Efficient Construction of Visual Cryptographic Scheme for Compartmented Access Structures

Sabyasachi Dutta, Tamal Bhore and Avishek Adhikari
Department of Pure Mathematics, University of Calcutta,
35 Ballygunge Circular Road,
Kolkata 700019, India
E-mail : saby.math@gmail.com,
tamaltml@gmail.com, avishek.adh@gmail.com

Abstract

In this paper, we consider a special type of secret sharing scheme known as Visual Cryptographic Scheme (VCS) in which the secret reconstruction is done visually without any mathematical computation unlike other secret sharing schemes. We put forward an efficient direct construction of a visual cryptographic scheme for compartmented access structure which generalizes the access structure for threshold as well as for threshold with certain essential participants. Up to the best of our knowledge, the scheme is the first proposed scheme for compartmented access structure in the literature of visual cryptography. Finding the closed form of relative contrast of a scheme is, in general, a combinatorially hard problem. We come up with a closed form of both pixel expansion as well as relative contrast. Numerical evidence shows that our scheme performs better in terms of both relative contrast as well as pixel expansion than the cumulative array based construction obtained as a particular case of general access structure.

keywords: Compartmented access structure, monotone access structure, probabilistic VCS, basis matrices.

1 Introduction

A traditional Visual Cryptographic Scheme (VCS) for a set of n participants $\mathcal{P} = \{1, 2, \ldots, n\}$ is a variant of secret sharing, that encodes a secret image SI into n shares which are distributed by the dealer among n participants (also known as parties) in the form of transparencies on which the shares are printed. Such shares have the property that only "qualified" subsets of participants can visually recover the secret image by carefully stacking the transparencies.

The first VCS was proposed by Naor and Shamir [12] where they considered the threshold access structure. Threshold access structure is a particular type of access structure where a fixed positive integer (less than or equal to the number of parties) is considered to be the threshold value. The qualified sets are those subsets of parties which have cardinality greater than or equal to the threshold value and any forbidden sets of parties have cardinality strictly less than the threshold value. This concept has been extended in [1,2,5] to general access structures. In the literature of (k, n)-threshold VCS, where k is the threshold value and n is the number of parties, most of the constructions are realized by constructing so called basis matrices. The mathematical operation that lies beneath the physical implementation of the above mentioned schemes is the Boolean operation

"OR". However the major problems for any OR-based visual cryptographic scheme are the huge share size (pixel expansion) and very poor contrast of the reconstructed image. Several papers have been published to minimize the pixel expansion and to maximize contrast. One may refer to [3,6,14] for a brief survey. All the works mentioned above fall under the deterministic model of visual cryptography. They are deterministic in the sense that when qualified sets of participants stack their shares, the secret image is recovered with probability 1.

In deterministic schemes the pixel expansion becomes so large that it becomes practically impossible to implement a scheme if the number of parties is large. To deal with the pixel expansion, Yang [16] has introduced a new model of visual cryptography in which the reconstruction of the secret image is probabilistic, but the shares have the same size of the secret image, i.e., the schemes have no pixel expansion. A first attempt to provide VCS without pixel expansion was done by Ito et al. in [11]. In both the models, each pixel is reconstructed "OR"ing the corresponding single pixel contained in the shares. Such models are called probabilistic, because they give no absolute guarantee on the correct reconstruction of the original pixel. In some cases, the reconstructed pixel may be wrong. In deterministic schemes when a qualified set of participants stack their shares then it must hold that they reconstruct the secret with probability 1. In probabilistic VCS each pixel can be correctly reconstructed only with a probability given as a parameter of the scheme. This means that the distribution matrices must be carefully selected in order to recover the secret and also make the scheme secure. For a probabilistic scheme, as done in [16], it is possible to define the probabilities of (in)correctly reconstructing a (black)white pixel, given a qualified set of participants. Since in probabilistic models the secret pixel is correctly reconstructed with some probability, the quality of the reconstructed images depends on how big the probability of correctly reconstructing the secret pixels is. The fundamental works in this area of probabilistic visual cryptography are by Yang [16,17] and by Cimato et al. [7]. The idea of Yang's construction is as follows. Given a (k, n)-threshold access structure first we need to construct basis matrices (S^0, S^1) to realize a deterministic (k, n)-VCS. During the share generation phase, the dealer chooses a column randomly from S^0 [resp. S^1] if the secret pixel is white [resp. black] and distributes the ith entry of the chosen column to the ith participant as his share. This idea was forwarded by Cimato et al. [7] where they proposed the idea of choosing more than one column randomly and distribute the ith entry of the chosen column to the ith participant as share. This technique increases the share size and makes the scheme expansible but at the same time it does increase the probability of correct reconstruction of the secret image.

Arumugam et al. [4] introduced $(k, n)^*$-VCS to capture a special type of access structure where one participant is "essential" and he needs the help of any $k-1$ parties other than him, to recover the secret image. Guo et al. [10] generalized $(k, n)^*$-VCS by considering (k, n)-VCS with t essential participants. We denote this by the notation t-$(k, n)^*$-VCS. Note that in the paper [10], the authors denote (k, n)-VCS with t essential participants by (k, n, t)-VCS. However, to keep parity with the original paper [4], we adopt the notation t-$(k, n)^*$-VCS for $0 \leq t \leq k$, $2 \leq k \leq n$ as also adopted in [9]. Thus for $0 \leq t \leq k \leq n$ and $\mathcal{P} = \{1, 2, 3, \ldots, n\}$, the collection of all minimal qualified sets for the t-$(k, n)^*$-VCS is given by $\{S \subseteq \mathcal{P} : 1, 2, \ldots, t \in S \; and \; |S| = k\}$. Here we have assumed, without loss of generality, the first t many parties are the essential parties. The secret image is not retrieved in the absence of any one of the essential parties. The rationale behind considering such an access structure was to address the scenario in a large company where a board of directors are essential any big decision making. In such a case all of the board members are essential. The case when t equals 1 is the work of Arumugam et al. [4] and when t equals 0 is the threshold access structure. Praveen et al. [13] considered the probabilistic model of t-$(k, n)^*$-VCS while Dutta et al. [8] considered XOR based t-$(k, n)^*$-VCS. Among other results they proved that the contrast in the probabilistic model for $(k, n)^*$-VCS is

equal to the contrast of the same in deterministic model [4].

1.1 Compartmented Access Structure and Related Notations

In this paper we consider a more general access structure than $(k,n)^*$ access structure, known as compartmented access structure. Such an access structure was first considered by Simmons [15] in the context of secret sharing schemes. In a compartmented access structure on the set of parties $\mathcal{P} = \{1, 2, \ldots, n\}$, there are different compartments, say $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_u$ having the property that $\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$ for all $i \neq j$ with $|\mathcal{C}_i| = n_i$ and positive integers $k, t_1, t_2, \ldots, t_u$ such that $k = t_1 + t_2 + \cdots + t_u$ and $n = n_1 + n_2 + \cdots + n_u$. The minimal qualified sets for this access structure are those subsets of $\mathcal{P}$ that contain t_1 many parties from $\mathcal{C}_1$, t_2 many parties from $\mathcal{C}_2$, ... , t_u many parties from $\mathcal{C}_u$ so that the subsets contain exactly k many parties. We notice that if there are two compartments $\mathcal{C}_1, \mathcal{C}_2$ with $\mathcal{C}_1 = \{1, 2, \ldots, t\}$ and $\mathcal{C}_2 = \{t+1, t+2, \ldots, n\}$ and $t_1 = t$, $t_2 = k - t$ then we have the access structure of a t-$(k,n)^*$. Thus compartmented access structure is a generalization of the t-$(k,n)^*$ access structure. To maintain the parity of notations we denote a VCS for a compartmented access structure by $\vec{t}$-$(k,\vec{n})^*$-VCS, where the symbols $\vec{t}$ and $\vec{n}$ depict the vectors $(t_1, t_2, \ldots, t_u)$ and $(n_1, n_2, \ldots, n_u)$ respectively such that $|\mathcal{C}_i| = n_i$ for all $i = 1, \ldots, u$, $t_1 + t_2 + \cdots + t_u = k$ and $n_1 + n_2 + \cdots + n_u = n$.

1.2 Our Contribution

We first give a direct efficient construction of basis matrices that realizes the visual cryptographic scheme on the compartmented access structure. Our construction of basis matrices is in a recursive manner. Up to the best of our knowledge, the scheme is the first proposed scheme for compartmented access structure in the literature of visual cryptography. We come up with a closed form of both pixel expansion as well as relative contrast. Numerical evidence shows that our scheme performs better in terms of both relative contrast as well as pixel expansion than the cumulative array based construction obtained as a particular case of general access structure.

2 The Model and Preliminaries

We follow the standard notations and symbols through out. For the sake of completeness we discuss some of the basic notations and tools needed for this paper. Let $\mathcal{P} = \{1, 2, 3, \ldots, n\}$ denote a set of participants. Let the compartments be $\mathcal{C}_1 = \{1, 2, \ldots, n_1\}$, $\mathcal{C}_2 = \{n_1+1, n_1+2, \ldots, n_1+n_2\}$, ..., $\mathcal{C}_u = \{n_1 + \cdots + n_{u-1} + 1, \ldots, n_1 + \cdots + n_{u-1} + n_u\}$ so that $n_1 + \cdots + n_{u-1} + n_u = n$.

Let $2^{\mathcal{P}}$ denote the set of all subsets of $\mathcal{P}$. Let $\mathcal{Q} \subset 2^{\mathcal{P}}$ and $\mathcal{F} \subset 2^{\mathcal{P}}$, where $\mathcal{Q} \cap \mathcal{F} = \emptyset$, respectively denote the set of all qualified sets and the set of all forbidden sets. The pair $(\mathcal{Q}, \mathcal{F})$ constitutes an access structure on $\mathcal{P}$. We denote the collection of all minimal qualified sets of participants by $\mathcal{Q}_{min}$ such that $Q \in \mathcal{Q}_{min}$ means Q contains exactly t_1 many parties from $\mathcal{C}_1$, t_2 many parties from $\mathcal{C}_2$, ... , t_u many parties from $\mathcal{C}_u$ so that total number of parties in Q is k. The collection of all maximal forbidden sets is denoted by $\mathcal{F}_{max}$ and is defined by $\mathcal{F}_{max} = \{F \in \mathcal{F} : \ for\ all\ i \notin F,\ F \cup \{i\} \in \mathcal{Q}\}$. The access structure considered here is monotone i.e., any subset of parties that contains a minimal qualified set is a qualified set and any subset of a forbidden set is forbidden.

Example 2.1 *If* $\mathcal{P} = \{1, 2, 3, 4, 5, 6, 7\}$, $\mathcal{C}_1 = \{1, 2\}$, $t_1 = 1$ *and* $\mathcal{C}_2 = \{3, 4, 5\}$, $t_2 = 2$ *and* $\mathcal{C}_3 = \{6, 7\}$, $t_3 = 2$, *then* $\mathcal{Q}_{min}$ *consists of the following minimal qualified subsets of participants* $B_1 = \{1, 3, 4, 6, 7\}$, $B_2 = \{1, 3, 5, 6, 7\}$, $B_3 = \{1, 4, 5, 6, 7\}$, $B_4 = \{2, 3, 4, 6, 7\}$,

$B_5 = \{2, 3, 5, 6, 7\}$, $B_6 = \{2, 4, 5, 6, 7\}$. *Note that both* $\{1, 3, 6\}$ *and* $\{1, 2, 3, 4, 5\}$ *are some of the members of* $\mathcal{F}$, *while* $\{1, 2, 3, 4, 5, 6\}$ *is a member of* $\mathcal{F}_{max}$.

Notations: Let S be an $n \times m$ Boolean matrix and let $X \subseteq \mathcal{P}$. By $S[X]$ we denote the matrix obtained by restricting the rows of S to the indices belonging to X. Further, for any $X \subset \mathcal{P}$ the vector obtained by applying the boolean OR operation "$\bigvee$", to the rows of $S[X]$ is denoted by S_X. The Hamming weight of the row vector which represents the number of ones in the vector S_X is denoted by $w(S_X)$.
Remark: In this paper, we shall be interested in monotone access structures only. As a result, in terms of defining our schemes, it is sufficient for us to restrict ourselves to the minimal qualified sets and maximal forbidden sets only. Recall that $\mathcal{Q}_{min}$ and $\mathcal{F}_{max}$ denote respectively the set of minimal qualified sets and maximal forbidden sets.

We are now in a position to give definition of a $\vec{t}$-$(k, \vec{n})^*$-VCS and then the definition of the basis matrices realizing it.

Definition 2.1 *Let* $\mathcal{P} = \{1, 2, 3, \ldots, n\}$ *be a set of participants. A* $\vec{t}$-$(k, \vec{n})^*$-*VCS on* $\mathcal{P}$ *is a visual cryptographic scheme such that the following two conditions hold:*

1. *Any minimal qualified set of participants can recover the secret.*
2. *Any maximal forbidden set of participants does not have any information about the secret image.*

Definition 2.2 *(via Basis Matrices) A* $\vec{t}$-$(k, \vec{n})^*$-*VCS is realized using two* $n \times m$ *binary matrices* S^0 *and* S^1 *called basis matrices, if there exist two sets of non-negative real numbers* $\{\alpha_X\}_{X \in \mathcal{Q}_{min}}$ *and* $\{t_X\}_{X \in \mathcal{Q}_{min}}$ *such that the following two conditions hold:*

1. (*contrast condition*) *If* $X \in \mathcal{Q}_{min}$, *then* S^0_X, *the "OR" of the rows indexed by* X *of* S^0, *satisfies* $w(S^0_X) \leq t_X - \alpha_X \cdot m$; *whereas, for* S^1 *it results in* $w(S^1_X) \geq t_X$.
2. (*security condition*) *If* $Y = \{i_1, i_2, \ldots, i_s\} \in \mathcal{F}_{max}$ *then the two* $s \times m$ *matrices* $S^0[Y]$ *and* $S^1[Y]$ *obtained by restricting* S^0 *and* S^1 *respectively to rows* $i_1, i_2, \ldots, i_s$ *are identical up to a column permutation.*

The number m is called the pixel expansion of the scheme. Also α_X and $\alpha_X \cdot m$ respectively denote the relative contrast and contrast of the recovered image reconstructed by the minimal qualified set X.

3 Construction of Basis Matrices

In this section we describe the method of constructing basis matrices for a monotone $\vec{t}$-$(k, \vec{n})^*$-VCS, where $\vec{t} = (t_1, t_2, \ldots, t_u)$, $\vec{n} = (n_1, n_2, \ldots, n_u)$ with $k = t_1 + t_2 + \cdots + t_u$. Let $\mathcal{P}_1 = \{1, 2, \ldots, n_1\}$, $\mathcal{P}_2 = \{n_1+1, n_1+2, \ldots, n_1+n_2\}, \ldots, \mathcal{P}_u = \{n_1+n_2+\cdots+n_{u-1}+1, \ldots, n_1+n_2+\cdots+n_{u-1}+n_u\}$ be the compartments in the access structure. We break the construction process into several simpler parts. Let on the participant set $\mathcal{P}_i$, for the (t_i, n_i)-VCS, the basis matrices be S^0_i and S^1_i and the corresponding pixel expansion be m_i, $i = 1, 2, \ldots, u$. Further, let $S^b_i = [C^b_{i,1} \quad C^b_{i,2} \quad \ldots \quad C^b_{i,m_i}]$, $b \in \{0, 1\}$, where $C^b_{i,j}$ denotes the jth column of S^b_i, where $j = 1, 2, \ldots, m_i$.
We now give describe the steps towards constructing the VCS for compartmented access structure.
Step 1:
Here we describe the construction method of the basis matrices for $\vec{t}_{ij}$-$(k_{ij}, \vec{n}_{ij})^*$-VCS, where $\vec{t}_{ij} = (t_i, t_j)$, $k_{ij} = t_i + t_j$ and $\vec{n}_{ij} = (n_i, n_j)$. For this construction, we consider the basis matrices (S^0_i, S^1_i) and (S^0_j, S^1_j) for the (t_i, n_i)-VCS and (t_j, n_j)-VCS respectively.
Consider the two following matrices

$$S^0_{ij} = \left[\begin{array}{cccc|cccc} m_jC^0_{i,1} & m_jC^0_{i,2} & ... & m_jC^0_{i,m_i} & m_jC^1_{i,1} & m_jC^1_{i,2} & ... & m_jC^1_{i,m_i} \\ S^0_j & S^0_j & ... & S^0_j & S^1_j & S^1_j & ... & S^1_j \end{array}\right] \text{ and}$$

$$S^1_{ij} = \left[\begin{array}{cccc|cccc} m_jC^0_{i,1} & m_jC^0_{i,2} & ... & m_jC^0_{i,m_i} & m_jC^1_{i,1} & m_jC^1_{i,2} & ... & m_jC^1_{i,m_i} \\ S^1_j & S^1_j & ... & S^1_j & S^0_j & S^o_j & ... & S^0_j \end{array}\right].$$

Though Lemma 3.1 (to be proved later), we shall show that the above two matrices are indeed basis matrices for $\vec{t}_{ij}$-$(k_{ij}, \vec{n}_{ij})^*$-VCS. Here the notation $m_jC^b_{i,k}$, $b \in \{0,1\}$, stands for the repetition of the $C^b_{i,k}$ column m_j times.

Step 2:
Here we describe the construction method of the basis matrices for $\vec{t}_{ijl}$-$(k_{ijl}, \vec{n}_{ijl})^*$-VCS where $\vec{t}_{ijl} = (t_i, t_j, t_l)$, $k_{ijl} = t_i + t_j + t_l$ and $\vec{n}_{ijl} = (n_i, n_j, n_l)$. Consider the two following matrices

$$S^0_{ijl} = \left[\begin{array}{cccc|cccc} m_lC^0_{ij,1} & m_lC^0_{ij,2} & ... & m_lC^0_{ij,m_{ij}} & m_lC^1_{ij,1} & m_lC^1_{ij,2} & ... & m_lC^1_{ij,m_{ij}} \\ S^0_l & S^0_l & ... & S^0_l & S^1_l & S^1_l & ... & S^1_l \end{array}\right] \text{ and}$$

$$S^1_{ijl} = \left[\begin{array}{cccc|cccc} m_lC^0_{ij,1} & m_lC^0_{ij,2} & ... & m_lC^0_{ij,m_{ij}} & m_lC^1_{ij,1} & m_lC^1_{ij,2} & ... & m_lC^1_{ij,m_{ij}} \\ S^1_l & S^1_l & ... & S^1_l & S^0_l & S^0_l & ... & S^0_l \end{array}\right].$$

Step $u-1$:
Construction of basis matrices for $\vec{t}_{12...(u-1)u}$-$(k_{12...(u-1)u}, \vec{n}_{12...(u-1)u})^*$-VCS where $\vec{t}_{12...u} = (t_1, t_2, \ldots, t_u)$, $k_{12...u} = t_1 + t_2 + \cdots + t_u$ and $\vec{n}_{12...u} = (n_1, n_2, \ldots, n_u)$. To construct the basis matrices, we consider the following matrices $(S^0_{12...(u-1)}, S^1_{12...(u-1)})$ and (S^0_u, S^1_u). Note that the basis matrices $(S^0_{12...(u-1)}, S^1_{12...(u-1)})$ is obtained recursively.
Consider the matrices

$$S^0_{12...u} = \left[\begin{array}{ccc|ccc} {}_uC^0_{12...(u-1),1} & ... & {}_lC^0_{12...(u-1),m_{12...(u-1)}} & {}_uC^1_{12...(u-1),1} & ... & {}_uC^1_{12...(u-1),m_{12...(u-1)}} \\ S^0_u & ... & S^0_u & S^1_u & ... & S^1_u \end{array}\right]$$

and

$$S^1_{12...u} = \left[\begin{array}{ccc|ccc} {}_uC^0_{12...(u-1),1} & ... & {}_lC^0_{12...(u-1),m_{12...(u-1)}} & {}_uC^1_{12...(u-1),1} & ... & {}_uC^1_{12...(u-1),m_{12...(u-1)}} \\ S^1_u & ... & S^1_u & S^0_u & ... & S^0_u \end{array}\right].$$

Remark: Note that in the above constructions, some of the t_i's may be 1. In that case, we consider $(1, n_i)$-VCS, although it does not make much sense in terms of practicality but it does mean that every participant alone can recover the secret. That means the parties must be given as their shares the secret itself! So the basis matrix S^0_i must be the $n \times 1$ column vector $[0, 0, 0, \ldots, 0]^t$ and S^1_i must be the $n \times 1$ column vector $[1, 1, 1, \ldots, 1]^t$. This also holds true if $n_i = 1$.

Let us first illustrate the above construction through the following example.

Example 3.1 *Let $\mathcal{P} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ be the set of parties and let $C_1 = \{1, 2, 3\}$, $C_2 = \{4, 5\}$, $C_3 = \{6, 7, 8, 9\}$ be a partition of $\mathcal{P}$ such that $t_1 = 2$, $t_2 = 2$, $t_3 = 3$ (notations have their usual meanings). Thus here we have the minimal qualified sets for the access structure as $\mathcal{Q}_{min} = \{124578, 124689, 124679, 124789, 125678, 125689, 125679, 125789, 134678, 134689, 134679, 134789, 135678, 135689, 135679, 135789, 234678, 234689, 234679, 234789, 235678, 235689, 235679, 235789\}$. For the sake of simplicity, we avoid the brackets, i.e., here 124578 stands for the set $\{1, 2, 4, 5, 7, 8\}$.*

Here we start with the visual cryptographic schemes $(2,3)$-VCS, $(2,2)$-VCS and $(3,4)$-VCS with $t_1 = 2$, $n_1 = 3$, $t_2 = 2$, $n_2 = 2$ and $t_3 = 3$, $n_3 = 4$ having the basis matrices as $S^0_1 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$, $S^1_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$; $S^0_2 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$, $S^1_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $S^0_3 =$

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}, \; S_3^1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Now to construct the basis matrices (S_{12}^0,S_{12}^1) realizing the above access structure we follow the technique described in Section 3. We take the following constituent basis matrices to construct the required matrices

$$S_{12}^0 = \left[\begin{array}{ccc|ccc} 2C_{1,1}^0 & 2C_{1,2}^0 & 2C_{1,3}^0 & 2C_{1,1}^1 & 2C_{1,2}^1 & 2C_{1,3}^1 \\ S_2^0 & S_2^0 & S_2^0 & S_2^1 & S_2^1 & S_2^1 \end{array}\right] \textit{ and}$$

$$S_{12}^1 = \left[\begin{array}{ccc|ccc} 2C_{1,1}^0 & 2C_{1,2}^0 & 2C_{1,3}^0 & 2C_{1,1}^1 & 2C_{1,2}^1 & 2C_{1,3}^1 \\ S_2^1 & S_2^1 & S_2^1 & S_2^0 & S_2^0 & S_2^0 \end{array}\right]$$

$$S_{123}^0 = \left[\begin{array}{cccccc|cccccc} 6C_{12,1}^0 & 6C_{12,2}^0 & 6C_{12,3}^0 & 6C_{12,4}^0 & 6C_{12,5}^0 & 6C_{12,6}^0 & 6C_{12,1}^1 & 6C_{12,2}^1 & 6C_{12,3}^1 & 6C_{12,4}^1 & 6C_{12,5}^1 & 6C_{12,6}^1 \\ S_3^0 & S_3^0 & S_3^0 & S_3^0 & S_3^0 & S_3^0 & S_3^1 & S_3^1 & S_3^1 & S_3^1 & S_3^1 & S_3^1 \end{array}\right]$$

and

$$S_{123}^1 = \left[\begin{array}{cccccc|cccccc} 6C_{12,1}^0 & 6C_{12,2}^0 & 6C_{12,3}^0 & 6C_{12,4}^0 & 6C_{12,5}^0 & 6C_{12,6}^0 & 6C_{12,1}^1 & 6C_{12,2}^1 & 6C_{12,3}^1 & 6C_{12,4}^1 & 6C_{12,5}^1 & 6C_{ij,6}^1 \\ S_3^1 & S_3^1 & S_3^1 & S_3^1 & S_3^1 & S_3^1 & S_3^0 & S_3^0 & S_3^0 & S_3^0 & S_3^0 & S_3^0 \end{array}\right].$$

Through the following lemmas, we are going to prove that the above mentioned recursive construction indeed produces basis matrices for the given compartmented access structure.

Lemma 3.1 *Let $(\overline{S^0}, \overline{S^1})$ be the basis matrices that realize a VCS for a general access structure $(\mathcal{Q}, \mathcal{F})$ on the set of participants $\overline{\mathcal{P}} = \{r+1, \ldots, r+n\}$ with pixel expansion m^*. Also let (V^0, V^1) be the basis matrices realizing a (k, r)-threshold VCS on a set of parties $\overline{\mathcal{P}} = \{1, 2, \ldots, r\}$ with pixel expansion m. If we write $V^0 = [C_1^0, C_2^0, \ldots, C_m^0]$ and $V^1 = [C_1^1, C_2^1, \ldots, C_m^1]$ where C_i^b denotes the ith column of the matrix V^b, $b \in \{0, 1\}$ then the following matrices (S^0, S^1) given by*

$$S^0 = \left[\begin{array}{cccc|ccc} m^*C_1^0 & m^*C_2^0 & ... & m^*C_m^0 & m^*C_1^1 & ... & m^*C_m^1 \\ \overline{S^0} & \overline{S^0} & ... & \overline{S^0} & \overline{S^1} & ... & \overline{S^1} \end{array}\right] \textit{ and}$$

$$S^1 = \left[\begin{array}{cccc|ccc} m^*C_1^0 & m^*C_2^0 & ... & m^*C_m^0 & m^*C_1^1 & ... & m^*C_m^1 \\ \overline{S^1} & \overline{S^1} & ... & \overline{S^1} & \overline{S^0} & ... & \overline{S^0} \end{array}\right]$$

realize a VCS on the participant set $\overline{\mathcal{P}} \cup \mathcal{P} = \{1, 2, \ldots, r, r+1, \ldots, r+n\}$ in which any minimal qualified set is the union of a minimal qualified set in $\mathcal{Q}_{min}$ with a minimal qualified set in the given threshold scheme.

Proof First we prove the security condition for the above construction. If we can prove the security condition for any maximal forbidden set in the resulting access structure then we are done. Now any maximal forbidden set F can arise in two different ways.

Case 1: Let $F = \overline{\mathcal{P}} \cup D$, where D is a $(k-1)$ subset of $\mathcal{P}$. Now since D is a forbidden set in the (k, r)-threshold VCS therefore it follows that the restricted matrices $V^0[D]$ and $V^1[D]$ are equal upto a column permutation. Without loss of generality, let $V^0[D] = V^1[D]$. Then the matrices obtained from them by replicating each column exactly m^* times should be equal. That is in our notation, $[m^*C_1^0[D] \cdots m^*C_m^0[D]] = [m^*C_1^1[D] \cdots m^*C_m^1[D]]$. Thus, when restricted to F the left (resp. right) portion of $S^0[F]$ is equal to the right (resp. left) portion of $S^1[F]$. This proves the security condition for this case.

Case 2: Let $F = \overline{F} \cup \mathcal{P}$, where $\overline{F} \in \underline{F_M}$. Now since $\overline{F}$ is a forbidden set, we may assume that the restricted matrices $(\overline{S^0}[\overline{F}], \overline{S^1}[\overline{F}])$ are equal. Now it is easy to see that when

restricted to F the left (resp. right) portion of $S^0[F]$ is equal to the right (resp. left) portion of $S^1[F]$. This completes the proof of security condition.

For proving the contrast condition we first mention that the pixel expansion of the resulting VCS is $2mm^*$. Let $\overline{\alpha}$ and α denote the relative contrasts of the $(\mathcal{Q}, \mathcal{F})$-VCS and (k, r)-threshold VCS respectively. Let X denote a minimal qualified set in the resulting access structure. Then $X = Q \cup B$, where $Q \in \mathcal{Q}_{min}$ and B is a k subset of $\mathcal{P}$.
Thus we have, $w(S^1_X) - w(S^0_X) \geq w(S^1_Q) - w(S^0_Q) \geq \overline{\alpha} m^*$. This proves the theorem. ■

Theorem 3.1 *The matrices $(S^0_{12\ldots u}, S^1_{12\ldots u})$ from a basis matrices for $\vec{t}_{12\ldots u}$-$(k_{12\ldots u}, \vec{n}_{12\ldots u})^*$-VCS with pixel expansion $2^{u-1} \cdot m_1 m_2 \cdots m_u$, where m_i is the pixel expansion of the (t_i, n_i)-VCS on the participant set $\mathcal{C}_i$.*

Proof: Proof of the theorem follows from the construction method in Section 3 and applying Lemma 3.1, $(u-1)$ times.
Remark: There exists VCS for any compartmented access structure $\vec{t}$-$(k, \vec{n})^*$-VCS with pixel expansion $2^{u-1} \cdot m_1 m_2 \cdots m_u$, where m_i is the pixel expansion of the (t_i, n_i)-VCS on the participant set $\mathcal{C}_i$. Moreover, letting $u = 2$, $|\mathcal{C}_1| = 1$ and $|\mathcal{C}_2| = n - 1$ with $t_1 = 1$ we have Theorem 2.3 in [4]. Also, if $u = 2$ and $|\mathcal{C}_1| = t$ and $|\mathcal{C}_2| = n - t$ with $t_1 = t$ we have Theorem 4 in [10].

3.1 Finding Closed Form for Relative Contrast

Theorem 3.1, ensures the existence of a compartmented VCS. However, finding closed form of relative contrast is a combinatorially challenging problem. In this section, we come up with a closed form of relative contrast for compartmented access structure using canonical threshold VCS. First let us define what a canonical VCS [6] is.

Let c denote a Boolean vector with $\overline{c}$ obtained from c complementing all its entries. In Boolean matrices S^0 and S^1 for $i = 0, 1$, let $f_{c,i}$ be the multiplicity of the column c in S^i, that is $f_{c,i}$ is the number of times the column c appears in S^i.

Definition 3.1 *[6] The basis matrices S^0 and S^1 of a (k, n)-VCS are in canonical form if, for $i = 0, 1$, the following two properties are satisfied.*

1. *For any two columns c and c' such that $wt(c) = wt(c')$, it results that $f_{c,i} = f_{c',i}$.*
2. *For any column c, it results that*

$$f_{c,i} = \begin{cases} f_{\overline{c},i} & \text{if } k \text{ is even} \\ f_{\overline{c},1-i} & \text{if } k \text{ is odd.} \end{cases}$$

A (k, n)-VCS whose basis matrices are in canonical form is referred to as a canonical (k, n)-VCS.

The second condition is too stringent and results in too much of pixel expansion. So the first condition is later taken to be the sole condition for defining canonical visual cryptographic scheme. To calculate the closed form of the relative contrast, let us use the following lemmas.

Lemma 3.2 *Let (S^0_i, S^1_i) denote canonical basis matrices for a (t_i, n_i)-VCS with pixel expansion m_i. Let $\mu^b_{l_i,i}$ denote the number of occurrences of each column of weight l_i in the basis matrix S^b_i, where $i = 1, 2, ..., u$ and $b \in \{0, 1\}$. For a minimal qualified set X, let us further assume $\vec{W_i}^b = (C^b_{X,i,1}, C^b_{X,i,2}, ..., C^b_{X,i,m_i})$ where $C^b_{X,i,j}$ is the "OR" of the jth column of the restricted matrix $S^b_i[X]$. Let Z^b_i denote the number of zeros in $\vec{W}^b_i$*
Then $Z^b_i = \sum_{l_i=0}^{n_i - t_i} \binom{n_i - t_i}{l_i} \mu^b_{l_i,i}$, where $i = 1, 2, ..., u$, $b \in \{0, 1\}$.

Proof: Let us understand the logic behind the counting principle. Let us suppose $\mu^0_{l_i,i}$ denote the frequency with which each column of weight l_i occur in basis matrix S^0_i. Let X be a minimal qualified set having t_i many parties in it. Observe that for a column vector $\vec{C}$ if at least one its entries is 1 then the "OR" of all the entries of the column becomes 1. Thus the "OR" value is 0 if and only if all the entries in the column are 0. We note that a column with weight l_i when restricted to X will have all zero entries if the l_i many 1's appear at positions which are not indexed by the indices in X. Therefor, those l_i many 1's can appear anywhere among the $(n_i - t_i)$ entries left in the column $\vec{C}$. Now, each column of weight l_i appears exactly $\mu^0_{l_i,i}$ times. Therefore, total number of columns with weight l_i and having zeros at the positions which are indexed by X is given by the expression $\binom{n_i - t_i}{l_i}\mu^0_{l_i,i}$. Also observe that if a column has weight $n_i - t_i$ or greater then it is not possible to get all zeros at the positions indexed by X. At least one 1 must appear somewhere. Varying l_i over $\{0, 1, \ldots, n_i - t_i\}$ we get the required expression for $b = 0$. Same is the argument for $b = 1$.

Lemma 3.3 *Let $\vec{W}^b_{12\ldots u} = (C^b_{X,12\ldots u,1}, C^b_{X,12\ldots u,2}, \ldots, C^b_{X,12\ldots u,u})$ where $C^b_{X,12\ldots u,j}$ denotes "OR" of the jth column of the restricted matrix $S^b_{12\ldots u}[X]$, for the minimal qualified set X of the access structure $\vec{t}_{12\ldots u}$-$(k_{12\ldots u}, \vec{n}_{12\ldots u})^*$-VCS having pixel expansion $m_{12\ldots u}$. Let $Z^b_{12\ldots u}$ denote the number of zeros in $\vec{W}^b_{12\ldots u}$, where $b \in \{0, 1\}$. Then*

$$Z^0_{12\ldots u} = \sum_{\vec{x}=(x_1,\ldots,x_u) such\ that\ wt(\vec{x})\ is\ even} Z_1^{x_1}\ Z_2^{x_2}\ \ldots\ Z_u^{x_u}$$

and

$$Z^1_{12\ldots u} = \sum_{\vec{x}=(x_1,\ldots,x_u) such\ that\ wt(\vec{x})\ is\ odd} Z_1^{x_1}\ Z_2^{x_2}\ \ldots\ Z_u^{x_u}.$$

Proof: Let us first write the minimal qualified set X as the disjoint union of parts $X_1, X_2, \ldots, X_u$ where each X_i is a subset of the ith level participants. Applying Lemma 3.2 separately for each X_i and then patching them up keeping in mind the construction given in Section 3 we get the result.

The following theorem is now straight-forward.

Theorem 3.2 *For a given compartmented access structure $\vec{t}_{12\ldots u}$-$(k_{12\ldots u}, \vec{n}_{12\ldots u})^*$, there exists a $\vec{t}_{12\ldots u}$-$(k_{12\ldots u}, \vec{n}_{12\ldots u})^*$-VCS with pixel expansion $m = 2^{u-1}\ m_1\ m_2\ \cdots\ m_u$ and relative contrast $\frac{\prod_{i=1}^{u}(Z_i^0 - Z_i^1)}{m}$.*

4 Probabilistic Construction

In this section we adopt the method of Yang [16] to construct non-expansible, probabilistic $\vec{t}$-$(k, \vec{n})^*$-VCS with the help of basis matrices realizing the same access structure in the deterministic model of VCS. We first give a generic construction method of probabilistic VCS realizing any general access structure and then we describe a method that realizes $\vec{t}$-$(k, \vec{n})^*$-VCS with better contrast. In the probabilistic scheme the secret image will be correctly recovered only with a certain probability. Let Q be a qualified set. Let $P_{w/w}(Q)$ be the probability of correctly reconstructing a white pixel in white from the S^0 matrix and $P_{w/b}(Q)$ be the probability of incorrectly reconstructing a black pixel in white from the S^0. Similarly we define the notations $P_{b/b}(Q)$ and $P_{b/w}(Q)$. To capture the idea of probability of correct reconstruction of the secret image we take the differences of the following probabilities:

$$P_{b/b}(Q) - P_{b/w}(Q) \tag{1}$$

and

$$P_{w/w}(Q) - P_{w/b}(Q). \tag{2}$$

Now a scheme is said to be β -probabilistic if there exists a positive constant β such that for any qualified set Q

$$P_{b/b}(Q) - P_{b/w}(Q) \geq \beta \tag{3}$$

and

$$P_{w/w}(Q) - P_{w/b}(Q) \geq \beta. \tag{4}$$

We now give the definition of a β-probabilistic VCS for general access structure as follows.

Definition 4.1 *Let $(\mathcal{Q}, \mathcal{F})$ denote a general access structure on a set of n participants. A β-probabilistic $(\mathcal{Q}, \mathcal{F})$ is defined by two collection of $n \times 1$ matrices C_W and C_B such that*

1. *There exists $\beta > 0$, such that for any minimal qualified set $Q \in \mathcal{Q}_{min}$ it must hold that $P_{b/b}(Q) - P_{b/w}(Q) \geq \beta$.*
2. *For any maximal forbidden set $F \in \mathcal{F}_{max}$, the two restricted collections $\{M^0[F] : M^0 \in C_W\}$ and $\{M^1[F] : M^1 \in C_B\}$ contain the same matrices with equal frequencies.*

We will use this definition to realize a general access structure in the probabilistic model. First we give a generic construction method of probabilistic VCS for general access structure based on Ateniese et al.'s construction [5] and Yang's construction [16]. Later on we shall show that the direct construction of probabilistic VCS for compartmented access structure based on the basis matrix construction as described in Section 3 has better relative contrast and pixel expansion than the construction based on cumulative array as described below.

4.1 Construction of Probabilistic VCS for General Access Structure

Let $(\mathcal{Q}, \mathcal{F})$ denote a general access structure on a set of n participants. For the sake of completeness, let us first define the prerequisite terms and then discuss about the construction method of deterministic VCS for general access structure as explained in [5].

A *cumulative map* (β, T) for $\mathcal{F}$ is a finite set T along with a mapping $\beta : \mathcal{P} \to 2^{\mathcal{P}}$ such that for $Q \subseteq \mathcal{P}$,

$$\bigcup_{a \in Q} \beta(a) = T \Leftrightarrow Q \in \mathcal{Q}.$$

A cumulative map (β, T) for any access structure can be constructed by using the collection of the maximal forbidden sets $\mathcal{F}_{max} = \{F_1, F_2, \ldots, F_t\}$ as follows. Let $T = \{T_1, T_2, \ldots, T_t\}$ and for any $i \in \mathcal{P}$, let $\beta(i) = \{T_j \mid i \notin F_j, 1 \leq j \leq t\}$. A *cumulative array* for $\mathcal{Q}$ can be constructed from the given cumulative mapping of $\mathcal{Q}$. A cumulative array is a $|\mathcal{P}| \times |T|$ Boolean matrix, denoted by CA, such that $CA(i, j) = 1$ if and only if $i \notin F_j$.

Let $t = |\mathcal{F}_{max}|$. Let CA be the cumulative array for $\mathcal{Q}$ obtained by using the cumulative map. Let $\widehat{S}^0$ and $\widehat{S}^1$ be the basis matrices for a (t, t)-VCS constructed by Naor and Shamir [12]. The basis matrices S^0 and S^1 for a VCS for the access structure $(\mathcal{Q}, \mathcal{F})$ can be constructed as follows. For any fixed i let $j_{i,1}, \ldots, j_{i,g_i}$ be the integers j such that $\mathrm{CA}(i, j) = 1$. The ith row of S^0 (S^1, resp.) consists of the "OR" of the rows $j_{i,1}, \ldots, j_{i,g_i}$ of $\widehat{S}^0$ ($\widehat{S}^1$, resp.). Then we have a deterministic $(\mathcal{Q}, \mathcal{F}, m)$-VCS with $m = 2^{t-1}$.

Construction of Probabilistic VCS for General Access Structure:
If we define $C_W = \{\vec{c} : \vec{c}$ *is a column of* $S^0\}$ and $C_B = \{\vec{d} : \vec{d}$ *is a column of* $S^1\}$ then

it is easy to see that these collections realize a probabilistic VCS on $(\mathcal{Q}, \mathcal{F})$ with relative contrast $\gamma = \frac{1}{2^{|\mathcal{F}_{max}|-1}} = \beta$.

Thus we have the following theorem.

Theorem 4.1 *Given any monotone access structure $(\Gamma_{qual}, \Gamma_{Forb})$ on a set of n participants, there exists a β-probabilistic VCS with $\beta = \frac{1}{2^{|\mathcal{F}_{max}|-1}}$, where $\mathcal{F}_{max}$ denotes the set of all maximal forbidden sets for the access structure $(\Gamma_{qual}, \Gamma_{Forb})$.*

Now, if we use the above construction method for constructing $\vec{t}$-$(k, \vec{n})^*$-VCS, we have the following Corollary.

Corollary 1 *For any given compartmented access structure $\vec{t}$-$(k, \vec{n})^*$, there exists a β-probabilistic $\vec{t}$-$(k, \vec{n})^*$-VCS with pixel expansion $m = 2^{sum} - 1$, where $sum = \binom{n_1}{t_1 - 1} + \binom{n_2}{t_2 - 1} + \cdots + \binom{n_u}{t_u - 1}$ and $\beta = \frac{1}{m}$.*

Proof: The proof follows from the fact that in case of compartmented access structure, $|\mathcal{F}_{max}| = \binom{n_1}{t_1 - 1} + \binom{n_2}{t_2 - 1} + \cdots + \binom{n_u}{t_u - 1}$. ■

4.2 Construction of Probabilistic $\vec{t}$-$(k, \vec{n})^*$-VCS

Based on the construction as described in Section 3 and the method proposed in [16], we are going to state the following Theorem.

Theorem 4.2 *For a given compartmented access structure $\vec{t}_{12\ldots u}$-$(k_{12\ldots u}, \vec{n}_{12\ldots u})^*$-VCS there exists a β-$\vec{t}_{12\ldots u}$-$(k_{12\ldots u}, \vec{n}_{12\ldots u})^*$VCS with $\beta = \frac{\prod_{i=1}^{u}(Z_i^0 - Z_i^1)}{m}$.*

4.3 Comparison among the schemes

In this section we provide few numerical evidences in Table 1 to justify that our direct construction method for compartmented access structure works better in terms of both pixel expansion as well as relative contrast (or β-probability) than the scheme obtained through Corollary 1 in Section 4.1.

5 Concluding Remarks and Open Issues

We have considered here an efficient direct construction of a visual cryptographic scheme for compartmented access structure having a closed form of both pixel expansion as well as relative contrast. Numerical evidence shows that our scheme performs better in terms of both relative contrast as well as pixel expansion than the cumulative array based construction obtained as a particular case of general access structure. Finding better scheme in terms of relative contrast and pixel expansion could be future direction of research.

Acknowledgement

Initial phase of this research work of the first author is supported by CSIR PhD Fellowship, Government of India, Grant No. 09/028(0808)/2010-EMR-I. Research of the third author is partially supported by National Board for Higher Mathematics, Department of Atomic Energy, Government of India, Grant No. 2/48(10)/2013/NBHM(R.P.)/R&D II/695.

Access structure	m_1	m_2	m_3	m_{our}	m_{CA}	β_{our}	β_{CA}
(2,2),(2,4)	2	8		32	32	1/32	1/32
(2,3),(2,3)	3	3		18	32	1/18	1/32
(2,2),(3,4)	2	6		24	128	1/24	1/128
(2,2),(4,4)	2	8		32	32	1/32	1/32
(2,3),(3,3)	3	4		24	32	1/24	1/32
(2,2),(2,2),(2,2)	2	2	2	32	32	1/32	1/32
(2,3),(2,4)	3	8		48	64	1/48	1/64
(1,3),(2,4)	1	8		16	16	1/16	1/16
(2,5),(2,2)	15	2		60	64	1/60	1/64
(3,5),(2,2)	16	2		32	512	1/32	1/512
(1,5),(2,2)	1	2		4	4	1/4	1/4
(1,2),(2,3),(2,2)	1	3	2	24	32	1/24	1/32

Table 1: Comparison between two schemes: m_{our} and β_{our} stand for the pixel expansion and the β probability for the scheme as described in Section 4.2 while m_{CA} and β_{CA} stand for the pixel expansion and the β probability for the scheme as described in Section 4.1

References

[1] Adhikari, A., "Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images", Design, Codes and Cryptography 73(3): 865-895 (2014).

[2] Adhikari, A., Dutta, T. K., and Roy, B., "A New Black and White Visual Cryptographic Scheme for General Access Structures," INDOCRYPT'04, Lecture Notes in Computer Science, Springer-Verlag, 3348, 399-413 (2004).

[3] Adhikari, A., and Bose, M., "A New Visual Cryptographic Scheme Using Latin Squares," IEICE Transactions on Fundamentals, E87-A, No. 5, 1998-2002 (2004).

[4] Arumugam, S., Lakshmanan, R., Nagar, A.K., "On (k, n)*-visual cryptography scheme", Design, Codes and Cryptography 71(1): 153-162 (2014).

[5] Ateniese, G. Blundo, C. Santis, A. De and Stinson, D.R., " Visual Cryptography for General Access Structures", Information and Computation, vol.129, 86-106 (1996).

[6] Blundo, C., D'arco, P., Santis, A. De and Stinson, D. R., "Contrast optimal threshold visual cryptography," SIAM J. of Discrete Math., vol. 16, issue 2, 224-261 (2003).

[7] Cimato S., De Prisco R., and De Santis A., "Probabilistic visual cryptography schemes", The Computer Journal, 49(1), 97-107 (2006).

[8] Dutta, S. and Adhikari, "A. XOR Based Non-monotone t-$(k, n)^*$-Visual Cryptographic Schemes Using Linear Algebra",(ICICS 2014), Lecture Notes in Computer Sciences, Springer, Volume 8958, pp 230-242.

[9] Dutta, S., Singh Rohit., R., and Adhikari, A. "Constructions and Analysis of Some Efficient t-$(k, n)^*$-Visual Cryptographic Schemes Using Linear Algebraic Techniques", Des. Codes Cryptography 80(1), 165-196 (2016).

[10] Teng Guo, Feng Liu, ChuanKun Wu, YaWei Ren, Wen Wang, "On (k,n) Visual Cryptography Scheme with t Essential Parties", ICITS 2013, Lecture Notes in Computer Science, 56-68 (2014).

[11] Ito R., Kuwakado H., and Tanaka H., "Image size invariant visual cryptography", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E82A(10), 2172-2177 (1999).

[12] Naor, M. and Shamir, A., "Visual Cryptography", Advance in Cryptography, Eurocrypt'94, Lecture Notes in Computer Science 950, 1-12, Springer-Verlag (1994).

[13] Kanakkath Praveen, K. Rajeev, M. Sethumadhavan, "On the Extensions of (k, n)*-Visual Cryptographic Schemes", SNDS 2014, CCIS 420, 231-238 (2014).

[14] S. J. Shyu and M. C. Chen, "Optimum pixel expansions for threshold visual secret sharing schemes", IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pt. 2, 960-969 (2011).

[15] Gustavus J. Simmons., "How to (really) share a secret", CRYPTO'88, Lecture Notes in Computer Science, LNCS 403, 390-448 (1990).

[16] Yang C.-N., "New visual secret sharing schemes using probabilistic method", Pattern Recognition Letters, 25, 481-494 (2004).

[17] Yang C.-N. and Chen T.-S., "Size-adjustable visual secret sharing schemes", IEEE Trans. Fundamentals, 88, 2471-2474 (2005).