SURVEY ON CHEATING AND PREVENTION TECHNIQUES IN VISUAL CRYPTOGRAPHY

BISWAPATI JANA

Abstract: Visual Cryptography (VC) Is A Unique Perfect Secure Technique In The Sense That If Y Is An Authorized Subset Of The Participants (P), Then The Participants In Y Can Recover The Secret Image By Stacking Their Transparencies Or Share Together And The Encrypted Message Can Be Decrypted Directly By The Human Visual System. But Cheating Is Also Possible In VC By Some Dishonest Participants Called Cheaters. Cheaters Form A Coalition In Order To Deceive Honest Participants. Many Cheating Prevention Schemes (CPS) Has Been Developed To Prevent Cheating Activities In VC. In This Survey, We Will Summarize Some Cheating Activities And Cheating Prevention Schemes In VC.

Keywords: Visual Cryptography (VC), Visual Secret Sharing (VSS), Cheating, Cheating Prevention Scheme (CPS).

Introduction: Visual Cryptography (VC) is introduced by Naor and Shamir [1] in 1994. In VC, a secret image is encrypted into several shares, which is completely unrecognizable. While the shares are separate, the secret image is completely incoherent. Each share holds different pieces of image and the secret image comes out only by stacking a sufficient number of shares together. They each rely on one another to obtain the secret image. Each participant holds a share. Shares are presented in transparencies. VC eliminates complex mathematical computation to recover the secret. The encrypted message can be decrypted directly by the Human Visual System (HVS).

Access Structure (A) of VC is the family of authorized subsets of participants i.e. $A=\{Q:Q\subset P \text{ and } Q \text{ can recover the secret } K\}$. According to Shamir [2] and Blakley [3], the methods to construct secret sharing schemes realizing the threshold access structure $A=\{Q:Q\subset P \text{ and } |Q| \geq t\}$ such that $1< t \leq n$ where $n=|P|$. This scheme is called t-out-of-n threshold scheme. A (t, n)-Visual

Cryptography Scheme [(t, n)-VCS] is a scheme where the secret image comes out if any t or more shares are stacked together. But no information about the secret image comes out if fewer than t shares are stacked. This scheme proposed by Shamir [2] is based on Lagrange Interpolating Polynomial. In VC some cheating activities may happen by some dishonest participant. They generate the fake share by taking help of their genuine share to cheat other participant. Also some outsider of the system can cheat other participant by generating fake share. Cheating prevention schemes are developed to prevent cheating activities in VC. Here we summarize cheating activities and prevention scheme in VC and analyze existing scheme based on security and complexity.

This paper is organized as follows: Section II provides Basic Visual Secret Sharing and section III defines about Cheating. While in Section IV, some Cheating activities in VC has been described and the cheating activities are compared with each other. Some Cheating Prevention Schemes has been illustrated in Section V. Section VI provides comparison of the schemes. Finally, Section VII concludes this paper.

Basic Visual Secret Sharing (VSS): A variant of k-out-of-n secret sharing scheme is a Visual Secret Sharing (VSS) scheme, where the shares are presented into transparencies. After taking the Secret Image (SI), the transparencies are generated; each white and black pixel of SI is handled separately. It appears as a collection of m black and white sub pixels in each of the n transparencies. Then one pixel of the SI corresponds to n m sub pixels i.e. also denoted by an n × m Boolean matrix, called as Base Matrix (S), such that $S_{ij} = 1$ if and only if the j^{th} sub pixel of the i^{th} share is black and $S_{ij} = 0$ if and only if the j^{th} sub pixel of the i^{th} share is white.

Horizontal transparencies vertical transparencies diagonal transparencies

Figure-1: Six possible patterns of sub-pixel arrangements with 50% gray. Each pattern is represented as [0 0 1 1], [1 1 0 0], [0 1 0 1], [1 0 1 0], [0 1 1 0], [1 0 0 1] from left to right.

The grey level of the stack of k shared blocks is determined by the Hamming Weight H (V) of the "or"ed m-vector V of the corresponding k rows in S. This gray level is interpreted by the visual system of the users

as black if H (V) ≥ d and as white if H (V) ≤ d - α * m for some fixed threshold d and relative difference α. According to Naor and Shamir [1], a solution to the (k, n)-VSS consists of two collections C_0 (for white) and C_1 (for black) of n × m base matrices. The solution is considered valid if the following conditions are hold:

(i) Contrast Conditions:

1. A block of a stacking result represents the colour is white by the HVS when the "or" V of any k of the n rows satisfies that H (V) is less than or equal to d - α * m for any matrix S_0 in C_0.
2. A block of a stacking result represents the colon is black by the HVS when the "or" V of any k of the n rows satisfies that H (V) is more than or equal to d for any matrix S_1 in C_1.

(ii) Security Condition: For any subset $\{i_1, i_2, \ldots, i_q\}$ of {1,2,. . . . ,n} with q < k, the two collections D_0 , D_1 of q × m matrices obtained by restricting each n × m matrix in C_0,C_1 to rows $i_1,i_2, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Cheating in Visual Secret Sharing(VSS): Horng et al.[5] proposed that cheating is possible in (k, n) VC when k is smaller than n. A Cheater is a dishonest participant who releases a transparency called Fake Transparency (FT) during reconstruction of the secret and forms a coalition in order to deceive honest participants.

Consider A, B and C are three participants in a 2-out-of-3 VC. One secret message is transformed into three distinct shares and delivered them. Stacking two of the three shares will reveal secret message. Say, A and B are two dishonest participants who intend to deceive the victim C. The process of cheating in VSS happens in this way are shown in Figure-2.

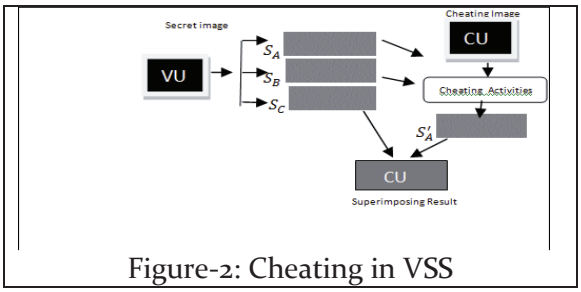

Figure-2: Cheating in VSS

Based on the definitions of Cheating in VSS proposed by De Prisco and

De Santis [4] , one can say that- For any pixel, if the probability of that the cheaters can successfully modify a black/white pixel into a white/black pixel and the stacking result is equal to 1, The cheating is called Deterministic Cheating. Pr [Black↔White] = 1 expresses that a Cheating Prevention Scheme will be insecure against deterministic cheating, where dishonest participants can modify a black/white pixel into a white/black pixel. This definition of cheating by De Prisco and De Santis [4], makes researchers more easily to analyze the security for Cheating Prevention Visual Secret Sharing (CPVSS). Here, We must assume n-1 cheaters (dishonest participants) and one victim in a (k,n) - VSS scheme.

According to Horng et al.[5], Cheating is possible in (k, n) VC where k< n. The key point of cheating is how to predict and rearrange the positions of black and white sub pixels in the victim's and cheater's transparencies. The cheating process is done in the way that the n-1 cheaters collusively use their transparencies to predict victim's transparencies (T). Then based on the prediction, they generate a fake transparency (FT). Finally, after stacking the fake transparency (FT) and victim's transparency (T) the cheating image comes out instead of the original secret image.

Consider a 2-out-of-3 VSS scheme. Here a secret image is transformed into three distinct transparencies T_A , T_B and T_C and delivered to A, B and C. Suppose A and B are two cheaters and C is the victim. During cheating, A and B create a fake transparency T_A'. After stacking T_A' and T_C, the cheating image is visually recovered instead of the original image. The cheaters predict the share of the victim using the collections of 3 × 3 matrices which are used to generate transparencies. Before create the fake transparencies they have to predict the structure of victim's transparencies using the collections for White pixel $C_0 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ and collections for black pixel $C_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

The two rows of above matrices are determined by the two cheaters, so the remaining row is the victim's share. If the pixel block in secret image and the pixel in cheating image is same then the block in fake transparencies T_A' will be same as before. There can be four cases written in Table 1. If the pixel in secret image is white but pixel in cheating image

is black and the block in share T_A & T_B are (1 0 0) & (1 0 0) respectively, then the cheaters predict the block of victim i.e. T_C=(1 0 0) because all rows in C_0 are identical. As the pixel in cheating image is black, they create two new blocks T'_A=(0 1 0) and T'_B=(0 0 1). Now the stacked block of any two of the transparencies T'_A, T'_B and T_C is black. Like this, if the pixel in secret image is black and the pixel in cheating image is white and the transparencies are T_A=(1 0 0) and T_B=(0 1 0) respectively. Then the predicted transparency of victim must be T_C=(0 0 1). As here the pixel in cheating image is white, so the new modified transparencies will be T'_A=(0 0 1) and T'_B=(0 0 1). The stacking result will represent white.

Table-1. The basic concept of cheating in 2-out-of-3 VC.

Cases	Pixel in secret message	Pixel in cheating message	Block in transparency T_A	Block in transparency T_B	Block in transparency T_C	Block in transparency T'_A	Block In Transparency T'_B
1	White	White	(100)	(100)	(100)	(100)	(100)
2	White	Black	(100)	(100)	(100)	(010)	(001)
3	Black	White	(100)	(010)	(001)	(001)	(001)
4	Black	Black	(100)	(010)	(001)	(100)	(010)

Cheating Activities in VC: According to Hu and Tzeng [9], there are two types of cheaters –1) Malicious Participant (MP), where MP $\in$ P.
2) Malicious Outsider (MO), where MO $\notin$ P.
There are two phases when cheating process happens against a VCS. The phases are –
1) Fake share construction phase: In this phase, fake shares are generated.
2) Image reconstruction phase: The genuine share and fake share are stacked together and then the fake image appears.
Cheating Process by an MP(CA-1): As the cheater is an MP, it is possible to use genuine share as a template to construct a set of fake share which are indistinguishable from its genuine share. In CA-1 [9], with the transparency of MP is T_1 ,one can assume that each pixel of T_1 has x black and y white sub pixels. The cheater then chooses a cheating image and prepares r fake transparencies FT_1, FT_2, ... , FT_r , where r = [m/x]-1. For

each white pixel of the fake image, the Cheater copy the corresponding sub pixels of the pixel in T_1 to each fake transparencies (FT). Suppose, the block is (0 1 1 0) in S_1, then the block in the fake transparencies FT will be (0 1 10). For each black pixel of the fake image, the cheater randomly assigns x black and y white sub pixels to each fake transparencies FT such that the pixel in the stacking of these fake transparencies and T_1 is perfect black . Actually a block in a stacking result will be perfect black, if and only if all sub pixels of the block are black. For example, a block in stacking result (1 1 1 1) is perfect black. Suppose, the block is (0 1 0 1) in T_1, as the stacking result is black pixel, so the block in Fake transparencies FT will be (1 0 1 0). In case of some prominent (n,n)- and (k,n)-VCS [1],[6],[7], the number of white and black sub pixels in a pixel are almost equal. Then the cheaters need only r=[m/x]-1 =1 fake share to cheat the victim successfully. As the cheaters set a cheating image and the goal is to generate fake transparency and make victim to accept the cheating image, CA-1 is a meaningful cheating.

Cheating Process by an MO (CA-2): In Hu and Tzeng's CA-2 [9], Malicious Outsider (MO) does not hold any genuine transparency; the MO only knows the transparency construction technique. As MO is the outsider, he does not know the right transparency size for the fake transparency. For this, Hu and Tzeng proposed one solution i.e. to try all possible transparency sizes. At first MO chooses a fake image and encode the fake image into two fake transparencies FT_1 and FT_2 with the optimal (2,2)-VCS. Then enough pairs of fake transparencies $FT_{1,i}$ and $FT_{2,i}$ with various sizes and sub pixel distributions are generated, where $1 \le i \le r$ for some r. Now the stacking of two fake transparency $FT_{1,c}$, $FT_{2,c}$ and T_v (Victim's transparency) shows the fake image for some c, where $1 \le c \le r$. For each white pixel of the fake image, the sub pixels of the block in FT_1 is same as FT_2 .If the block in FT_1 is (0 0 1 1), then the block in FT_2 will be (0 0 1 1). For each black pixel, the corresponding sub pixels of the block in FT_1 and FT_2 is complement to each other. For example, if the block in FT_1 is (1 0 1 0), then the block in FT_2 will be (0 1 0 1) .So, the MO in CA-2 successfully cheats a VCS if the right transparency size is obtained.

Cheating an EVCS by an MP(CA-3): The VCS in which the shares are meaningful or identifiable to every participant, is called Extended VCS (EVCS) [1][9]. Here, different transparencies may have different transparency images. At first glance, cheating is very difficult in EVCS because the cheater have no information about the transparency images

that appear on the genuine transparency and for this, cheater does not known the distributions of black and white pixels of the transparency images. Based on the observation "If the contrast is too small, it is hard to see the image", Hu and Tzeng demonstrated a method of cheating an EVCS. Here, the fake transparencies are used to reduce the contrast between the transparency images and the background. The larger the size and contrast of the image are, the more black sub pixels need to add to the fake transparencies. Consider, P_1 (Cheater with transparency T_1) chooses a fake image and creates T_1' without the transparency image. The transparency image of T_1 is removed by this way that in each black pixel, d black sub pixels is changed into white sub pixels, where d is the difference between the numbers of black sub pixels of a black and white pixel. After this according to **CA-1**[9] using T_1' , r temporary fake transparencies FT_i' , $1 \leq i \leq r$ is created , where r=[m/x]-1. Now d white sub pixels are randomly changed into black sub pixels of each pixel of the transparency image in FT_i' , $1 \leq i \leq r$. FT_i is constructed by randomly adding $\in$ m black sub pixels(changing from white sub pixels) to each pixel in FT_i' . $\in$ is the threshold for contrast that human eyes distinguish the image from the background and it is obtained by experiments. Now the stacking of genuine transparency and fake transparencies reveal the fake image.

Most EVCS have a small contrast. So, cheating is possible by adding a small number of black sub pixels to the pixels of transparency images in the fake transparencies.

De Prisco and De Santis's Cheating Activity (DD-CA) : Based on DD-CA ,Cheating is also possible in (2,n)-VSS and (n,n)-VSS [4]. Cheating in (2,n)-VSS is same as Horng et al.'s [5].In DD-CA, 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. It is a non-meaningful cheating. Here, for a block all the 0s and the 1s in any n-2 transparencies from the n-1 transparencies hold by the n-1 cheaters are swapped. For this, the color of the block will be modified. For example, in a (3,3)-VSS, a cheater holds one transparency. We assume that there is a block (1 1 0 0) in this transparency. The cheater can only replaces (1 1 0 0) with (0 0 1 1). Now the cheater can modify the color of the block from white to black or from black to white.

Comparison With the cheating activities: It has been shown that

Horng et al.'s [4] cheating activity is meaningful cheating, Hu and Tzeng's CA-1 ,CA-2 and CA-3 [9] are also meaningful cheating, but De Prisco and De Santis's [4] cheating activity is non-meaningful cheating.

Cheaters hold genuine transparency in Horng et al.'s CA, Hu and Tzeng's CA-1 ,CA-3 and DD-CA. But in Hu and Tzeng's CA-2, as cheater is malicious outsider, cheater doesn't hold any genuine transparency.

In Horng et al.'s CA, Cheaters have the abilities to know the secret. But, Cheaters have no abilities to know the secret in Hu and Tzeng's CA-1, CA-2, CA-3 and DD-CA.

In Horng et al.'s CA , (k,n)-VSS, k < n is suffer from the cheating activity. In Hu and Tzeng's CA-1 , CA-2 , CA-3 and De Prisco and De Santis's CA , (n, n)-VSS is suffer from the cheating activity. In all types of cheating activities, cheaters know the encoding algorithm.

Table 2: Comparison with Cheating Activities

Cheating Activities	Non-meaningful/ Meaningful	Hold Genuine Trans-parency	Ability to Know Secret	Types of VSS	Ability to know Encoding Algorithm
Horn get al.'s CA	Meaningful	Yes	Yes	(k,n)-VSS,K<n	Yes
CA-1	Meaningful	Yes	No	(n,n)-VSS	Yes
CA-2	Meaningful	No	No	(n,n)-VSS	Yes
CA-3	Non-Meaningful	Yes	No	(n,n)-VSS	Yes

Cheating Prevention Schemes:A Cheating Prevention Scheme (CPS) is under the VSS Scheme where the probability of successful cheating will be negligible. Cheating activities are preventable if the participants suspect that the transparencies are not genuine. There are two classes of CPS. One is share authentication where each participant is provided with an additional transparency to authenticate other transparencies. Share authentication is designed to provide the participants the way such that they can verify the integrity of the transparencies before decoding secret images. Other is blind authentication where some property of the image is used to authenticate the decoded secret image. This authentication is

designed to make it harder for the cheaters such that they can't predict the structure of the transparencies of other participants.

Authentication Based Cheating Prevention Scheme (HCT1): This scheme (HCT1) was proposed by G. Horng, T. Chen and D.S.Tsai [5]. Here, each participant uses an extra transparency to verify the integrity of other transparencies by means of the appearance of verification logo. This scheme consists of transparencies T_i and verification transparency V_i . Transparencies T_i are generated by 2-out-of-n VCS and verification transparencies V_i are generated by 2-out-of-2 VCS. Each participant should provide the dealer a unique verification logo L_i which is used to verify the authenticity of other transparencies. When verification transparency is stacked onto other participant's transparency, then the logo will be appeared on the stacked transparencies. Consider, there are three participants- X, Y and Z. According to the scheme, X posses T_x and V_x , Y posses T_y and V_y and Z posses T_z and V_z . V_x is the verification transparency to verify the correctness of T_y and T_z . Firstly the participants determine their individual logo L_x , L_y and L_z . The logos are sent to the dealer. For authentication, Y stacks V_y onto T_x (T_z) and check. If L_y appears on the stacked transparencies, Y should accept the transparency. If not, then Y should reject the transparency. When authentication succeeds then Y stacks T_y onto T_x (T_z) to decode the secret image. As all logos are confidential, cheaters don't know the secret logo. So, the probability to create a fake transparency to pass the verification is negligible.

2-out-of-(n+l) Cheating Prevention Scheme (HCT2): This scheme is also proposed by G. Horng, T. Chen and D.S.Tsai [5] and referred to as HCT2. This method uses 2-out-of-(n+ l) VC instead of 2-out-of-n, where l ≥ 1. The dealer creates (n+ l) transparencies but only delivers n transparencies to the n participants. When at least two transparencies are stacked, the secret image comes out. Because of generating l extra transparencies, the probability for cheaters to change the black pixels into white pixels without detection is very small. If the victim's transparency is T and B be a block of T which corresponds to a black pixel of a secret image, then the probability that the cheaters can correctly guess the structure of each block B is 1/(1+ l). It is noticeable that the 2-out-of-(n+l) VC prevents black pixels of the secret image from cheating, but leave white pixels of it vulnerable .This weakness is resolved by consisting two complementary parts in secret image. Two binary images are complementary to each other if and only if they have same size and for all

corresponding pixels, one is black and other is white. The reconstructed image is authentic if two parts represent same message. Then the probability that the cheaters can correctly guess the structure of victim's transparency is negligible.

Hu-Tzeng's Cheating Prevention scheme (HT): Hu-Tzeng's [5] scheme is a share authentication based cheating prevention scheme . The main thing of this scheme uses a generic transformation to generate new transparencies by adding two sub pixels to every block of every original transparency. This scheme 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. It performs the following steps with inputs C_0 and C_1 where C_0 and C_1 are base matrices as the Naor–Shamir's (k,n)-VSS scheme.

Let $T_0 = \left(\begin{array}{cc|c} 1 & 0 & \\ \vdots & & S^0 \\ 1 & 0 & \end{array}\right)$ and $T_1 = \left(\begin{array}{cc|c} 1 & 0 & \\ \vdots & & S^1 \\ 1 & 0 & \end{array}\right)$

- T_0 and T_1 are to be used as the base matrices for generating transparencies.
- Each participant P_i chooses a verification image, then generate a verification transparency V_i as follows:

(a) For each white pixel in the verification image, the block of V_i constructed based on (1 0 0 . . .0) (after corresponding permutation as for the transparencies in step 2).

(b) For each black pixel in the verification image, the block of V_i constructed based on (0 1 0 . . .0) (after corresponding permutation as for the transparencies in step 2).

In the verification phase of the secret image, before stacking transparencies, each participants stacks V_i with T_j to get the stacking result to check his own verification image.

De Prisco and De Santis's schemes (PS1 and PS2): In 2009, De Prisco and De Santis proposed two cheating prevention schemes [11] : 2-out-of-n (PS2) scheme and n-out-of-n scheme(PS1). Here the base matrices are C_0 and C_1 .Each of them are obtained by simply adding an extra column with all os to the base matrices of the scheme of Naor and Shamir [1]. PS1(n-out-of-n) scheme requires $2(n+1)^2$ sub pixels for sharing a pixel.

In 2-out-of-n scheme (PS2), the base matrices have $2^n + n + 1$ dimension. Here one pixel will be expanded to $2^n + n + 1$ sub pixels. The base matrices are C_0 and C_1. Each of them is consisted of three parts: C_1, C_2, and C_3. C_1 is

all the possible 2^n binary column vectors of length n, C_2 is a column of all 0, C_3 is the Naor–Shamir's base matrix [1]. The base matrices are denoted by $C_0 = (C_1^0 | C_2^0 | C_3^0)$ and $C_1 = (C_1^1 | C_2^1 | C_3^1)$ For a 2-out-of-3 VSS scheme , C_0 and C_1 will be-

$$C_0 = \left(\begin{array}{cccccccc|ccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array}\right) \qquad C_1 = \left(\begin{array}{cccccccc|ccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

This scheme is a cheating prevention scheme without a complementary image. Therefore, for any black or white pixel, the cheaters cannot infer the actual value of victim's sub pixels.

TCH Cheating Prevention Schem: Du-Shiau Tsai, Tzung-Her Chen, Gwoboa Horng [10] proposed TCH scheme. In this scheme, shares are generated by Genetic Algorithms. TCH adopts multiple secret images with the same visual meaning. Each qualified subset reveals the corresponding reconstructed secret image and the others are left unknown to potential cheaters. If the visually reconstructed secret image is authentic, then any participant accepts the decoded result. In this scheme, the fitness function of the Genetic Algorithm was designed according to a 2-out-of-n VSS. But this is not guaranteed that the quality which is obtained will be same because the Genetic Algorithm 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.

Cheating Prevention in Visual Cryptography using Steganographic Scheme: In 2013, Biswapati Jana, Madhumita Mallick, Partha Chowdhuri and Shyamal Kumar Mondal [13] proposed a steganographic approach to detect fake transparency and then revealed secret image from original transparency.Here a secret image is distributed into n secret transparencies. Then embed secret text within each transparency for authentication. At the time of recovering the receiver first decode the secret text from each transparency and check the secret text is matched or not. If it is not matched, then that particular transparency is fake transparency. So fake image will be shown when stacking. The participant can cheat other. If the shares are genuine, then by stacking the shares one can retrieve the original secret message.

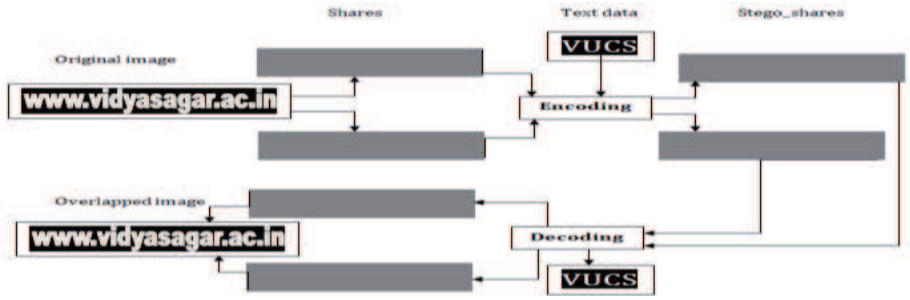

Figure 3: Encoding and Decoding method

In this scheme, it has been shown that stacking the fake transparency with all other transparencies includes the transparency(T_1) by which the fake transparency is created, it will show the Fake image, and when stack the Fake transparency with all other transparencies excluding T_1 then show overlapping image of original image and fake image. This cheating is known as Partial Cheating, which creates the confusion among the users about the original image. A big advantage in this scheme [13] is fake transparency can be detected by checking the message, embedded within it and there is no need to use any extra verification transparency.

Cheating Prevention in Visual Cryptographic Schemes using Message Embedding: A Hardware Based Practical Approach: Biswapati Jana, Debasis Giri, Shyamal Kumar Mondal and Sharmistha Jana implement the scheme[13] by a hardware-based practical approach. There are so many advantages for implementation in hardware are stated below-(i) It is light-weight and portable (ii) the hardware module easily connected with other system through USB (iii) Higher processing speed compared to software implementation (iv) Less cost than software implementation. In the embedding module it takes a transparency as cover-image and inserts the bit of hidden message text into the LSB of cover image. The embedding architecture consists of two D-Flip Flop (FF), a 2:1 multiplexer and an 8-bit shift register. The two D FF take cover-image data and secret text data as inputs. The image read frequency is eight times the text read frequency. So, an 8-bit shift registers which are used to select the LSB of the each pixel value of cover image. The output of the LSB is fed back to the MSB of the shift register. This architecture represents that a logical 1is given at 8th clock pulse. The 2:1 multiplexer selects text data bit and insert into LSB of the cover image depending on the output of shift register. Thus, an architecture of n bit LSB embedding is shown in Figure 4.

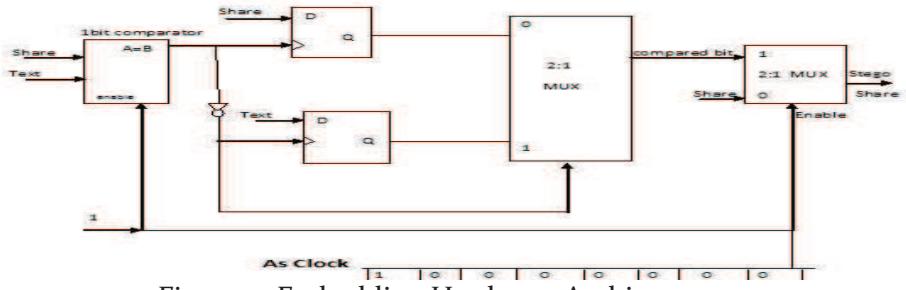

Figure 4: Embedding Hardware Architecture

In the decoding phase, the data encoding in the least significant bit of the stego image data will be decoded and gives the text data back in its original form. This architecture utilizes D-FF, Multiplexers, etc. The D-FF takes the stego-share image data as the input. This D-FF is triggered by a clock only at the time intervals corresponding to LSB , so that the text data is continuously given out at the output of D-FF. Figure 5 shows this concept.

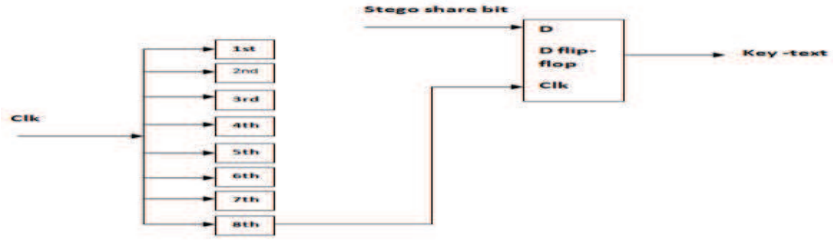

Figure 5: Recovering Hardware Architecture

Comparison: If one compare the cheating prevention schemes, then it can be shown that HCT1 is a share authentication based cheating prevention scheme. Whereas HCT2 is a blind authentication based cheating prevention scheme. Hu-Tzeng's scheme is also share authentication based scheme. De Prisco and De Santis's 2-out-of-n and n-out-of-n scheme is based on blind authentication. Du-Shiau Tsai, Tzung-Her Chen, Gwoboa Horng's TCH scheme is a blind authentication based scheme.

With respect to the total number of sub pixels for sharing a pixel,HCT1 requires $2n^2$ sub pixels because an extra share is used to verify the correctness of the other shares.HCT2 needs $2(n+l)^2$. HT requires

2n(n+2) sub pixels because this scheme needs verification transparencies and each original transparency is enlarged. TCH requires n^2 sub pixels for sharing a pixel. In De Prisco and De Santis's PS2 scheme, one pixel will be expanded to $(2^n + n + 1)$ sub pixels. So it requires $n*(2^n + n + 1)$ sub pixels and PS1 scheme requires $2(n+1)^2$ sub pixels.

The share authentication based cheating prevention approach can be applied to.general access structure but blind authentication based approach is more suitable for threshold access structure. HCT1 scheme uses general access structure. HCT2 and HT scheme uses k-out-of-n access structure. TCH and PS2 scheme uses 2-out-of-n access structure. De Prisco and De Santis's PS1 uses n-out-of-n access structure.

With respect to the method of share generation, HCT1 and HCT2 use the share construction method of traditional VC. HT uses a modified VC by the basis matrices T^0 and T^1 . TCH uses Genetic Algorithm (GA) for share generation. Comparison can be shown with respect to prevention of shares against cheating, the following schemes are designed according to Authentic Condition (AC). HCT1 prevents only these blocks within the corresponding verification logo. HCT2 only prevents blocks that were created for presenting black pixels. PS1, PS2 and HT prevent all blocks of each transparency from cheating.

Table-3: Comparison with Cheating Prevention Schemes

Scheme	Type of Cheating Prevention	Sub pixels	Access Structure	Added Transparency	Share generation	Comp. Complexity	Security
HCT1	Share Authentication	2^2	General	Required	Base matrices	O(n)	Insecure
HCT2	Blind Authentication	$2(+)^2$	k-out-of-n	Required	Base matrices	O(n)	Secure
HT	Share Authentication	2n(n+2)	k-out-of-n	Required	Base matrices	O(n)	Insecure
TCH	Blind Authentication	^{2}	2-out-of-n	Required	Genetic Algorithm	O(n)	Insecure
PS1	Blind Authentication	$2(+1)^2$	2(n)-out-of-n	Required	Base matrices	O(n)	Secure
PS2	Blind Authentication	$n*(2^n + n + 1)$	2-out-of-n	Not required	Base matrices	$O(2^n)$	Insecure

In all types of cheating prevention technique except PS2 , extra

transparency have to be added. With respect to computational complexity, complexity required for HCT1, HCT2, HT, TCH and PS1 is O(n) and for PS2 the complexity will be $O(2^n)$.

In the security point of view, all schemes are designed for preventing a known secret cheating attack. HCT1, HT ,PS2 and TCH are not proved to be secure but it is proved that HCT2 and PS1 are Secure.

Conclusion: In this paper, we summarized the different cheating activities and different cheating prevention scheme in VC. So many cheating prevention scheme are discussed here with respect to share/blind authentication, computational complexity, sub pixels and security. Though the perfect secure solution of cheating prevention is not proposed, which need for security analysis under different types of attacks. Using some advanced steganographic schemes cheating prevention can be solved in future.

References:

1. M. Naor and A. Shamir, "Visual cryptography," in Proc. Advances in Cryptology, 1994, vol. 950, LNCS, pp. 1–12.
2. Shamir, "How to share a secret," Comm. ACM 22 ,pp. 612–613,1979.
3. 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.
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. 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.
7. C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," J. Cryptol., vol. 12, no. 4, pp. 261–289, 1999.
8. Y.C. Chen, G. Horng, and D.S. Tsai, "Comment on Cheating Prevention in Visual Cryptography," IEEE Transactions on Image Processing (Accepted), 2012.
9. 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.
10. Tsai, D.S., Chen, T.H., Horng, G.B, "A cheating prevention scheme for binary visual cryptography with homogeneous secret images," Pattern Recognit., 2007, 40, pp. 2356–2366.
11. Prisco, R.D., De Santis, "A Cheating immune (2,n)-threshold visual secret sharing," SCN 2006, Springer, Berlin, 2006, (LNCS, 4116), pp. 216–228.
12. 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.
13. 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
14. Biswapati Jana, Sharmistha Jana, Shyamal Kumar Mondal and Debasis Giri "CHEATING PREVENTION IN VISUAL CRYPTOGRAPHIC SCHEMES USING MESSAGE EMBEDDING: A HARDWARE BASED PRACTICAL APPROACH", 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.

***

Biswapati Jana/Assistant Professor/ Department of Computer Science/
Vidyasagar University/ Paschim Medinipur/Pin-721102/
West Bengal, India. /biswapati.jana@mail.vidyasagar.ac.in