Results on (2, *n*) Visual Cryptographic Scheme

Kanakkath Praveen and M.Sethumadhavan

Amrita Vishwa Vidyapeetham
Amrita Nagar P.O, Ettimadai,Coimbatore-641 112
praveen.cys@gmail.com, m_sethu@cb.amrita.edu

Abstract. In the literature a lot of studies were carried out on (2, *n*) visual cryptographic scheme (*VCS*) using either XOR or OR operation. A scheme on ideal contrast (2, *n*) *VCS* with reversing using combined OR and NOT operations was reported. In this paper, a construction on an ideal contrast (2, *n*) *VCS* using combined XOR and OR operations with less amount of transparencies than ideal contrast (2, *n*) *VCS* with reversing using OR and NOT operations is proposed. This paper also shows a construction of (2, *n*) *VCS* with pixel expansion one which perfectly reconstruct the white pixels and probabilistically reconstruct the black pixel using XOR operation.

Keywords: Visual Cryptography, Secret sharing, Perfect Reconstruction, Probabilistic scheme.

1 Introduction

Secret sharing scheme is a method of generating shares from a secret, and the generated shares are distributed to a group of participants. The dealer distributes shares to each participant in such a way that, while combining sufficient number of shares (*k* or more) the participants can reconstruct the secret but fewer than *k* participants are not allowed to reconstruct. Such a system is called as (*k*, *n*) threshold scheme. Naor and Adi Shamir in 1994 developed a (*k*, *n*) OR based visual cryptographic scheme (*VCS*) [1] for sharing secret images. The basic parameters for a *VCS* are pixel expansion and contrast. The pixel expansion is a measure of number of sub pixels used for encoding a pixel of secret image while contrast is the difference in grey level between black pixel and white pixel in the reconstructed image. Droste [3] in 1998 proposed a *VCS* with less pixel expansion than Naor's *et al.* scheme. In 2006 Bose et.al [7] proposed an optimal (2, *n*) *VCS*. In 2008 Sreekumar *et al.* [8] proposed a Uniform Secret Sharing Scheme for (2, *n*) *VCS*. In 2010 Liu *et al.* [9] proposed an XOR based (2, *n*) *VCS* with optimal pixel expansion but the contrast is not ideal. A *VCS* for general access structure was introduced by Ateniese *et al.* [2] in 1996. Adhikari *et al.* [4] in 2004 also constructed a *VCS* for general access structure. In 2005 Tylus *et al.* [5] proposed a *VCS* based on XOR operation. The (*k*, *n*) *VCS* and (2, *n*) *VCS* are special cases of general access structure constructions. Cimato *et al.* [10] in 2005 proposed an ideal contrast general access structure *VCS* with reversing using OR and NOT operations. An ideal contrast (2, *n*) *VCS* can be constructed using Cimato *et al.* construction.

J. Lloret Mauri et al. (Eds.): SSCC 2014, CCIS 467, pp. 335–340, 2014.

In this paper, we propose a construction of an ideal contrast (2, *n*) *VCS* using combined XOR and OR operations with optimal amount of transparencies. This scheme is better than the method proposed by Cimato et.al in the amount of transparencies. In 2004 Yang *et al.* [6] constructed a probabilistic non expandable *VCS* with same contrast level of the expandable *VCS* using OR operation. In this paper we show a construction of non expandable (2, *n*) *VCS* which perfectly reconstruct the white pixel and probabilistically reconstruct the black pixel.

Let $P = \{P_1, P_2, P_3,\ldots, P_n\}$ be the set of participants, and 2^P denote the power set of P. Let us denote Γ_{Qual} as qualified set and Γ_{Forb} as forbidden set. Let $\Gamma_{Qual} \in 2^P$ and $\Gamma_{Forb} \in 2^P$ where $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. Any set $A \in \Gamma_{Qual}$ can recover the secret image whereas any set $A \in \Gamma_{Forb}$ cannot leak out any secret information. Let $\Gamma_0 = \{A\in \Gamma_{Qual}: A' \notin \Gamma_{Qual}$ for all $A' \subseteq A, A' \neq A\}$ be the set of minimal qualified subset of P. The pair $\Gamma = (\Gamma_{Qual}, \Gamma_{Forb})$ is called the access structure of (2, *n*) *VCS*. Let S be an $n \times m$ Boolean matrix and $A \subseteq P$, the vector obtained by applying the Boolean XOR operation to the rows of S corresponding to the elements in A is denoted by S_A. Let $w(S_A)$ denotes the Hamming weight of vector S_A. Definition for the basis matrix of (2, *n*) *VCS* using XOR operation is given in [9]. In the next section an existing ideal contrast (2, *n*) *VCS* is discussed.

2 Cimato's Ideal Contrast (2, *n*) *VCS*

Let $P = \{P_1, P_2,\ldots. P_n\}$ be the set of participants. The share generation and decryption phase is given below.

1. Let K be the secret binary image of size $(p \times q)$ .For each participant u, $1 \leq u \leq n$ the share construction is given as.

   $$Sh_{(u,j)}(g,h) = \begin{cases} (u,j)^{\text{th}} \text{ elementof } S^0 & \mathit{if}\ K(g,h)=0 \\ (u,j)^{\text{th}} \text{ elementof } S^1 & \mathit{if}\ K(g,h)=1 \end{cases} ;1 \leq g \leq p,$$

   $1\leq h \leq q$ and $1\leq j \leq m$. Each participant u will have m transparencies with same size of the secret image. S^0 and S^1 are the basis matrices which can be constructed using perfect black pixel reconstruction scheme [2, 11].

2. Let us define a function $f(x) = \begin{cases} 1 & \mathit{if} \quad x == 0 \\ 0 & \mathit{if} \quad x == 1 \end{cases}$.

3. In the decryption phase, the stacking of any 2 of the n shares of the participants is done using the following steps. Apply steps from *a*) to *c*) for all pixels.

   a. Let $\lambda_j(g,h)$ = OR-ing any pairs $(Sh_{(x,j)}, Sh_{(y,j)})$ for all $j = 1,..,m$, $x \neq y$ and x, y are $\in \{1, 2, 3\ldots n\}$.

   b. $\sigma(g,h)$ = OR all $f(\lambda_j(g,h))$ for $j = 1,.., m$.

   c. Find $K = f(\sigma(g,h))$ for $1\leq g \leq p$, $1\leq h \leq q$.

3 Proposed Ideal Contrast (2, *n*) *VCS* using Liu's Construction

Let $P = \{P_1, P_2, P_3, \ldots, P_n\}$ be the set of participants. The share generation and decryption phase is given below

1. From the Construction 1 in [9] generate a matrix M with distinct rows of size $n \times m$, $m = \lceil \log_2 n \rceil$.
2. Two collections of $n \times m$ Boolean matrices S^0 and S^1 is given as $S^1 = \{C(i) : C(i)$ be the $n \times m$ matrix obtained by a cyclic shift on the rows of M over (i) positions$\}$ and all the rows in the matrix S^0 is same and are generated by randomly selecting a single row from M.
3. Let K be a binary secret image of size $(p \times q)$.For each participant u, $1 \le u \le n$ the share construction is given as.

$$Sh_{(u,j)}(g,h) = \begin{cases} (u,j)^{\text{th}} \text{ elementof } S^0 & \text{if } K(g,h)=0 \\ (u,j)^{\text{th}} \text{ elementof } S^1 & \text{if } K(g,h)=1 \end{cases} ; 1 \le g \le p,$$

   $1 \le h \le q$ and $1 \le j \le m$. Each participant u will have m transparencies with same size of the secret image.

4. In the decryption phase, the stacking of any 2 of the n shares of the participants is done using the following steps. Apply steps from a) and b) for all pixels $(p \times q)$.
   a) Let $\lambda_j(g,h)$ = XOR-ing any pairs $(Sh_{(x,\ j)}, Sh_{(y,\ j)})$ shares for all $j=1,\ldots,m$, $x \neq y$ and x, y are $\in \{1,2,3,\ldots n\}$.
   b) $\sigma(g,h)$ = OR-ing all $\lambda_j(g,h)$ for $j=1,\ldots, m$; where $1 \le g \le p$, $1 \le h \le q$, $\sigma(g,h)$ is the reconstructed secret which is same as that of K.

The number of transparencies of the proposed scheme using Liu's construction is $\lceil \log_2 n \rceil$ which is better than $2^{(n-1)}$ (resp. n) transparencies of ideal contrast (2, n) *VCS* using Ateniese *et al.* (resp. Blundo *et al.*) scheme.

3.1 Example

Let $P = \{P_1, P_2, P_3, P_4\}$ be the set of participants. The basis matrices S^0 (resp.S^1) for a (2, 4) *VCS* is constructed as follows. Let $M = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$, then according to the construction the randomly selected row from M is (0, 1). Then $S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$ .Suppose the secret matrix is given as $K = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Two transparencies of each participant are given as follows.

$$P_1 \Rightarrow Sh_{(1,1)} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, Sh_{(1,2)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, P_2 \Rightarrow Sh_{(2,1)} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, Sh_{(2,2)} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$

$$P_3 \Rightarrow Sh_{(3,1)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, Sh_{(3,2)} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, P_4 \Rightarrow Sh_{(4,1)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, Sh_{(4,2)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

In the decryption phase if P_2 and P_3 combines the two transparencies obtained are $\lambda_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\lambda_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, then $\sigma = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, which ideally reconstruct the secret K.

4 Proposed Probabilistic Non Expandable (2, *n*) *VCS*

Let $P = \{P_1, P_2, P_3, \ldots, P_n\}$ be the set of participants. The basis matrices S^0 (resp.S^1) of size $n \times 1$ is given as S^0= {"either" n tuple column vector with all zeros "or" n tuple column vector with all ones} and S^1= {any n tuple column vector with r ones where $r = \left\lfloor \frac{n}{2} \right\rfloor$ or $\left\lceil \frac{n}{2} \right\rceil$ }.The reconstruction is done by XOR-ing any two shares. The patters $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in a matrix S^0 will give a white pixel during reconstruction and the patters $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ in a matrix S^1 will give a black pixel during reconstruction. It is clear that during reconstruction the white pixels will reconstruct perfectly in white region but the reconstruction of black pixel in black region is probabilistic. In order to increase the probability of occurrence of black pixel in black region we need to increase the number of patterns of $\begin{bmatrix}0\\1\end{bmatrix}$ and $\begin{bmatrix}1\\0\end{bmatrix}$ in a matrix S^1.In the paper [9] it is given that if we are selecting a n tuple column vector with r ones the occurrence of the patterns $\begin{bmatrix}0\\1\end{bmatrix}$ and $\begin{bmatrix}1\\0\end{bmatrix}$ reaches its maximum when r = $\left\lfloor \frac{n}{2} \right\rfloor$ or $\left\lceil \frac{n}{2} \right\rceil$.The probability of occurrence of black pixel in the black region is observed as Prob(b/b) = $\frac{\left\lfloor \frac{n}{2} \right\rfloor \times \left\lceil \frac{n}{2} \right\rceil}{\binom{n}{2}}$.The probability of occurrence of black pixel in the white region is observed as Prob(b/w) =0. The relative contrast is given as Prob(b/b) - Prob(b/w).

4.1 Example

Let us define two sets D^0 and D^1 as D^0= $\{\begin{bmatrix}0\\0\\0\\0\end{bmatrix},\begin{bmatrix}1\\1\\1\\1\end{bmatrix}\}$ and D^1= $\{\begin{bmatrix}0\\0\\1\\1\end{bmatrix},\begin{bmatrix}1\\1\\0\\0\end{bmatrix},\begin{bmatrix}0\\1\\1\\0\end{bmatrix},\begin{bmatrix}1\\0\\0\\1\end{bmatrix}\}$, $S^0 \in D^0$ and $S^1 \in D^1$. Let S^0 and S^1 be the second matrix from D^0 and D^1 respectively. The possible pairs of patterns from the matrix S^0 is $\{\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}1\\1\end{bmatrix}\}$ and S^1 is $\{\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}1\\1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix}\}$.The white pixel 0 will be reconstructed perfectly but black pixel 1 will be reconstructed with a probability of 4/6.So the contrast of the scheme is 4/6.

5 Conclusion

Cimato *et al.* proposed an ideal contrast (2, *n*) *VCS* using the basis matrices of Ateniese *et al.* and Blundo *et al.* perfect black construction scheme. In this paper we proposed an ideal contrast (2, *n*) *VCS* using Liu's construction. The number of transparencies of the proposed scheme is better than that of existing construction. The contrast of the probabilistic schemes completely depends up on the basis matrices used, except in case of random grid constructions. The proposed probabilistic non expandable (2, *n*) *VCS* has better contrast than that of existing schemes.

References

1. Naor, M., Shamir, A.: Visual Cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
2. Ateniese, G., Blundo, C., Santis, A.D., Stinson, D.R.: Visual Cryptography for general access structures. Information and Computation 129, 86–106 (1996)
3. Droste, S.: New results on visual cryptography. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 401–415. Springer, Heidelberg (1996)
4. Adhikari, A., Dutta, T.K., Roy, B.: A New Black and White Visual cryptographic scheme for general access structures. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 399–413. Springer, Heidelberg (2004)
5. Tylus, P., Hollman, H.D.L., Lint, J.H.V., Tolhuizen, L.: XOR based visual cryptographic schemes. Design Codes and Cryptography 37(1), 169–186 (2005)
6. Yang, C.N.: New Visual secret sharing scheme using probabilistic method. Pattern Recognition Letters 25(4), 481–494 (2004)
7. Bose, M., Mukerjee, R.: Optimal (2, *n*) Visual Cryptographic scheme. Design Codes and Cryptography 40(3), 255–267 (2006)
8. Sreekumar, A., Babusundar, S.: Uniform secret sharing scheme for (2, *n*) threshold using Visual Cryptography. International Journal of Information Processing 2(4) (2008)
9. Feng, L., Wu, C.K.: Optimal XOR based (2, *n*) Visual Cryptographic scheme. IACR Cryptology eprint Archives (2010)
10. Cimato, S., Santis, A.D., Ferrara, A.L., Masucci, B.: Ideal contrast Visual Cryptographic scheme with reversing. Information Processing Letters 93, 199–206 (2005)
11. Blundo, C., Bonis, A.D., Santis, A.D.: Improved schemes for Visual Cryptography. Design Codes and Cryptography 24, 255–278 (2001)