pair (Γ_{q}, Γ_f) is called access structure of a secret image, where $\Gamma_q \cap \Gamma_f = \phi$. Using the access structure, the basis matrices C^0 and C^1, that satisfy the contrast and the security conditions, are constructed.

Extended visual cryptography

The principal idea of the Extended Visual Cryptography (EVC) proposed by [4] is the generation of innocent looking shares, instead of noise-like shares generated by [1] and [3]. The innocent looking shares have two advantages over the noise-like ones: the first one is the facility to distinguish the share of one participant from the shares of others and the second advantage is the cheating prevention. Although it has been proposed a technique for cheating the EVC scheme [9], it is more complicated than the techniques used for cheating the conventional VC scheme. To generate innocent looking shares, the number of sub-pixels must be increased and as a consequence the pixel expansion *m* is also increased. Figure 2 shows an example of (*2,3*)-EVC, where *m*=4 and *α*=1/4. Droste [5] proposed an another realization de EVC scheme called S-extended *n* out of *n* scheme, in which the basis matrices are constructed concatenating basis matrices generated using (*n-i*,*n-i*)-VC scheme (*i*=1..*n*-1) .

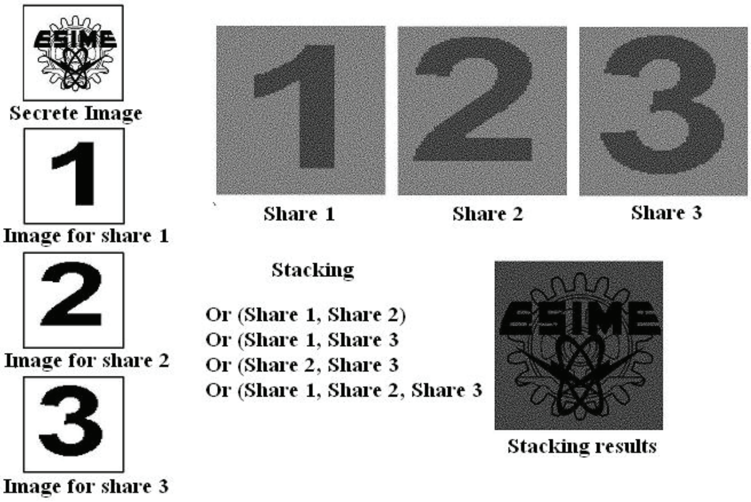

Figure 2 An example of (2,3)-EVC Scheme

Cheating methods for VC

All VC schemes [1, 2-5] are vulnerable against cheating, if one or more dishonest participants try to cheat other honest participants [8, 9]. Authors of [8] pointed out an easy cheating method for the (*2,n*)-threshold VC scheme [1], in which (*n-1*) cheaters guess the secret image and the share of an honest participant, modifying then adequately their shares to force the revealed image to be a desired faked one. In [9], authors pointed out that all VC schemes, included EVC scheme, can be cheated by a dishonest participant; if a cheater can construct fake shares using his own share and a desired fake image. The authors introduced a perfect blackness, which means that after stacking of the shares, all sub-pixels for a black secret pixel have value '1', representing perfect blackness. The perfect blackness can be obtained easily, generating a faked share composed of sub-pixels with complementary values of an authentic share, according to the fake secret image [9]. Figure 3 shows examples of successful cheating for (*2,2*)-VC and (*2,2*)-EVC schemes.

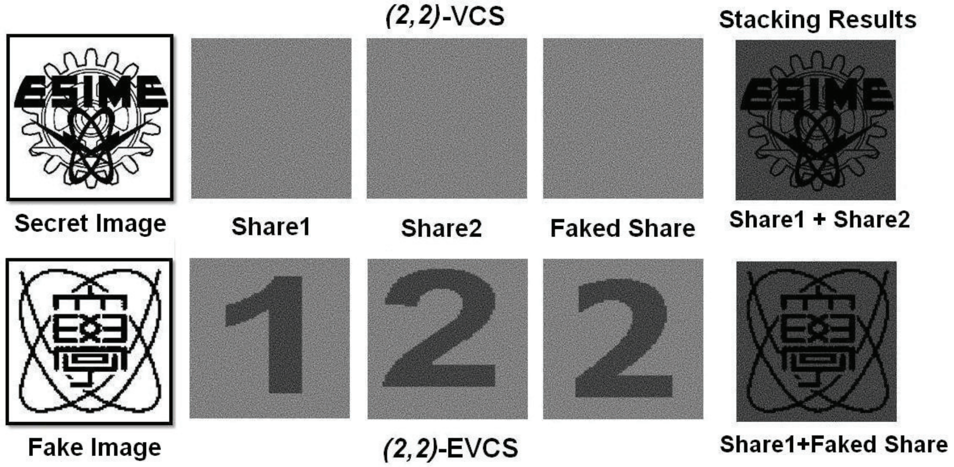

Figure 3 Example of successful cheating in (*2,2*)-VC and (*2,2*)-EVC schemes

In figure 3 the participant who possesses the ‘Share1’ generates the ‘Faked Share’ (fourth column of both rows), according to the given fake secret image, under the (*2,2*)-VC or (*2,2*)-EVC scheme. In both schemes, stacking two authentic shares the authentic secret image can be revealed (upper element of the fifth column), however stacking ‘Share1’ and ‘Faked Share’ the fake image (lower element of the fifth column) is revealed instead of the authentic secret image.

Cheating prevention algorithms

To avoid cheating by dishonest participants, some cheating prevention algorithms have been proposed in the literature [8-10], which are classified basically into: additional share methods [8, 9] and watermarking-based methods [10]. In the additional share method, some additional shares are created together with the participants’ shares for cheating prevention. In [8, 9], an additional share is used to prevent cheaters from estimating easily the share of an honest participant. While in the watermarking-based cheating prevention algorithms, a watermark image is embedded into the shares, which is used for authentication of each share. Lou et al. [10] proposed a technique to encrypt a binary secret image I of $n_1 \times n_2$ pixels and a watermark pattern W of $(n_1/2) \times n_2$ pixels using (*2,2*)-VC scheme. In this method, the images I and W are encrypted into two noise-like shares S1 and S2. Then, the secret image I can be revealed by stacking S1 and S2, while the watermark pattern W can be extracted by stacking the half upper part of S1 and the half lower part of S2; and then it is used for authentication of the two shares S1 and S2. If the extracted W does not correspond to the embedded one, the shares S1 and/or S2 are faked shares. Figure 4 shows the Luo’s VC scheme with cheating prevention [10]. In this scheme only the half upper part of S1 and the half lower part of S2 are used, however unused half lower part of S1 and the half upper part of S2 can be used efficiently to improve cheating prevention capability. It is worth noting that the two shares generated in this scheme are noise-like binary images, which are difficult to distinguish among them.

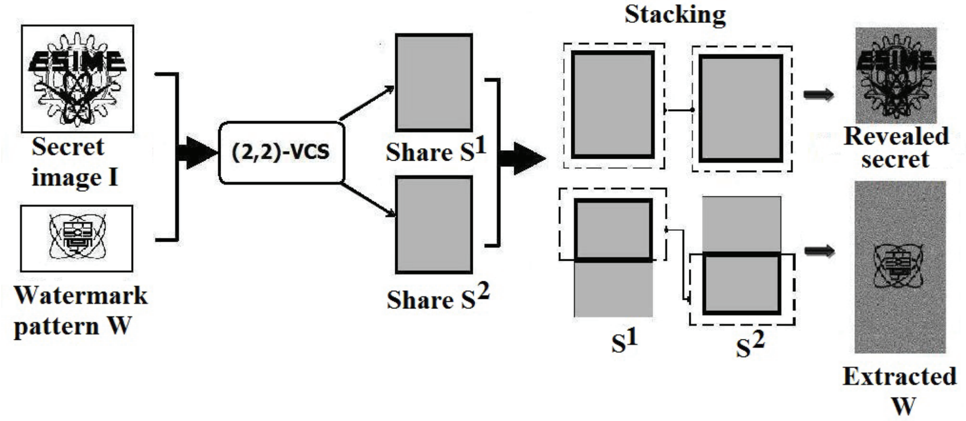

Figure 4 Cheating prevention method proposed by Luo et al. [10]

Proposed EVC scheme with cheating prevention

The main purpose of the proposed EVC scheme is to improve the cheating prevention capability, by encrypting a secret image and two watermark patterns with half size of the secret image, into two shares S1 and S2. The secret image and two watermarks are revealed as follows: 1) the secret image I is revealed by stacking the two shares, S1 and S2. 2) The first watermark pattern W1 is extracted by stacking the upper half part of S1 and the lower half part of S2. 3) The second watermark pattern W2 is extracted by stacking the lower half part of S1 and the upper half part of S2. The second and third stacking are called shifting stacking. In addition, each share itself is a meaningful innocent looking image, which allows visual recognizing among them.

Share image construction process

According to the increase of the data amount for encryption, the construction process of the share images becomes more complex. Let I be a binary secret image, W1 and W2 be two binary watermark patterns, J1 and J2 be innocent looking images and two shares denoted by S1 and S2. As mentioned above, W1 and W2 are decrypted using shifting stacking. Then the upper and lower halves of the secret image, the two innocent looking images and the two share images are denoted by I_U, I_L, J^1_U, J^1_L, J^2_U, J^2_L, S^1_U, S^1_L, S^2_U and S^2_L, respectively, as shown by figure 5.

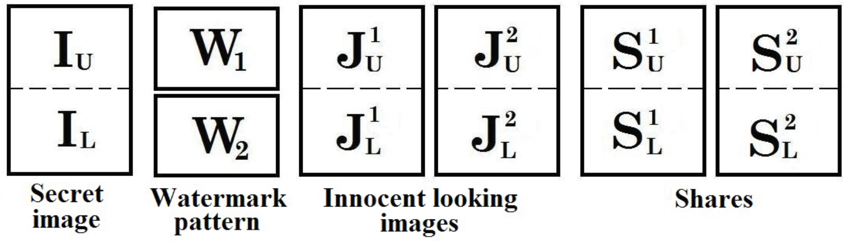

Figure 5 Notation of input and output data of the proposed EVC scheme

Considering that Γ_q is the set of qualified combination of shares that can decrypt a secret image and the two watermark patterns, then Γ_q^i is the access structure of Γ_q if $i \in \{IU, IL, W1, W2\}$. Then the access structure Γ_q^i can be denoted by the qualified combination of shares as

$$\Gamma_q^{\mathrm{I_U}} = \left\{\mathrm{S}_U^1, \mathrm{S}_U^2\right\},\ \Gamma_q^{\mathrm{I_L}} = \left\{\mathrm{S}_L^1, \mathrm{S}_L^2\right\},$$
$$\Gamma_q^{\mathrm{W_1}} = \left\{\mathrm{S}_U^1, \mathrm{S}_L^2\right\},\ \Gamma_q^{\mathrm{W_2}} = \left\{\mathrm{S}_L^1, \mathrm{S}_U^2\right\} \qquad (5)$$

To construct the basis matrices which generate the four shares $\mathrm{S}_U^1, \mathrm{S}_U^2, \mathrm{S}_L^1, \mathrm{S}_L^2$, Droste's multiple-secret EVC scheme [5] is applied in the proposed scheme. Depending on the pixel values of I_U, I_L, $\mathrm{W}_1, \mathrm{W}_2$, J_U^1, J_L^1, J_U^2, J_L^2, the basis matrices B^T can be constructed as the concatenation of matrices shown by table 1, where T is the set of qualified combinations whose stacking result produces a black pixel.

Table 1 Elements for basis matrices B^T for the proposed scheme

S	J_U^1	J_L^1	J_U^2	J_L^2	I_U	I_L	W_1	W_2
	$\{\mathrm{S}_U^1\}$	$\{\mathrm{S}_L^1\}$	$\{\mathrm{S}_U^2\}$	$\{\mathrm{S}_L^1\}$	$\{\mathrm{S}_U^1,\mathrm{S}_U^2\}$	$\{\mathrm{S}_L^1,\mathrm{S}_L^2\}$	$\{\mathrm{S}_U^1,\mathrm{S}_L^2\}$	$\{\mathrm{S}_L^1,\mathrm{S}_U^2\}$
$S \in T$	$\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$	$\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$	$\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$	$\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$	$\begin{bmatrix}0&1\\1&1\\1&0\\1&1\end{bmatrix}$	$\begin{bmatrix}1&1\\0&1\\1&1\\1&0\end{bmatrix}$	$\begin{bmatrix}0&1\\1&1\\1&1\\1&0\end{bmatrix}$	$\begin{bmatrix}1&1\\0&1\\1&0\\1&1\end{bmatrix}$
$S \notin T$	$\begin{bmatrix}0\\1\\1\\1\end{bmatrix}$	$\begin{bmatrix}1\\0\\1\\1\end{bmatrix}$	$\begin{bmatrix}1\\1\\0\\1\end{bmatrix}$	$\begin{bmatrix}1\\1\\1\\0\end{bmatrix}$	$\begin{bmatrix}0&1\\1&1\\0&1\\1&1\end{bmatrix}$	$\begin{bmatrix}1&1\\0&1\\1&1\\0&1\end{bmatrix}$	$\begin{bmatrix}0&1\\1&1\\1&1\\0&1\end{bmatrix}$	$\begin{bmatrix}1&1\\0&1\\0&1\\1&1\end{bmatrix}$

For example the pixel values of four innocent looking images $\mathrm{J}_U^1, \mathrm{J}_L^1, \mathrm{J}_U^2, \mathrm{J}_L^2$ are black, white, black and white, respectively and four stacking results $\{\mathrm{S}_U^1,\mathrm{S}_U^2\}$, $\{\mathrm{S}_L^1,\mathrm{S}_L^2\}$, $\{\mathrm{S}_U^1,\mathrm{S}_L^2\}$, $\{\mathrm{S}_L^1,\mathrm{S}_U^2\}$ produce pixel values of black, black, white and white, which correspond to the pixel values of the secret image and two watermark pattern $\mathrm{I_U}, \mathrm{I_L}, \mathrm{W}_1, \mathrm{W}_2$. A basis matrix B^T with $T = \{\{\mathrm{S}_\mathrm{U}^1\}, \{\mathrm{S}_\mathrm{U}^2\}, \{\mathrm{S}_\mathrm{U}^1, \mathrm{S}_\mathrm{U}^2\}, \{\mathrm{S}_\mathrm{L}^1, \mathrm{S}_\mathrm{L}^2\}\}$ is given by (6).

$$B^T = \begin{bmatrix}1\\1\\1\\1\end{bmatrix} \circ \begin{bmatrix}1\\0\\1\\1\end{bmatrix} \circ \begin{bmatrix}1\\1\\1\\1\end{bmatrix} \circ \begin{bmatrix}1\\1\\1\\0\end{bmatrix} \circ \begin{bmatrix}0&1\\1&1\\1&0\\1&1\end{bmatrix} \circ \begin{bmatrix}1&1\\0&1\\1&1\\1&0\end{bmatrix} \circ \begin{bmatrix}0&1\\1&1\\1&1\\0&1\end{bmatrix} \circ \begin{bmatrix}1&1\\0&1\\0&1\\1&1\end{bmatrix}$$
$$= \begin{bmatrix}1&1&1&1&0&1&1&1&0&1&1&1\\1&0&1&1&1&1&0&1&1&1&0&1\\1&1&1&1&1&0&1&1&1&1&0&1\\1&1&1&0&1&1&1&0&0&1&1&1\end{bmatrix} \qquad (6)$$

According to the pixel values of the innocent looking images; and those of the secret image and the watermark patterns, B^T is constructed. Therefore B^T is a collection of n x m Boolean matrices, where n is the number of shares and m is the pixel expansion. Before the assignment of sub-pixels for each share, the columns of the matrix B^T of a specific T are permuted randomly, and then each row vector of B^T forms the sub-pixels of each share. The basis matrices B^T must satisfy the contrast and security conditions given by [5]:

1) For $z = \{i_1, \ldots\ldots, i_q\} \notin T$, exists dz where $1 \leq dz \leq m$ with α and m constants, such that all matrices B^T satisfy:

$$Hw\left[OR(B^T(z))\right] \leq d_z - \alpha \cdot m \qquad (7)$$

2) For $z = \{i_1, \ldots\ldots, i_q\} \in T$, exists dz where $1 \leq dz \leq m$ with α and m constants, such that all matrices B^T satisfy:

$$Hw\left[OR(B^T(z))\right] \geq d_z \qquad (8)$$

where $B^T(z)$ are $\{i_r | i_r \in z, r = 1.\, q\}$-th row vectors of the matrix B^T.

3) For all $z = \{i_1, \ldots\ldots, i_q\} \in \{1, \ldots n\}$, the restrictions of row z of B^T establish that it must contain the same elements with the same frequencies for all T.

The proposed EVC scheme with cheating prevention is shown in figure 6, where one secret image I and two watermark patterns W1 and W2 are encrypted using innocent looking images J1 and J2 into two shares S1 and S2 .

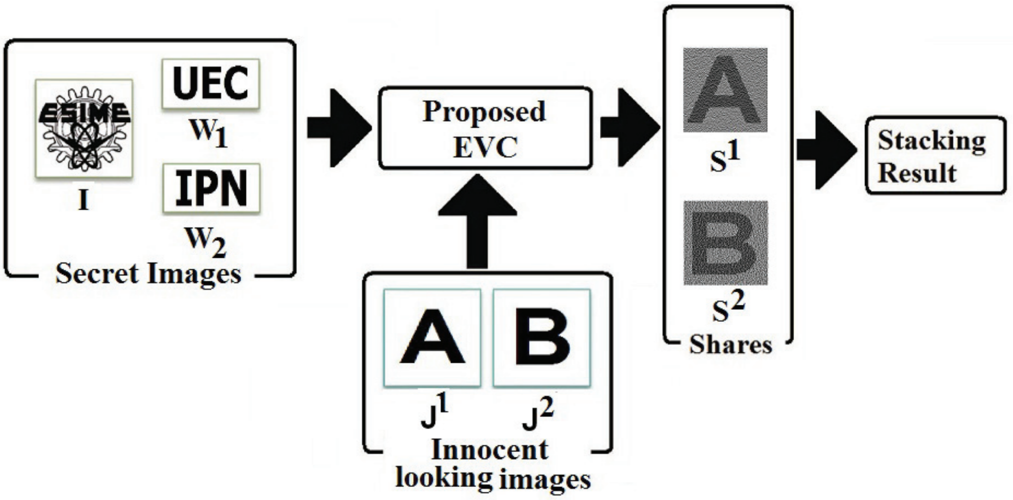

Figure 6 Proposed cheating prevention EVC scheme

Secret image revealing process

Firstly to authenticate the two shares, the watermark patterns W1 and W2 must be extracted correctly, otherwise one or both shares would be considered as faked, and then the revealed secret would also be a fake image. To extract the watermark patterns, the shifting stacking is performed. The first watermark pattern W1 is extracted stacking the upper half of the share S1 and the lower half of share S2, and the W2 is perceived by staking the lower half of S1 and the upper half of S2. These processes are shown in figure 7. The extracted watermark patterns can be recognized visually by dealer or third party, or numerically extracted by

$$\overline{\mathrm{W}}_b(k) = \begin{cases} 1 & \text{if } \; H_w\left(\widetilde{\mathrm{W}}_b\left(sp(k)\right)\right) \geq Th_1 \\ 0 & \text{otherwise} \end{cases} \qquad (9)$$

where $\widetilde{\mathrm{W}}_b,\ b\in\{1,2\}$ is the extracted pattern, H_w is the Hamming weight, *sp(k)* is a vector of *m* sub-pixels for *k*-th pixel of $\mathrm{W}_b,\ b\in\{1,2\}$,, and $Th_1 = d_z$. Here the size of W_b and $\overline{\mathrm{W}}_b$ is the same and the normalized correlation (*NCb*) values for each extracted watermark pattern can be computed by (10).

$$NC_b = \frac{\sum_k \mathrm{W}_b(k)\overline{\mathrm{W}}_b(k)}{\sum_k \mathrm{W}_b(k)^2} \quad ,b\in\{1,2\} \qquad (10)$$

To get a *NCb* value in range [-1,1], before its computation, two binary patterns W_b and $\overline{\mathrm{W}}_b$ must be converted to bipolar binary patterns (0→-1, 1→1). If the *NCb* value is larger than a determined threshold value *Th2*, the extracted watermark patterns can be considered as authentic. The threshold value *Th2* is determined experimentally to be 0.8. Once the two shares are determined as authentic, the secret image can be revealed stacking these shares, as shown in figure 8.

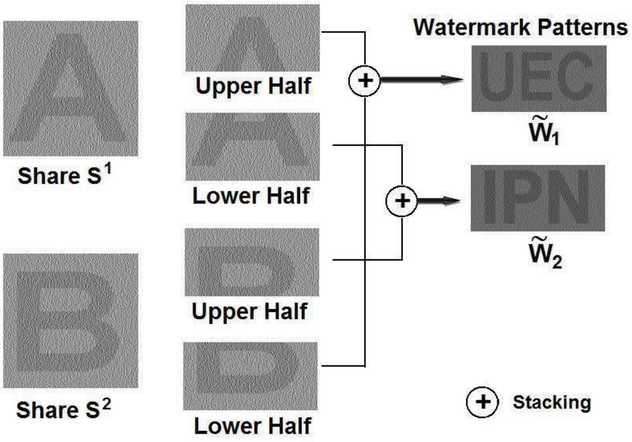

Figure 7 Watermark patterns extraction processes

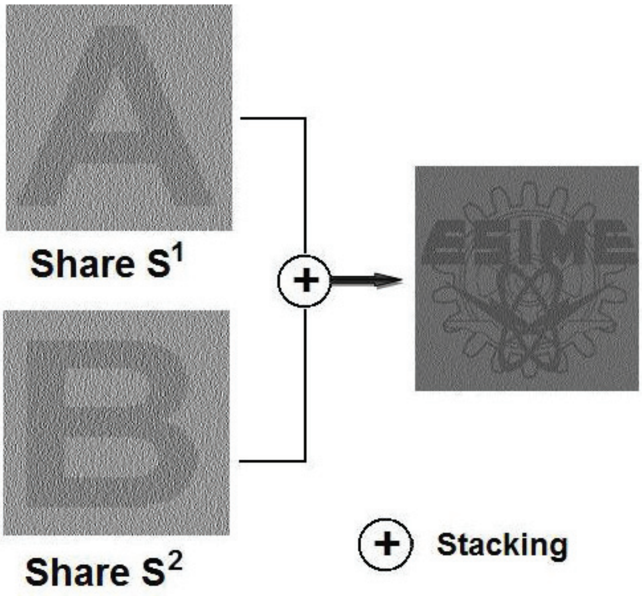

Figure 8 Stacking process to reveal the secret image

Experimental results

Several secret images, watermark patterns and innocent looking images as share images are used, to evaluate the performance of the proposed EVC scheme with cheating prevention mechanism. Figure 9 shows some examples of these images, in which the images of the first row are secret images including a halftone image (d), generated from a grayscale image using the Floyd-Steinberg halftoning method [11], the images of the second row are watermark patterns and the innocent looking images are shown in the last row.

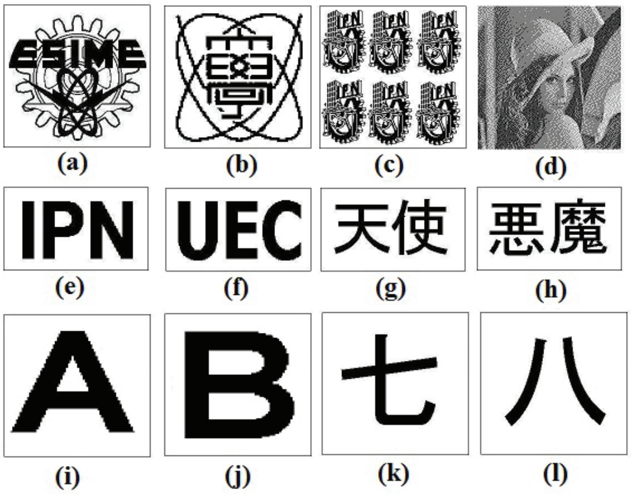

Figure 9 Examples of images used for secret, watermark and shares

Figure 10 shows two innocent looking shares for two participants, the revealed secret image and two extracted watermark patterns, whose original versions are figure 9 (i), (j), (a), (e) and (f), respectively. The pixel expansion *m* is equal to 12 (vertical expansion 3 x horizontal expansion 4) and the relative contrast *α* is equal to 1/12. The normalized correlation values of both watermark patterns computed by (10) are 1, which means that the extracted watermark patterns are exactly the same as their encrypted versions, therefore the two shares are considered as authentic and then the revealed secret image is also authentic.

The cheating technique mentioned by [9] is not so easy to be applied to the proposed scheme, because firstly the share images used in the proposed scheme are innocent looking images instead of noise-like images, secondly the results of shifting stacking must be the encrypted watermark patterns. Figure 11 shows an example of cheating attack using [9], together with the two extracted watermark patterns and the revealed secret image. In this case both watermark patterns cannot be recognized visually, and its normalized correlation value is 0.01 and -0.02, respectively, and as a consequence at least one of these shares is considered as faked one. Therefore also the revealed image can be determined as fake one.

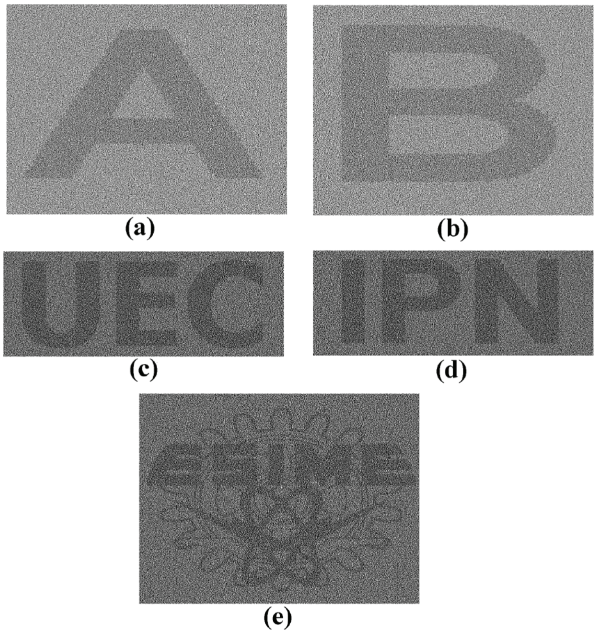

Figure 10 (a), (b) Authentic share images, (c) (d) extracted watermark images, (e) revealed secret image

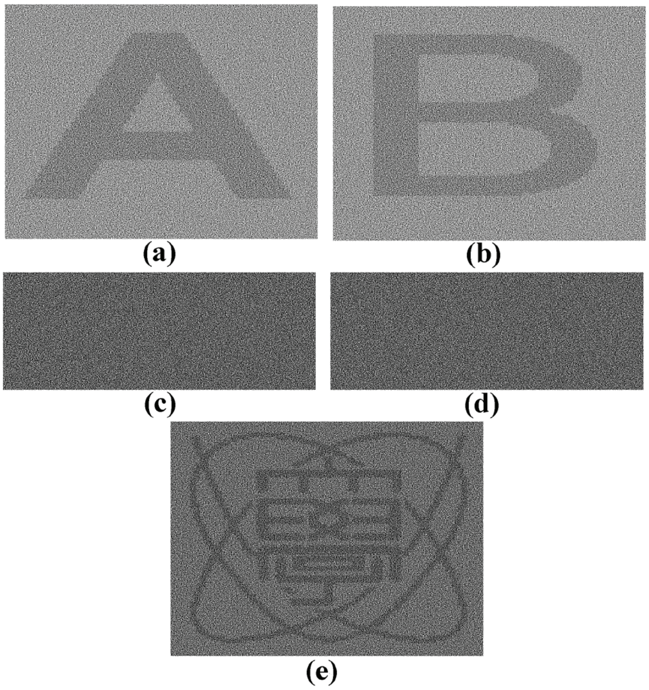

Figure 11 (a) authentic share, (b) faked share created by first participant, (c) and (d) are extracted watermark patters with NC values 0.01 and -0.02, respectively, (e) fake image

Conclusions

In this paper, an extended visual cryptography (EVC) scheme with cheating prevention mechanism is proposed, in which to authenticate two shares, two watermark patterns must be extracted correctly using shifting stacking before the secret image is revealed. To perform this authentication process, two watermark patterns and a secret image are encrypted into two shares. Additionally the proposed EVC generates innocent looking shares instead of noise-like shares. The innocent looking shares provide an advantage over the conventional noise-like shares, because this type of shares can be used to identify the participants.

Compared to the Lou's method [10], our proposal offers a stronger cheating prevention capability because, unlike the Lou's scheme, it uses EVC scheme. The evaluation results show that the proposed scheme prevents cheating by encrypting two watermark patterns instead of one as in the Lou's scheme.

Acknowledgment

We thank to the National Science and Technology Council of Mexico (CONACyT), to the University of Electro-Communications of Japan and to the National Polytechnic Institute of Mexico for the financial support provided during the realization of this research.

References

1. M. Naor, A. Shamir. *Visual cryptography*. Advances in Cryptology-EUROCRYPT' 94. Ed. Springer-Verlag. 1994. pp. 1-12.
2. A. Shamir. "How to Share a Secret". *Communications of the ACM*. Vol. 22. 1979. pp. 612-613.
3. G. Ateniese, C. Blundo, A. De Santis, D. Stinson. "Visual Cryptography for General Access Structures". *Int. J. of Computing*. Vol. 129. 1996. pp. 86-106.
4. G. Ateniese, C. Blundo, A. De Santis, D. Stinson. "Extended Scheme for Visual Cryptography". *Theoretical Computer Science*. Vol. 11. 1997. pp. 179-196.
5. S. Droste. *New Results on Visual Cryptography*. Lecture Notes in Computer Science, Advances in Cryptology. Ed. Springer-Verlag. Berlin, Germany. 1996. pp. 401-415.
6. C. Hegde, S. Manus, P. Shenoy, K. Vengopal, L. M. Patnaki. *Secure Authentication using Image Processing and Visual Cryptography for Banking Applications*. 16th Int. Conf. on Advanced Comp. and Comm. Chennai, India. 2008. pp. 65-72.
7. Y. Rao, Y. Sukonkina, C. Bhagwati, U. Singh. *Fingerprint based authentication application using visual cryptography methods (Improved ID Card)*. 2008 IEEE Region 10 Conf. Hyderabad, India. 2008. pp. 1-5.
8. G. Horng, T. Chen, D-S Tsai. "Cheating in Visual Cryptography". *Designs, Codes and Cryptography.* Vol. 38. 2006. pp. 219-236.
9. C-M Hu, W-G Tzeng. "Cheating Prevention in Visual Cryptography". *IEEE Trans. on Image Processing.* Vol. 16. 2007. pp. 36-43.
10. H. Luo, J. Pan, Z. Lu, B. Liao. *Watermarking based Transparency Authentication in Visual Cryptography.* 3rd Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing. Kaohsiung, Taiwan. 2007. pp. 303-306.
11. M. Mese, P. Vaidyanathan. "Recent Advances in Digital Halftoning and Inverse Halftoning Methods". *IEEE Trans. on Circuits and Systems-I.* Vol. 49. 2002. pp. 790-805.