CHEATING PREVENTION IN HIERARCHICAL VISUAL SECRET SHARING SCHEME USING WEIGHT MATRIX-BASED STEGANOGRAPHY

BISWAPATI JANA, SHYAMAL KUMAR MONDAL, DEBASIS GIRI

Abstract: To prevent cheating in proposed Hierarchical Visual Secret Sharing (HVSS) scheme, a steganographic scheme has been used to detect fake share using weight matrix-based embedding method. In this approach, we have used a secret key (K) and a weight matrix (W) to hide critical information (B) into the share on each level of HVSS. The basic ideas are- (i) to use a different binary operator XOR to protect the secret key (K) from being compromised, and (ii) to use a weight matrix (W) to increase the data hiding rate while maintaining high quality of the host share image in each level of HVSS. The share generator generate weight matrix W_l for the level L_l and each level generate another weight matrix W_i' using the formula $W_i' = \{W_i * 5 \bmod 8+1\}$ where i= 0,1,2,….level number to design and maintain the hierarchical structure of HVSS. The experimental results demonstrate that the proposed scheme is superior to the previous technique in terms of performance and security.

Keywords: Visual Cryptography (VC), Visual Cryptography Scheme (VCS), Size Invariant Visual Cryptography Scheme (SIVCS), Visual Secret Sharing (VSS), Hierarchical Visual Secret Sharing (HVSS).

Introduction: Naor and Shamir [1] invented the Visual Cryptography (VC) in which a secret image (printed text, picture, etc.) is encrypted in a perfectly secure way such that the secret can be decoded directly by the human visual system. VC [7] provides a very powerful technique by which one can be distributed into two or more shares. When the shares are superimposed exactly together, the original secret can be discovered without computer participation. Aside from the obvious applications to information hiding, VC [9-12] can be applied to access control, copyright protection, watermarking, visual authentication, and identification. A Cheater is a dishonest participant who releases a transparency, called Fake Share (FS) during reconstruction of the secret and form a coalition in order to deceive honest participants. Horng et, al. [2] proposed that cheating is possible in (k, n) VC when k is smaller than n. According to Hu and Tzeng [3], there are two types of cheaters – (i) Malicious Participant (MP), where MP ∈ P. (ii) Malicious Outsider (MO), where MO ∉ P. Where P is the participants who contain geneuine share. The cheating method by MP, uses his genuine share as a template to construct a set of fake shares which are indistinguishable from its genuine share. In Hu and Tzeng's cheating activities [3], Malicious Outsider (MO) does not hold any genuine share, the MO only knows the share construction technique. As MO is the outsider, he does not know the right share size for the fake share. For this, Hu and Tzeng [3] gives one solution i.e. to try all possible transparency sizes. In DD-CA (De Prisco and De Santis's Cheating Activity) [4], the cheaters don't set a cheating image, so they don't know the stacking result of all transparencies. Their goal is to generate fake transparencies and make some pixels in the stacked result to be different color. Cheating activities [8] are preventable if the participants suspect that the transparencies are not genuine. In Hu-Tzeng's [3] scheme the share authentication uses a generic transformation to generate new transparencies by adding two sub pixels to every block of every original transparency. This scheme [3] generates a verification transparency for each participant such that the stacking result of the new transparency with the verification transparency will reveal a verification image. De Prisco and De Santis [4] [9] proposed two cheating prevention schemes, 2-out-of-n (PS2) scheme and n-out-of-n scheme (PS1). Du-Shiau Tsai, Tzung-Her Chen, Gwoboa Horng [5] proposed TCH scheme for cheating prevention in VC. In his scheme, shares are generated by Genetic Algorithms (GA). But this is not guaranteed that the quality which is obtained will be same because the GA is a kind of heuristic algorithm. For this, the dealer should control the quality of all decoded secret images before delivering all transparencies i.e. all transparencies should be indistinguishable. In 2013, B. Jana et al [6] proposed a steganographic approach to detect fake transparency and then revealed secret image from original transparency. In their method, a secret image is distributed into n secret transparencies. Then embed secret text within each transparency for authentication. A big advantage in their scheme [6] is fake transparency can be detected by checking the message, embedded within it and there is no need to use any extra verification transparency.

In this paper we proposed Hierarchical Visual Secret Sharing (HVSS) scheme. A cheating prevention scheme has been proposed in HVSS using a steganographic scheme which detect fake share by weight matrix-based embedding method. The experimental results demonstrate that the proposed scheme is superior to the previous technique in terms of performance and security. This paper is organized as follows: Section II provides our proposed method. While Section III shows some experimental results. Finally, Section IV concludes this paper.

Proposed Method: Hierarchical Visual Sceret Sharing (HVSS) encrypts the secret in number of levels. As the number of levels in hierarchical visual cryptography increases, the secrecy of data tends to increase. In a hierarchical structure, a user in a higher class has access to the information items of security classes of lower levels, but not of upper levels. Hierarchical structures are

used in many applications including military, government, educational institute, private corporations, computer network systems etc.

Here a secret image(S) can be distributed into n secret shares, each of these are unique subset of original secret. Now for each share, a unique secret have to choose and level-2 shares would be generated by Ex-ORing a level-1 share with its corresponding unique secret. At the time of stacking the level-2 shares, the corresponding unique secret reveals which was chosen by the parent level-1 share. The participant can cheat other by generating fake share (FS). Cheating is prevented using an authentication based cheating prevention technique, where each participant uses a weight matrix (W) to inseart verification code in to the share. At the time of recovering the original secret, first decode the secret code from the share then EX-OR with another share. The block diagram of proposed work is shown in Figure-1.

This scheme heavily relies on the weight matrix W to represent the embedded data. An m×n matrix W can serve as a weight matrix if each element of {1, 2, . . . , 2r-1} appears at least once in W, i.e. {[W]i,j , i=1...m , j=1...n} = {1, 2, . . . , 2r-1}. As 2r-1 ≤ m.n and there are many choices for W, One can first pick 2r-1 elements in W and assign {1, 2, . . . , 2r-1} to them. The remaining {mn - (2r-1)} elements can be assigned randomly. Let W be a weight matrix and F_i be a block of F. Below we show how to embed r bits of data, say $b_1b_2.....b_r$, into F_i by changing at most two bits in F_i . Our goal is to modify F^i into F_i' to ensure the following invariant:

SUM $((F_i' \oplus K) \times W) = b_1b_2.....b_r \pmod{2r}$ ……(1)

Suppose the size of K and W is 3×3. Here, consider a 3×3 LSB block F_i of the host image F. It has been shown how to embed r=2 bits of data in F_i. Let's assume the following inputs –

$F_i = \begin{bmatrix}1&1&0\\1&0&0\\1&1&0\end{bmatrix}$, $K = \begin{bmatrix}0&1&1\\1&1&0\\0&1&1\end{bmatrix}$, $W = \begin{bmatrix}1&2&3\\1&2&3\\1&2&3\end{bmatrix}$ Perform a bitwise exclusive-OR on F_i and K

$F_i \oplus K = \begin{bmatrix}1&1&0\\1&0&0\\1&1&0\end{bmatrix} \oplus \begin{bmatrix}0&1&1\\1&1&0\\0&1&1\end{bmatrix} = \begin{bmatrix}1&0&1\\0&1&0\\1&0&1\end{bmatrix}$ Next, let $\otimes$ be the pair wise multiplication operator on two equal size integer matrices. $(F_i \oplus K) \otimes W = \begin{bmatrix}1&0&1\\0&1&0\\1&0&1\end{bmatrix} \otimes \begin{bmatrix}1&2&3\\1&2&3\\1&2&3\end{bmatrix}$ $= \begin{bmatrix}1&0&3\\0&2&0\\1&0&3\end{bmatrix}$. Summing all elements in above result, SUM $((F_i \oplus K) \otimes W) = 1+3+2+1+3 = 10$. Now, say b_1b_2 is the embedding data and need to embed into F_i. Suppose that F_i is changed to F_i'. Here b_1b_2 is a binary number, so, this scheme will ensure the following invariant:

SUM $((F_i' \oplus K) \otimes W) = b_1b_2 \pmod 4$ ….(2)

With this invariant, the receiver can derive b_1b_2 by computing SUM $((F_i' \oplus K) \otimes W) \pmod 4$.

Our intention is to change as few bits in F_i as possible for security. Since, SUM $((F_i \oplus K) \otimes W) = 2$, if fortunately $b_1b_2 = 2$, then there is no need to modify F_i. Otherwise some bits has to be modified. Observe that if we complement bit $[F_i]_{j,k}$, then $[F_i \oplus K]_{j,k}$ will be complemented. If $[F_i \oplus K]_{j,k}$ is swapped from 0 to 1, then the modular sum will be increased by $w_{j,k}$; otherwise the sum will be decreased by $w_{j,k}$. For instances, if we swap $[F_i]_{1,1}$, the sum will be decreased by $w_{1,1} = 1$, and if we swap $[F_i]_{1,2}$, the sum will be increased by $w_{1,2} = 2$.

The algorithm for **embedding scheme** are stated below:

Step-1: The LSB of secret image F (size is multiple of m×n) is to be modified to embed a critical information B using a secret key K (size of m×n) and a weight matrix W (size of m×n) and r (no of bits to embed in each block).

Step-2: Partition F into blocks (Fi) of size m×n

Step-3: To get weight matrix, pick 2r - 1 elements in W and assign {1,2, . . . , 2r - 1} to them. The remaining (mn-(2r - 1)) elements assigned randomly.

Step 4: Compute $F_i \oplus K$.

Step 5: Compute SUM $((F_i \oplus K) \otimes W)$.

Step 6: From the matrix $S_i \oplus K$, compute for each w = 1, 2,….. 2r - 1 the following set:

$S_w = \{(j,k) | ([W]_{j,k} = w \text{ or } [F_i \oplus K]_{j,k} = 0) \text{ V } ([W]_{j,k} = 2r - w \text{ or } [F_i \oplus K]_{j,k} = 1)\}$

Intuitively, S_w is the set containing every matrix index (j,k) such that if we complement $[F_i]_{j,k}$, we can increase the sum in **step 5** by w. There are actually two possibilities to achieve this : 1) If $[W]_{j,k} = w$ and $[F_i \oplus K]_{j,k} = 0$, then complementing $[F_i]_{j,k}$ will increase the weight by w, and 2) If $[W]_{j,k} = 2r - w$ and $[F_i \oplus K]_{j,k} = 1$, then complementing $[F_i]_{j,k}$ will decrease the weight by 2r - w , or equivalently increase the sum by w (under mod 2r) .

Step 7: Define a weight difference:

$d = (b_1 , b_2 , ... , b_r) - SUM ((F_i \oplus K) \otimes W) \pmod{2r}$

Step 8: Increase the sum in **step 5** by d. If d=0, then no need to modify F_i, otherwise run the following step to modify S_i to S_i'. $S_w = S_w'$, for any w = w' (mod 2r).

Randomly pick h ∈ {0,1,2, . . . , 2r - 1} such that Shd ≠∅ and S-(h-1)d ≠∅

Randomly pick a (j,k) ∈ Shd and complement the bit $[F_i]_{j,k}$.

Randomly pick a (j,k) ∈ S-(h-1)d and complement the bit $[F_i]_{j,k}$.

Intuitively, to increase the sum by d, one can pick two nonempty sets Shd and S-(h-1)d . Since these sets indicate the locations where one can complement F_i to increase the weight by hd and –(h-1)d, respectively. The overall effect is an increase of the weight by d.

Experimental Result:

The cheating can be prevented by our proposed method using matrix embedding method in HVSS. It has been implemented using MATLAB (2008a Version) to detect a Fake Share (FS) using steganography. The hirarchy is maintain by changing the weight matrix. Malicious Participant (MP) may cheat by creating a FS by taking

another fake image in Figure-2 and giving it to others when asked for the share. The FS is created with the help of the original share (S1) using fake share generation algorithm [6] which is shown in Figure -3. It would be impossible to detect it with a normal look that it is a FS and not the original one.

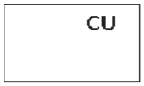

Fig-2: Fake image. and S.

Fig-3: Generation of Fake Share

Fig-4: Stacking of Fake Share

The result of the FS1 with the share S1 is shown in Figure-4 which only shown fake image. Also overlapping the FS1 with all other shares including original share S1 are shown in Figure-5 which only shown fake image. In Figure -6, the result of stacking of fake share with any one share excluding S1 are shown. When stack FS1 with all the shares excluding the S1, one can get both the images in an overlapped manner which will create a confusion, called ***Partial Cheating***. This is known as partial cheating as it creates a kind of confusion between the participants about the original image.

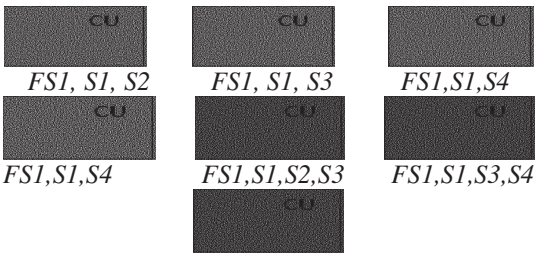

Figure-5: Overlapping the Fake Share with all other shares Including original share (S1) which shown fake image.

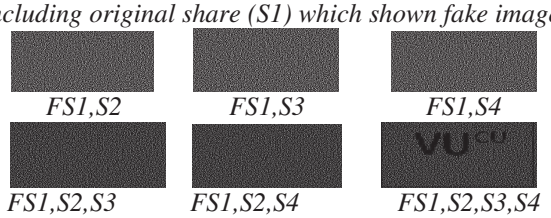

Figure-6: Overlapping the FS1 with all other shares excluding original share (S1) which shown overlapped image for partial cheating.
(Here we using only two share, so no information can be retrieve.)

Distortion is measured by means of two parameters namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The MSE is calculated by using the equation-3,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{i=1}^{N} X(i,j) - Y(i,j) \quad \text{.....(3)}$$

Where M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image X (i, j) represents the pixels in the original image and Y (i, j), represents the pixels of the stego-image. The PSNR is calculated using the equation-4,

PSNR=10

$$\log_{10}\left(\frac{I_{max}^{2}}{MSE}\right) db \quad \text{.....(4)}$$

Where I_{max} is the intensity value of each pixel which is equal to 255 for 8 bit gray scale images. Higher the values of PSNR better the image quality. The analysis in terms of PSNR of original share and stego-share has gives promising result. It has been found that from the same capacity the PSNR of our propose algorithm is better than other one [6] and is near to **79.8.**

To test the security in our proposed method we calculate relative entropy (the differences) between the probability distributions of the original share and the stego share has been calculated by equation (3). Let p_m and q_n be probability measures for clear image M and stego image N, respectively. The relative entropy distance D (N||M) (also known as Kullback-Leibler distance) is defined in equation-5

$$D(N||M) = \sum_{n} q_n(x)\log\frac{q_n(x)}{p_n(x)} \quad \text{.....5}$$

Relative entropy between two probability distribution functions is zero that means the system is perfectly secure. D (N||M) is a nonnegative continuous function and equals to zero iff p_m and q_n coincide. Thus D (N||M) can be naturally viewed as a distance between the measures p_m and q_n.

Conclusion: A new technique for cheating Prevention in Hirarachical Visual Secret Sharing (HVSS) has been proposed, which is required in most of the organizations. The hi-rarchical structure is maintain by changing the weight matrix in each level of HVSS.

Cheating in HVSS is prevented by embedding the secret code with minimum change. We try to improve the embedding efficiency to embed the secret code in the share to presearve the quality of the superimposed image by matrix method. PSNR is **79.8** in our proposed method which is better than existing methods. No verification share is required to prevent the cheating in HVSS. The relative entropy of the probability distribution of the original share and stego share is zero which implies that our system assumed to be perfectly secure. The size of the share will be increase proportionaly with the level of HVSS. One can use size in varient visual secret sharing to overcome the size increse problem in future.

References:

1. M. Naor and A. Shamir, "Visual cryptography," in Proc. Advances in Cryptology, 1994, vol. 950, LNCS, pp. 1–12.
2. G.B. Horng, T.H. Chen, and D.S. Tsai, "Cheating in Visual Cryptography," Designs, Codes and Cryptography, Vol. 38, pp. 219– 236, 2006.
3. C.M. Hu and W. G. Tzeng, "Cheating prevention in visual cryptography," IEEE Transactions on Image Processing, Vol. 16, No. 1, pp. 36–45, 2007.
4. R. De Prisco, A. De Santis,"Cheating immune threshold visual secret sharing,"J.comput,53(2010) 1485-1496.
5. G.B. Horng, T.H. Chen, and D.S. Tsai, "Cheating in Visual Cryptography," Designs, Codes and Cryptography, Vol. 38, pp. 219– 236, 2006.
6. Biswapati Jana, Partha Chowdhuri, Madhumita Mallick and Shyamal Kumar Mondal "Cheating Prevention in Visual Cryptographic using Steganographic Scheme", International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT-2014), technically sponsored by IEEE Delhi Section & IEEE-CIS(Delhi Section), which is scheduled to be held, at Krishna Institute of Engineering & Technology, Ghaziabad, India, February 07-08, 2014.
7. Shamir, "How to share a secret," Comm. ACM 22, pp. 612–613, 1979.
8. Y.C.Chen, G.Horng, D.S. Tsai, "Share authentication based cheating prevention in Naor–Shamir's visual cryptography," J. Comput. 22 (1) (2011) 57–65
9. C. Blundo, P. D'Arco, A. De Santis, D.R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM J. Discrete Math. 16 (2) ,pp. 224–261,2003.
10. Prisco, R.D., De Santis, "A Cheating immune (2,n)-threshold visual secret sharing," SCN 2006, Springer, Berlin, 2006, (LNCS, 4116), pp. 216–228.
11. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptographyfor general access structures," Inf. Comput., vol. 129, no. 2,pp. 86–106, 1996.
12. O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Optics Letters, Vol. 12, No. 6, pp. 377 - 379, 1987.

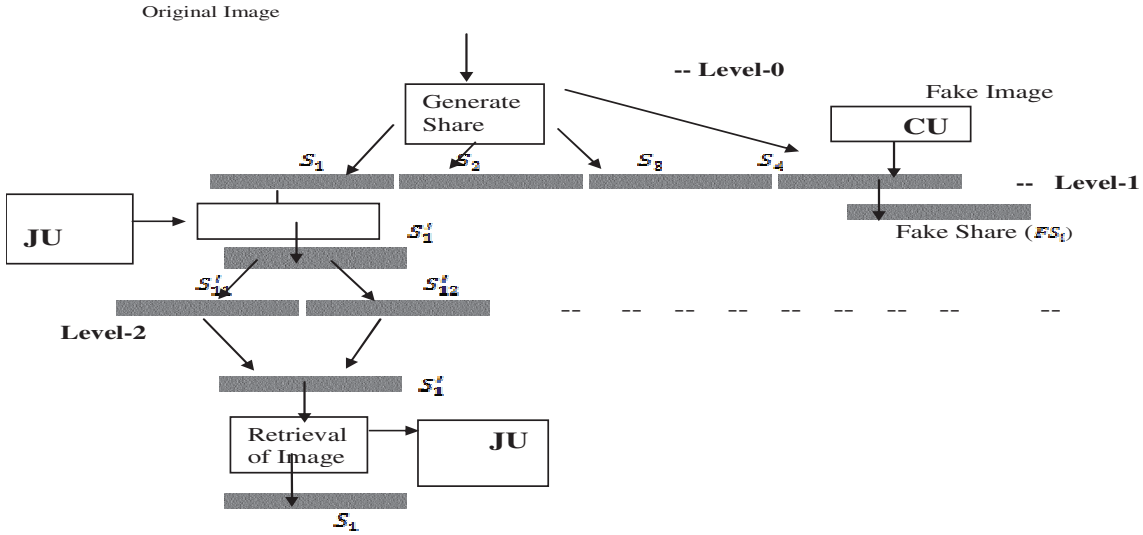

Figure -1: Block diagram of proposed HVSS scheme

***

Biswapati Jana /Assistant Professor/ Department of Computer Science/ Vidyasagar University/ Paschim Medinipur/ biswapati.jana@mail.vidyasagar.ac.in

Shyamal Kumar Mondal/ Associate Professor/ Department of Applied Mathematics/Vidyasagar University/ Paschim Medinipur/shyamal_260180@yahoo.com

Debasis Giri/ Professor/Department of Computer Science Engineering/ Haldia Institute of Technology/ Haldia/debasis_giri@hotmail.com