Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 131 (2018) 336–343

Procedia Computer Science

www.elsevier.com/locate/procedia

8th International Congress of Information and Communication Technology (ICICT-2018)

Constructing visual cryptography scheme by hypergraph decomposition

Teng Guo[a,*], LinNa Zhou[a]

[a]School of Information Science and Technology, University of International Relations, Poshang Cun 12, Haidian District, Beijing 100091, China

Abstract

A threshold visual cryptography scheme, denoted as (*k, n*)-VCS for short, can encrypt a secret image into *n* share images. The physical stacking of any *k* share images can reveal the secret content while any less than *k* share images will leak no information of the secret content. Besides the threshold access structure, general access structure VCSs are studied in the following works. In this paper, we first build a hyper star access structure VCS from a hyper star without center access structure VCS. Then we build a normal form hyper star access structure VCS from a full threshold VCS, and prove that its pixel expansion is optimal. At last, we propose a method of constructing general access structure VCS from its several decomposed normal form hyper star access structure VCSs.

Keywords: Visual Cryptography; Access Structure; Hypergraph Decomposition

1. Introduction

Naor and Shamir proposed the notion of *k* out of *n* visual cryptography scheme in [1], denoted as (*k, n*)-VCS for short, where a secret image is encrypted into *n* share images so that the physical stacking of any *k* share images can decrypt the secret content while any less than *k* share images will leak no information of the secret content. In most cases, VCSs need to encrypt binary images, which only have white and black pixels, denoted as □ and ■ respectively. In a (*2, 2*)-VCS, every white pixel is encrypted into two patterns ((□■, □■) and (■□, ■□) respectively) each with probability one half while every black pixel is encrypted into two patterns ((□■, ■□) and (■□, □■)

* Corresponding author. Tel.: +86-010-62861449; fax: +86-010-62861449.
E-mail address: guoteng.cas@gmail.com

10.1016/j.procs.2018.04.172

respectively) each with probability one half. From any single share pattern, we have □■ and ■□ each with probability one half, regardless of the content of the secret pixel. Hence we will gain no information of the secret content from any single share. If we denote □ by 0 and denote ■ by 1, the pixel stacking model can be characterized by the Boolean OR operation on {0, 1}. Therefore, the decrypted white pixel can be □■ and ■□ each with probability one half while the decrypted black pixel will be ■■ for sure. We can still see the secret content from the decrypted image with *50%* loss of contrast. As we can see, each secret pixel is encrypted into two pixels for each share image, which is defined as the *pixel expansion* and denoted as *m* usually. The pixel expansion of the previous (*2, 2*)-VCS is two.

Ateniese et al. proposed the notion of general access structure VCS in [2]. In this paper, we denote the participant set by $P = \{1, 2, 3, , n\}$, and a general access structure consists of two specifications that are the set of qualified sets $\Gamma_{Qual} \subseteq 2^P$ and the set of forbidden sets $\Gamma_{Forb} \subset 2^P$ respectively. For any set $X \in \Gamma_{Qual}$, the secret content can be decrypted by physically stacking their share images, but any set $Y \in \Gamma_{Forb}$ gains no information of the secret content. From the above definition, we have $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. In *k* out of *n* access structure, it is easy to verify that we have $\Gamma_{Qual} = \{B \subseteq P : |B| \geq k\}$ and $\Gamma_{Forb} = \{B \subseteq P : |B| \leq k-1\}$. There are two lines of work to construct VCSs, where one line uses combinatorial techniques [1,2,3,4], and the other line uses optimization search techniques [5,6,7]. Our constructions will follow the first line of work.

The following contents can be divided into three parts. In Section 2, access structure notations and previous results are introduced. In Section 3, our constructions and relevant theoretical analysis are presented in detail. Section 4 gives a brief summary of our work.

2. Preliminary

2.1. Some backgrounds

In this section, we first give some background knowledge of graph and hypergraph access structures. Then we give the formal definition of VCS.

For any graph $G = (V(G), E(G))$, each vertex corresponds to certain party of *P,* and the basis of the qualified set of Γ is exactly the edge set of *G*, in such a case, Γ is also known as graph access structure. A star $H = (V, E)$ is a graph with a vertice $c \in V$ such that each $e \in E$ contains *c*, known as the center.

A hypergraph *H* is a pair (V, E), where *V* is the vertex set and $E = \{e_1, e_2, \ldots, e_m\} \subseteq 2^V \setminus \emptyset$ is the hyperedge set. In *k*-uniform hypergraph, all the hyperedges are of size *k*. The subhypergraph H_A induced by a subset *A* of *V* is defined by $H_A = (A, \{e_i \cap A : e_i \cap A \neq \emptyset\})$.The partial hypergraph H_J induced by a subset *J* of $\{1, 2, \ldots, m\}$ is defined by $H_J = (V, \{e_i : i \in J\})$. A hyperstar *H=(V,E)* is a hypergraph with a set of vertices $C \subset V$ such that each hyperedge $e \in E$ contains *C* and $e \setminus C \neq \emptyset \in V \setminus C$, where *C* is called the center. Furthermore, if $|e \setminus C| = 1$ holds for each hyperedge $e \in E$, then the hyper star *H=(V,E)* is called a normal form hyperstar. In a normal form hyperstar *H=(V,E)* with center *C*, each hyperedge contains *C* and another vertex in $V \setminus C$. Any access structure Γ can be expressed by certain hypergraph $H = (P, \Gamma_{Qual})$ where each party corresponds to certain vertex and each qualified set corresponds to certain hyperedge.

In [2], general access structure VCS is formally defined as below:

Definition 1: $\Gamma = (Q, F)$ consists of *n* parties. The Boolean matrices (S^0, S^1) of $n \times m$ form, implement a (Γ, m)-VCS if the following requirements are met:

(Contrast): A positive real number α and a set of positive integers $\{t_X | X \in Q\}$ exist so that for any participant set $X \in Q$, we have $w(S_X^0) \leq t_X - \alpha m$ and $w(S_X^1) \geq t_X$.

(Security): For any participant set $Y \in F$, $S^0[Y]$ and $S^1[Y]$ are equivalent under the column permutation.

Remark: α is known as the *relative contrast* while *m* is known as the *pixel expansion*. S_X^0 represents the stacking result of the X rows of S^0, and $w(S_X^0)$ represents the Hamming weight of S_X^0. S_X^1 and $w(S_X^1)$ are defined analogously.

2.2. Previous results

For a star $G_S = (V, E)$ with center $P_C \in V$, all its edges are of the form $P_C \cup v_i$, where $v_i \in V \setminus \{P_C\}$. We can build a G_S-VCS by using a *(2,2)*-VCS [1] as follows, referring to[2].

Construction 1:

Input: A known *(2,2)*-VCS with basis matrices S_0 and S_1.

Output: A star G_S-VCS with center *C*, whose basis matrices are M_0 and M_1.

Step 1. Generate two basis matrices S_0 and S_1 by the *(2,2)*-VCS in[1], where S_0 is used for encrypting a white pixel and S_1 is used for encrypting a black pixel.

Step 2. For party P_C, the *1*-st row of S_0 (resp.S_1) is copied to the *C*-th row of M_0 (resp.M_1). Each remaining row of M_0 (resp.M_1) is filled with the *2*-nd row of S_0 (resp.S_1).

Step 3. Output M_0 and M_1 as the basis matrices for G_S-VCS.

Example 1: For a star $G_S = (\{1,2,3,4,5\}, \{(1,2),(1,3),(1,4),(1,5)\})$ with center $\{1\}$, the following matrices S_0 and S_1 constitute a G_S-VCS.

$$S_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } S_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}$$

Blundo et al. first propose to decompose a given graph access structure into several star access structures, and then combine the basis matrices for the several star access structures to obtain the basis matrices for the given graph access structure[8]. Formally, their construction is stated as follows:

Construction 2:

Input: Several given star G_S^i-VCS with $i = 1, 2, ..., t$, whose basis matrices are S_0^i and S_1^i respectively.

Output: A graph *G*-VCS with $G = G_S^1 \cup G_S^2 \cup \ldots \cup G_S^t$, whose basis matrices are S_0 and S_1.

Step 1. For each party not in $\cup_{e \in G_S^i} e$, add an all zero row for him in S_0^i and S_1^i. The modified basis matrices for star G_S^i on *P* are denoted by $\hat{S}_0^i$ and $\hat{S}_1^i$.

Step 2. Concatenate the *t* modified basis matrices for the star VCSs together, we will get $S_0 = \hat{S}_0^1 \circ \hat{S}_0^2 \circ \cdots \circ \hat{S}_0^t$ and $S_1 = \hat{S}_1^1 \circ \hat{S}_1^2 \circ \cdots \circ \hat{S}_1^t$.

Step 3. Output S_0 and S_1 as the basis matrices for *G*-VCS.

3. Our work

Given a hyperstar *H=(V,E)* with center *C*, define $H \setminus C = (V \setminus C, \{e \setminus C : e \in E\})$. Given a $H \setminus C$-VCS, we can build a *H*-VCS by Constuction 3. S_0 and S_1 represent the two basis matrices of the known $H \setminus C$-VCS with pixel expansion *m*, from which, the two basis matrices M_0 and M_1 of *H*-VCS are constructed. Equation 1 of constructing S_{j+1}^0 and S_{j+1}^1 from S_j^0 and S_j^1 can be applied iteratively.

$$S_{j+1}^0 = \begin{bmatrix} \overbrace{0\ldots0}^{m} & \overbrace{1\ldots1}^{m} \\ S_j^0 & S_j^1 \end{bmatrix}$$
$$S_{j+1}^1 = \begin{bmatrix} \overbrace{0\ldots0}^{m} & \overbrace{1\ldots1}^{m} \\ S_j^1 & S_j^0 \end{bmatrix} \qquad (1)$$

Construction 3:

Input: A given $H \setminus C$-VCS with |*C*|=*t*, whose basis matrices are S_0 and S_1.

Output: A *H*-VCS, whose basis matrices are M_0 and M_1.

Step 1. From *j=0* to *j=t-1*, do

Step 2. Construct S_{j+1}^0 and S_{j+1}^1 from S_j^0 and S_j^1 by using Equation 1, where $S_0^0 = S_0$ and $S_0^1 = S_1$.

Step 3. Output $M_0 = S_t^0$ and $M_1 = S_t^1$.

Theorem 1: The output matrices M_0 and M_1 of Construction 3 constitute a *H*-VCS, where *H=(V,E)* is a hyperstar with center *C*.

Proof: We will use the proof by induction approach. First, we prove the basis part. If |*C*|=*t=1*, then we have:

$$M^0 = \begin{bmatrix} \overbrace{0\dots0}^{m} & \overbrace{1\dots1}^{m} \\ S_0 & S_1 \end{bmatrix}$$

$$M^1 = \begin{bmatrix} \overbrace{0\dots0}^{m} & \overbrace{1\dots1}^{m} \\ S_1 & S_0 \end{bmatrix}$$

Contrast: For any qualified set $A \in H$, we have a qualified set $A' \in H \setminus C$ and $A' \cup C = A$. Since A' only contains rows of $H \setminus C$, we have $M^0[A'] = S_0[A']||S_1[A']$ and $M^1[A'] = S_1[A']||S_0[A']$. Furthermore, $M^0[A] = S_0[A']||\overbrace{1\dots1}^{m}$ and $M^1[A] = S_1[A']||\overbrace{1\dots1}^{m}$. Hence, $w(M^1[A]) - w(M^0[A]) = w(S_1[A']) - w(S_0[A']) > 0$. The contrast condition holds.

Security: For any forbidden set *B*, we have either $C \not\subset B$ or $B \cap (H \setminus C)$ is a forbidden set of $H \setminus C$-VCS. If we have $C \not\subset B$, then $M^0[B] = S_0[B]||S_1[B]$ and $M^1[B] = S_1[B]||S_0[B]$ are equivalent under the column permutation. The security condition holds in this case. If we have that $D = B \cap (H \setminus C)$ is a forbidden set of $H \setminus C$-VCS, $S_0[D]$ and $S_1[D]$ are equivalent under the column permutation, which implies that $M^0[B]$ and $M^1[B]$ are equivalent under the column permutation. The security condition also holds.

Now we come to prove the induction part. Suppose the conclusion holds for |C_j| =*j>0,* we prove that the conclusion holds for |C_{j+1}|=*j+1*.

$$S_{j+1}^0 = \begin{bmatrix} \overbrace{0\dots0}^{m} & \overbrace{1\dots1}^{m} \\ S_j^0 & S_j^1 \end{bmatrix}$$

$$S_{j+1}^1 = \begin{bmatrix} \overbrace{0\dots0}^{m} & \overbrace{1\dots1}^{m} \\ S_j^1 & S_j^0 \end{bmatrix}$$

Contrast: For any qualified set $A \in (H \setminus C) \cup C_{j+1}$, we have a qualified set $A' \in (H \setminus C) \cup C_j$ and $A' \cup \{j+1\} = A$. Since participant $j+1$ corresponds to the new (first) row of S_{j+1}^0 and S_{j+1}^1, we have $S_{j+1}^0[A'] = S_j^0[A']||S_j^1[A']$ and $S_{j+1}^1[A'] = S_j^1[A']||S_j^0[A']$. Furthermore, $S_{j+1}^0[A] = S_j^0[A']||\overbrace{1\dots1}^{m}$ and $S_{j+1}^1[A] = S_j^1[A']||\overbrace{1\dots1}^{m}$. Hence, $w(S_{j+1}^1[A]) - w(S_{j+1}^0[A]) = w(S_j^1[A']) - w(S_j^0[A']) > 0$. The contrast condition holds.

Security: For any forbidden set *B*, we have that either $j+1 \notin B$ holds or $B \cap ((H \setminus C) \cup C_j)$ is a forbidden set of $((H \setminus C) \cup C_j)$-VCS. If we have that $j+1 \notin B$ holds, then $S_{j+1}^0[B] = S_j^0[B]||S_j^1[B]$ and $S_{j+1}^1[B] = S_j^1[B]||S_j^0[B]$ are equivalent under the column permutation. The security condition holds. If we have that $D = B \cap ((H \setminus C) \cup C_j)$ is a forbidden set of $((H \setminus C) \cup C_j)$-VCS, $S_j^0[D]$ and $S_j^1[D]$ are equivalent under the column permutation, which implies that $S_{j+1}^0[B]$ and $S_{j+1}^1[B]$ are equivalent under the column permutation. The security condition also holds.

Remark: Since *(1, 1)*-VCS has basis matrices $S_0^0 = [0]$ and $S_0^1 = [1]$. Let it be the $H \setminus C$-VCS, where *C* is in the center and contains the remaining *n-1* parties. Using Construction 3, we can obtain a *(n, n)*-VCS. Since the pixel expansion of the above built *(n, n)*-VCS is 2^{n-1}, it is optimal according to [1].

Example 2: The following *(3,3)*-VCS is built from the *(2,2)*-VCS, and the *(2,2)*-VCS is built from the *(1,1)*-VCS, and the *(1,1)*-VCS has basis matrices $S_0^0 = [0]$ and $S_0^1 = [1]$.

The (*2,2*)-VCS has basis matrices S_1^0 and S_1^1:

$$S_1^0 = \begin{bmatrix} 0 & 1 \\ S_0^0 & S_0^1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

$$S_1^1 = \begin{bmatrix} 0 & 1 \\ S_0^1 & S_0^0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

The (*3,3*)-VCS has basis matrices S_2^0 and S_2^1:

$$S_2^0 = \begin{bmatrix} 00 & 11 \\ S_1^0 & S_1^1 \end{bmatrix} = \begin{bmatrix} 00 & 11 \\ 01 & 01 \\ 01 & 10 \end{bmatrix}$$

$$S_2^1 = \begin{bmatrix} 00 & 11 \\ S_1^1 & S_1^0 \end{bmatrix} = \begin{bmatrix} 00 & 11 \\ 01 & 01 \\ 10 & 01 \end{bmatrix}$$

For normal form hyperstar *H=(V,E)* with center *C*, all its hyperedges are of the form $C \cup \{v_i\}$, where $v_i \in V \setminus C$. We can build an *H*-VCS by using a $(|C|+1, |C|+1)$-VCS in [1] as follows.

Construction 4:

Input: A given $(|C|+1, |C|+1)$-VCS, whose basis matrices are S_0 and S_1.

Output: A *H*-VCS, whose basis matrices are M_0 and M_1.

Step 1. Generate two basis matrices S_0 and S_1 by the *(|C|+1,|C|+1)*-VCS in [1], where S_0 is used for encrypting a white pixel and S_1 is used for encrypting a black pixel.

Step 2. For each party P_{i_j} $(1 \le j \le |C|)$ in the center *C*, the *j*-th row of S_0 (resp.S_1) is copied to the i_j-th row of M_0 (resp.M_1). Each remaining row of M_0 (resp.M_1) is filled with the *(|C|+1)*-th row of S_0 (resp.S_1).

Step 3. Output M_0 and M_1 as the basis matrices for *H*-VCS.

Theorem 2: The output matrices M_0 and M_1 of Construction 4 constitute a *H*-VCS, where *H=(V,E)* is a normal form hyperstar with center *C*. Besides, the *H*-VCS is optimal w.r.t. pixel expansion.

Proof: Contrast: The stacking of any hyperedge of *H* is equaivalent to the stacking of *|C|+1* different shares generated by the *(|C|+1,|C|+1)*-VCS in [1], from which we know its contrast is $\frac{1}{2^{|C|}}$.

Security: Any forbidden set *F* of *H* cannot contain any hyperedge of *H*, thus the number of non-repeating shares in *F* is strictly less than *|C|+1*.From the security condition of the *(|C|+1,|C|+1)*-VCS in [1], we know that the *H*-VCS is secure.

It is easy to see that the pixel expansion of the above *H*-VCS is $2^{|C|}$. Since the optimal pixel expansion of *(|C|+1,|C|+1)*-VCS is $2^{|C|}$ in [1] and any *H*-VCS implies a *(|C|+1,|C|+1)*-VCS by considering a hyperedge of *H* . Hence the pixel expansion of the constructed *H*-VCS is optimal.

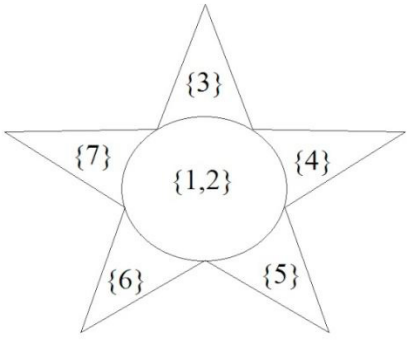

Fig.1. A normal form hyperstar with center$\{1, 2\}$

Example 3: For normal form hyperstar $H = (\{1,2,3,4,5,6,7\}, \{(1,2,3),(1,2,4),(1,2,5),(1,2,6),(1,2,7)\})$ with center$\{1, 2\}$ in Fig. 1, the following matrices S_0 and S_1 constitute a VCS for access structure *H*.

$$S_0 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \text{ and } S_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Similar to the graph decomposition technique in[8], we can first decompose a given access structure into several normal form hyperstars and then combine the basis matrices for the several normal form hyperstars to obtain the basis matrices for the given access structure. Formally, the above idea is stated as follows:

Construction 5:

Input: *t* given normal form hyperstar H_i-VCS, whose basis matrices are S_0^i and S_1^i $(1 < i < t)$.

Output: A Γ-VCS, whose basis matrices are S_0 and S_1.

Step 1. Given an access structure Γ on *P*, suppose its basis is Γ_0, which can be decomposed into several normal form hyperstars $H_1, H_2, \ldots, H_t$, such that $\Gamma_0 = H_1 \cup H_2 \cup \ldots \cup H_t$.

Step 2. Suppose the constructed basis matrices for normal form hyperstars H_i are denoted by S_0^i and S_1^i. For each participant not in $\cup_{e \in H_i} e$, add an all zero row for him. The modified basis matrices for hyperstars H_i on *P* are denoted by $\hat{S}_0^i$ and $\hat{S}_1^i$.

Step 3. Concatenate the *t* modified basis matrices for the normal form hyperstars together, we get $S_0 = \hat{S}_0^1 \circ \hat{S}_0^2 \circ \cdots \circ \hat{S}_0^t$ and $S_1 = \hat{S}_1^1 \circ \hat{S}_1^2 \circ \cdots \circ \hat{S}_1^t$.

Step 4. Output S_0 and S_1 as the basis matrices for Γ-VCS.

Theorem 3: The output matrices S_0 and S_1 of Construction 4 constitute a Γ-VCS.

Proof: Contrast: For each $X \in \Gamma_0$, X belongs to at least one of the normal form hyperstars $H_1, H_2, \ldots, H_t$. Denote the subscript set of H_is that contain X by *A*. In other words, X is contained in H_is, where $i \in A$, and X is not contained in H_is, where $i \notin A$. Suppose the pixel expansion for H_i-VCS is m_i, where $i \in \{1, 2, \ldots, t\}$. The contrast for H_i-VCS w.r.t. X is denoted by α_i^X, where $i \in A$. From the security condition of H_i-VCS, the contrast is 0 w.r.t. *X*, where $i \notin A$. For the constructed Γ-VCS, the contrast w.r.t. X is

$$\alpha^X = \frac{\sum_{i \in A} m_i \alpha_i^X}{\sum_{i \in \{1,2,\ldots,t\}} m_i} > 0.$$

Security: For each $X \notin \Gamma$, X is not contained in any of the H_is. Since each pair of $\hat{S}_0^i$ and $\hat{S}_1^i$ satisfies the security condition with respect to *X*. The pair of their concatenations S_0 and S_1 also satisfies the security condition with respect to *X*.

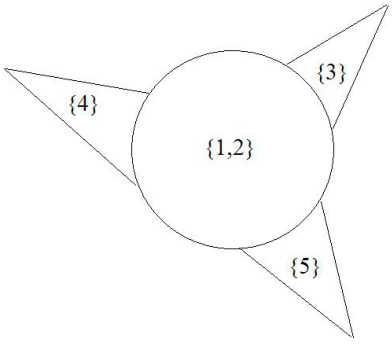

Fig. 2. The first normal form hyperstar with center{1, 2}

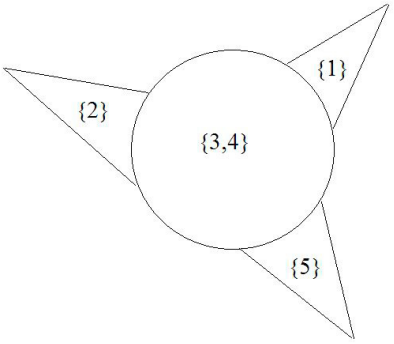

Fig. 3. The second normal form hyperstar with center $\{3, 4\}$

Example 4: $\Gamma_0 = (\{1,2,3,4,5\}, \{(1,2,3),(1,2,4),(1,2,5),(1,3,4),(2,3,4),(3,4,5)\})$ is first decomposed into two hyperstars H_1 and H_2, where $H_1 = (\{1,2,3,4,5\}, \{(1,2,3),(1,2,4),(1,2,5)\})$ with center $\{1,2\}$ and $H_2 = (\{1,2,3,4,5\}, \{(1,3,4),(2,3,4),(3,4,5)\})$ with center $\{3,4\}$, referring to Figs. 2 and 3.

The basis matrices S_0^1 and S_1^1 constitute a H_1-VCS.

$$S_0^1 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \text{ and } S_1^1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

The basis matrices S_0^2 and S_1^2 constitute a H_2-VCS.

$$S_0^2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \text{ and } S_1^2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

The concatenation of S_0^1 and S_0^2 and the concatenation of S_1^1 and S_1^2 constitute the basis matrices S_0 and S_1 of the Γ-VCS respectively.

$$S_0 = S_0^1 \circ S_0^2 = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$$S_1 = S_1^1 \circ S_1^2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

4. Conclusions

In this paper, we propose three constructions, which include building a hyper star access structure VCS from a hyper star without center access structure VCS, building a normal form hyper star access structure VCS, building a general access structure VCS from several small normal form hyper star access structure VCSs, respectively. The theoretical anaysis of those constructions are also presented.

Acknowledgements

This work was supported by Fundamental Research Funds for the Central Universities, University of International Relations, grant No. 3262016T47 and the key project of NFSC grant No. U1536207 and the NFSC project grant No. 61671448 and the National Key R&D Programs of China grant No.2016YFB0801405 and grant No.2016QY08D1600 and grant No.2016YFB0800100.

References

1. Naor M, Shamir A. Visual cryptography In: Santis AD, editors. EUROCRYPT 1994, Springer-Verlag Berlin, Lecture Notes in Computer Science, Vol. 950, 1–12.
2. Ateniese G, Blundo C, Santis AD, Stinson DR. Visual cryptography for general access structures. article. *Information and Computation 1996;* **129**: 86-106.
3. Blundo C, Bonis AD, Santis AD. Improved schemes for visual cryptography. article. *Designs, Codes and Cryptograph y 2001*; **24**:255-278.
4. Blundo C, Cimato S, Santis AD. Visual cryptography schemes with optimal pixel expansion. article. *Theoretical Computer Science 2006*; **369**:169-182.
5. Shen G, Liu F, Fu ZX, Yu B. Perfect contrast xor-based visual cryptography schemes via linear algebra. article. *Designs, Codes and Cryptography 2017;* **85**:15-37.
6. Bose M, Mukerjee R. Optimal (k, n) visual cryptographic schemes for general k. article. *Designs, Codes and Cryptography 2010;* **55**:19-35.
7. Jia XX, Wang DS, Nie DX, Zhang CY. Collaborative visual cryptography schemes. article. *IEEE Transactions on Circuits and Systems for Video Technology 2016*; **99**: 1-14.
8. Blundo C, Santis AD, Stinson DR, Vaccaro U. Graph decomposition and secret sharing schemes. In: Rueppel RA, editors. EUROCRYPT 1992, Springer-Verlag Berlin, Lecture Notes in Computer Science, Vol. 658, 1–24.