Designs, Codes and Cryptography (2019) 87:1699–1711
https://doi.org/10.1007/s10623-018-0570-6

Maximal contrast color visual secret sharing schemes

Sabyasachi Dutta[1] · **Avishek Adhikari**[2] · **Sushmita Ruj**[3]

Received: 10 February 2018 / Revised: 15 September 2018 / Accepted: 4 October 2018 /
Published online: 26 October 2018

Abstract
The transition of visual secret sharing from a *black & white* secret image to a color image is not straight-forward. There are several models of color superposition principle. In this paper we present color visual cryptographic scheme realizing monotone access structure. We first give a generic construction method to share a color image in same color model. In particular, our construction achieves maximal contrast. We also give a direct and efficient construction of visual secret sharing for $(k, n)^*$-access structure.

Keywords Color visual secret sharing · Cumulative array · Essential participant · Pixel expansion · Contrast

Mathematics Subject Classification 15A03 · 94A60

1 Introduction

A 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 in the form of transparencies on which the shares are photocopied. Such shares have the property that only "qualified" subsets of participants can visually recover the secret image by carefully stacking the transparencies. A monotone

Communicated by C. Blundo.

✉ Avishek Adhikari
avishek.adh@gmail.com

Sabyasachi Dutta
saby.math@gmail.com

Sushmita Ruj
sush@isical.ac.in

[1] R C Bose Centre for Cryptology & Security, Indian Statistical Institute, 203, B T Road, Kolkata 700108, India

[2] Department of Pure Mathematics, University of Calcutta, 35, Ballygunge Circular Road, Kolkata 700019, India

[3] Cryptology & Security Research Unit, Computer & Communication Sciences Division, Indian Statistical Institute, 203, B T Road, Kolkata 700108, India

(k, n)-threshold visual cryptographic scheme consists of two phases - *sharing* phase and *reconstruction* phase. During the sharing phase the dealer encodes the secret image into n pieces and gives each participant a piece. He does this encoding in such a manner that *any* set of k or more participants can reconstruct the secret image by stacking their shares and any set of $k-1$ or less participants can not reconstruct the secret. During the reconstruction phase if k or more participants come together and carefully stack their shares they will be able to retrieve the secret image visually with some loss in contrast.

The first threshold black and white VCS was proposed by Naor and Shamir [23]. This concept has been extended in [1–3,5,7–10,16,25] to general access structures. Recently Arumugam et al. [6] considered a special type of access structure lying in between the threshold access structure and general access structure. They called it $(k, n)^*$-access structure, to address the scenario where one participant is "essential" and he needs the help of any $k-1$ parties other than him, to recover the secret image. Some of the works that forwarded this idea can be found in [14,15,17,25].

Color visual cryptography was first conceptualized by Verheul–Tilborg [27]. They first showed how to share a colored secret image among participants and gave construction of a color (n, n)-visual cryptographic scheme. The transition from sharing a black and white image to sharing a colored image is not straight-forward. There are issues with the color superposition principle. In B/W image superposition of two white pixels results in white pixel whereas if at least one of the two is a black pixel, the resulting pixel is black. The situation is not so simple for color images. Superposition of two different colors may give rise to a third color. Therefore, conceptualizing the model of color superposition is absolutely necessary. Broadly speaking, there are three major color models [13]: *same color* model, *no darkening* model and *general* model. In the same color model, the superposition of pixels with different colors is not allowed with the exception of the annihilator/masking "•" color. Thus superposing two same colored pixels gives back that color while superposing a colored pixel with "•" gives back "•". However in this model the darkening problem is not addressed. Superposition of two i colored pixels gives back one i colored pixel. The no-darkening model is similar to the same color model in the sense that two different colors cannot be superimposed but differs in the fact that when two or more same colored pixels are superimposed then a darker version of the color is reconstructed. Finally, in the general model no restrictions on superpositions are put - the color superposition satisfies real world color superposition principles. So the darkening problem is also considered.

The work of Cimato et al. [12] considered the construction of (k, n)-threshold color visual secret sharing in the no-darkening model. Their construction was based on the basis matrices of a $(k-1, k-1)$-threshold black & white visual cryptographic scheme. The pixel expansion of the resulting c-color VCS is given by $c\binom{n}{k}2^{k-2}$ and achieves "maximal contrast". The term maximal contrast loosely means that while trying to recover a pixel of some color no other false colored pixel is reconstructed. They have also given a construction for c-color $(2, n)$-VCS with pixel expansion $c(n-1)$. The general model of color superposition was considered in an early work by Rijmen et al. [24]. The works [4,21] also considered the real color superposition principles. Using results from the [4,21] one can generically construct $(2, n)$-threshold color visual secret sharing schemes from black and white cryptographic schemes. In the same color model there are various works e.g. [10,11,27,28]. All of these works encode the color pixels in such a manner that the (implementation of) superpositions of pixels satisfy the same color model. Verheul et al. [27] constructed c color (n, n)-threshold scheme, $(k, c-1)$-threshold scheme and (k, c)-scheme when c is a prime power. This makes the constructions quite restrictive in nature. Blundo et al. [10] gave constructions of c color

$(2, n)$-schemes and (n, n)-schemes. Koga et al. [21] and Yang et al. [28] provided color visual cryptographic schemes for (k, n)-threshold access structures. Moreover, the latter gave a construction method for color VCS realizing general access structures. Several other color visual cryptographic schemes [18,20,22,26] were proposed that have extra features. Iwamoto [19] introduced a "weaker notion of security" and formulated integer linear programming to color VCS. For more literature and in-depth survey one can refer to [13].

Our contribution: We first provide a generic construction method to realize a color visual secret sharing scheme over any monotone access structure in the same-color model. Moreover our scheme achieves maximal contrast. Next we give a direct construction method (in Sect. 3.2) for an important class of access structures viz. $(k, n)^*$-access structure based on color $(k-1, n-1)$-scheme. We also study the relationship between the parameters of the schemes. Lastly we conclude the paper with some experimental results.

2 Prerequisites

We state some basic definitions and concepts that will be needed throughout this paper.

2.1 The color model

We will follow the Verheul–Tilborg [27] model of color visual cryptography (CVCS). The model can be perceived as the Same Color model (SC model) of color visual cryptography. In this model, a colored image is an array of pixels each of which may have one of the c different colors $0, 1, \ldots, c-1$.

The infrastructure of the color superposition principle is the following:
Each secret pixel is divided into m subpixels of color $0, 1, \ldots, c-1$. If some subpixels are placed one top of the other and held to light then a light of color i filters through the stacked subpixels if and only if all the subpixels are color i. Otherwise, no light i.e. *black* color filters through the stacking. The color "*black*" is denoted by $\bullet$ and always is distinguishable from the c colors.
The "generalized OR"(GOR) denoted by $\vee$, of the elements $0, 1, \ldots, c-1$ is defined as follows: $i \vee i = i$ and $i \vee \bullet = \bullet$ for all $i = 0, 1, \ldots, c-1$ and $i \vee j = \bullet$ for all $i \neq j$ where $i, j = 0, 1, \ldots, c-1$.
For any n-dimensional vector V with entries from the set $\{0, 1, \ldots, c-1\}$, we will denote with $z_i(V)$, the number of coordinates in V equal to i where $i = 0, 1, \ldots, c-1$. For example, if $V = (0, 1, 1, 2, 2, 2)$ with entries from the set $\{0, 1, 2\}$, then $z_0(V) = 1$, $z_1(V) = 2$ and $z_2(V) = 3$.

2.2 Color visual cryptographic scheme

A (k, n) threshold access structure consists of some "qualified sets" and some "forbidden sets". Any subset containing k or more participants is a qualified set and rest are forbidden sets. We are now in a position to define an *unconditionally secure* (k, n)-threshold visual cryptographic scheme with c colors. We will denote such a scheme by $(k, n)_c$-CVCS where small letter c denotes the number of *true* colors.

Definition 1 Let $\mathcal{P} = \{1, 2, \ldots, n\}$ be a set of participants. A c-colored (k, n)-threshold visual cryptographic scheme on $\mathcal{P}$ is a scheme that satisfies following two conditions:

1. Any subset of k participants can recover the secret image.
2. Any subset of participants with size strictly less than k does not have any information about the secret image.

A $(k, n)_c$-CVCS scheme can be implemented by means of c many *basis* matrices $S^0, S^1, \ldots, S^{c-1}$ where S^b corresponds to the color $b \in \{0, 1, \ldots, c-1\}$. Entries of the matrices come from the set $\{0, 1, \ldots, c-1\}$. During *share generation* phase the dealer chooses the matrix S^b, if the secret pixel is $b \in \{0, 1, \ldots, c-1\}$ and then applies a random column permutation on the matrix S^b and gives the participant P_i the i-th row of the resulting matrix as the participant's share for all i. When the dealer wants to share a c-colored image then for each constituent pixel he repeatedly performs the above process till all the pixels are shared. We now formally define what basis matrices are.

Definition 2 (*Adopted from* [10,28]) A $(k, n)_c$-CVCS with pixel expansion m is realized using c many $n \times m$ matrices $S^0, S^1, \ldots, S^{c-1}$ called basis matrices, if there exist two non-negative numbers h, l with $l < h$ such that the following two conditions hold:

1. (*Contrast condition*) If $X = \{i_1, i_2, \ldots, i_k\} \subseteq \mathcal{P}$ i.e., if X is a qualified set, then for any $b \in \{0, 1, \ldots, c-1\}$ the component-wise "GOR" of the rows of S^b indexed by X denoted by S^b_X, satisfies $z_b(S^b_X) \geq h$; whereas, for $b' \neq b$ it results in $z_{b'}(S^b_X) \leq l$.
2. (*Security condition*) If $Y = \{i_1, i_2, \ldots, i_s\} \subset \mathcal{P}$ with $s < k$ then the c many $s \times m$ restricted matrices $S^0[Y]$, $S^1[Y]$, $\ldots$, $S^{c-1}[Y]$ obtained by restricting $S^0, S^1, \ldots, S^{c-1}$ respectively to rows indexed by $i_1, i_2, \ldots, i_s$ are identical up to column permutations.

The above definition can be extended from (k, n) threshold access structure to any arbitrary access structure on a set of participants. An access structure on a set of parties $\mathcal{P} = \{1, 2, \ldots, n\}$ can be described by the collection of all qualified sets $\mathcal{Q}$ and forbidden sets $\mathcal{F}$. The collection of *minimal* qualified sets is defined as $\mathcal{Q}_{min} = \{B \subseteq \mathcal{P} : \forall C \subsetneq B,\ C \in \mathcal{F}\}$. On the other hand, the collection of *maximal* forbidden sets is defined as $\mathcal{F}_{max} = \{F \subseteq \mathcal{P} : \forall i \notin F,\ F \cup \{i\} \in \mathcal{Q}\}$. We consider monotone access structure in which if a set B is qualified then so is every set that contains B and if F is a forbidden set then so is every subset of it. Hence if we specify $\mathcal{Q}_{min}$ and $\mathcal{F}_{max}$, the access structure is uniquely specified. We now define basis matrices for color VCS realizing a general access structure $(\mathcal{Q}, \mathcal{F})$ with c many colors.

Definition 3 (*Adapted from* [28]) A $(\mathcal{Q}, \mathcal{F})_c$-CVCS with pixel expansion m is realized using c many $n \times m$ matrices $S^0, S^1, \ldots, S^{c-1}$ called basis matrices, if there exist two non-negative numbers h, l with $l < h$ such that the following two conditions hold:

1. (*Contrast condition*) If $X \in \mathcal{Q}$ i.e., if X is a qualified set, then for any $b \in \{0, 1, \ldots, c-1\}$ the component-wise "GOR" of the rows of S^b indexed by X, satisfies $z_b(S^b_X) \geq h$; whereas, for $b' \neq b$ it results in $z_{b'}(S^b_X) \leq l$.
2. (*Security condition*) If $Y \in \mathcal{F}$ then the c many $s \times m$ restricted matrices $S^0[Y]$, $S^1[Y]$, $\ldots$, $S^{c-1}[Y]$ obtained by restricting $S^0, S^1, \ldots, S^{c-1}$ respectively to rows indexed by the participants of Y, are identical up to column permutations.

In [10] the contrast of a color VCS is defined as $\alpha = \frac{h-l}{h+l}$ (keeping parity with [27]) and the *loss of contrast* is measured by $\frac{h-l}{m(h+l)}$. However, in [11] the contrast of a CVCS is

defined to be the value $\frac{h-l}{m}$ keeping parity with the well-known definition of contrast given in [23]. Paper [10] defines a scheme to be *maximal contrast* CVC if the value $l = 0$. That is, a scheme is of maximal contrast if while trying to reconstruct a color $i \in \{0, 1, \ldots, c-1\}$ no other colored pixel $j(\neq i)$ is reconstructed. We summarize in the following definition.

Definition 4 (*Adopted from* [10]) Keeping the same notations as Definition 3, the contrast of a color CVCS is defined to be $\alpha = \frac{h-l}{h+l}$. A scheme is said to have *maximal contrast* if $l = 0$.

3 Main results

We first construct color visual cryptographic schemes for any monotone general access structure. As a building block we assume the existence of $(n, n)_c$-CVCS [10,12,19,21,28].

3.1 Color VCS for general access structures

We present a construction technique to realize color visual cryptographic schemes for any monotone general access structure. Moreover our construction method achieves maximal contrast. Let $\mathcal{P} = \{1, 2, \ldots, n\}$ be a set of n participants and $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ be a given access structure. Let $\mathcal{Q}_{min} = \{B_1, B_2, \ldots, B_r\}$ and $\mathcal{F}_{max} = \{F_1, F_2, \ldots, F_t\}$. We will keep these notations fixed for the rest of this section.

We take the help of construction of $(n, n)_c$-CVCS and use the *cumulative array* of the given access structure.

First we recall the idea of cumulative array (see [7]) for $\mathcal{Q}_{min}$. The cumulative array (CA) is an $n \times t$ Boolean matrix such that $CA(i, j) = 1$ if and only if $i \notin F_j$ where n is the number of participants, $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, t\}$.

Example 1 The cumulative array for the access structure on a set of six participants with $\mathcal{Q}_{min} = \{1234, 1235, 1236\}$ is given by,

Parties	$F_1 = \{123\}$	$F_2 = \{12456\}$	$F_3 = \{13456\}$	$F_4 = \{23456\}$
1	0	0	0	1
2	0	0	1	0
3	0	1	0	0
4	1	0	0	0
5	1	0	0	0
6	1	0	0	0

where {123} means the set {1, 2, 3}, {12456} means the set {1, 2, 4, 5, 6} etc.

Let us consider our access structure $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ on a set of n parties $\mathcal{P}$ where $\mathcal{F}_{max} = \{F_1, F_2, \ldots, F_t\}$.
Let $S^0_{(t,t)}, S^1_{(t,t)}, \ldots, S^{c-1}_{(t,t)}$ respectively denote the basis matrices obtained for the c colors corresponding to a (t, t)-threshold access structure. Constructions of such basis matrices can be found in [10,12,19,21,28]. Each of basis matrices has size $t \times m$, where the t rows are indexed by the maximal forbidden sets $\{F_1, F_2, \ldots, F_t\}$ with respect to which the CA is constructed. Here m denotes the pixel expansion of the $(t, t)_c$-CVCS.

Let us write

$$S^0_{(t,t)} = \begin{bmatrix} .. & R^0_1 & .. \\ .. & R^0_2 & .. \\ .. & .. & .. \\ .. & R^0_t & .. \end{bmatrix}, \quad S^1_{(t,t)} = \begin{bmatrix} .. & R^1_1 & .. \\ .. & R^1_2 & .. \\ .. & .. & .. \\ .. & R^1_t & .. \end{bmatrix}, \ldots\ldots\ldots\ldots, S^{c-1}_{(t,t)} = \begin{bmatrix} .. & R^{c-1}_1 & .. \\ .. & R^{c-1}_2 & .. \\ .. & .. & .. \\ .. & R^{c-1}_t & .. \end{bmatrix},$$

where $\cdot R^\alpha_i \cdot$ denotes the ith row of $S^\alpha_{(t,t)}$ for all colors $\alpha = 0, 1, \ldots, c-1$ and for all $i = 1, 2, \ldots, t$.

Now *construct* the following $n \times m$ matrices $S^0, S^1, \ldots, S^{c-1}$ as indicated:
Let $i \in \{1, 2, \ldots, n\}$ i.e. i be a participant and also assume i does not belong to the maximal forbidden sets $F_{j_1}, F_{j_2}, \ldots, F_{j_s}$.

For the color $\alpha \in \{0, 1, \ldots, c-1\}$, construct

i-th row of S^α = GOR of those rows in $S^\alpha_{(t,t)}$ for which $i \notin F_j$

$$= R^\alpha_{j_1} \vee R^\alpha_{j_2} \vee \cdots \vee R^\alpha_{j_s}.$$

Collecting all the facts described above we now have the following theorem.

Theorem 1 *The matrices $S^0, S^1, \ldots, S^{c-1}$ constructed in the above manner realize a color visual cryptographic scheme on the monotone access structure $(\mathcal{Q}_{min}, \mathcal{F}_{max})$.*

Proof First we prove the security condition (*see Definition* 3). If F is a forbidden set then it is contained in some maximal forbidden set. Since we are considering monotone access structures therefore without loss of generality, let us assume that F itself is a maximal forbidden set. Let $F = F_i$ for some $1 \le i \le t$. We observe that for any color $\alpha \in \{0, 1, \ldots, c-1\}$ the accumulated shares of the participants in F_i lacks the i-th row R^α_i of the basis matrix $S^\alpha_{(t,t)}$. So the security condition now follows from the security condition of $(t, t)_c$-CVCS.

To prove the contrast condition (*see Definition* 3) let us suppose B be a minimal qualified set. Consider the portion of cumulative array $CA[B]$ restricted to the rows indexed by the parties in B. It is easy to see that every column of the restricted array $CA[B]$ contains at least one 1, otherwise if there is a column (*say*, j-th one) in $CA[B]$ such that all the entries are 0 then $B \subseteq F_j$ which is not possible. Therefore the GOR of the shares corresponding to any color α of the parties in B is actually equal to the GOR of *all* the rows of $S^\alpha_{(t,t)}$. Hence the contrast condition follows from the contrast condition of $(t, t)_c$-CVCS. □

Note 1 The $(t, t)_c$-color schemes [10,27,28] existing in the *same color* model have maximal contrast. Thus our color visual secret sharing scheme also achieves maximal contrast in the *same color* model.

Corollary 1 *If the $(t, t)_c$-CVCS has pixel expansion m then the pixel expansion of the CVCS for the general access structure also has pixel expansion m. Moreover, the parameters h, l of the general CVCS are equal to the parameters of the underlying $(t, t)_c$-CVCS.*

Example 2 Let us consider the access structure given in Example 1. Let us consider three colors 0, 1, 2. Since there are *four* maximal forbidden sets, we first consider a $(4, 4)_3$-CVCS.

The basis matrices for $(4, 4)_3$-CVCS are given by [10]:

$$S^0_{(4,4)} = \begin{bmatrix} 011122221001212001020 \\ 011212212000012120102 \\ 012112122120000001122 \\ 021111222121200120000 \end{bmatrix}, S^1_{(4,4)} = \begin{bmatrix} 100022220111111020202 \\ 100202202110202111102 \\ 102002022021102110211 \\ 120000222020211021111 \end{bmatrix},$$

$$S^2_{(4,4)} = \begin{bmatrix} 200011110222222010101 \\ 200101101220101222201 \\ 201001011012201220122 \\ 210000111010122012222 \end{bmatrix}.$$

Thus the basis matrices for the access structure $\mathcal{Q}_{min} = \{1234, 1235, 1236\}$ are given by:

$$S^0 = \begin{bmatrix} 021111222121200120000 \\ 012112122120000001122 \\ 011212212000012120102 \\ 011122221001212001020 \\ 011122221001212001020 \\ 011122221001212001020 \end{bmatrix},$$

$$S^1 = \begin{bmatrix} 120000222020211021111 \\ 102002022021102110211 \\ 100202202110202111102 \\ 100022220111111020202 \\ 100022220111111020202 \\ 100022220111111020202 \end{bmatrix},$$

$$S^2 = \begin{bmatrix} 210000111010122012222 \\ 201001011012201220122 \\ 200101101220101222201 \\ 200011110222222010101 \\ 200011110222222010101 \\ 200011110222222010101 \end{bmatrix}.$$

3.2 Color VCS on $(k, n)^*$-access structure

In the previous section we dealt with general access structure. In this section, we deal with a special kind of access structure, known as $(k, n)^*$-access structure. We put forward a direct construction method for realizing such $(k, n)^*$-color VCS in the *same color* model.
To define the access structure, let $\mathcal{P} = \{1, 2, \ldots, n\}$ be a set of participants. Suppose the party 1 is the leader and the secret image cannot be retrieved in his absence. We call party 1 an *essential* party. However he cannot retrieve the secret image alone. He needs the help of at least $k - 1$ *regular* parties from the rest of $n - 1$ parties in order to reconstruct the secret image. The resulting access structure is called a $(k, n)^*$-access structure which is slightly more general than a threshold access structure but not as general as general access structure. In this section we build color visual cryptographic schemes realizing $(k, n)^*$-access structure. Though we can build it using the generic construction given in Sect. 3.1, we provide a simpler and direct construction method. Our construction is based on the basis matrices of a $(k - 1, n - 1)_c$-CVCS. Moreover we show that this construction technique gives better results than the generic method. We will denote a c-color visual cryptographic scheme on a $(k, n)^*$-access structure by $(k, n)^*_c$-CVCS.

A $(k, n)^*$-access structure can be described by the collection of all minimal qualified sets $\mathcal{Q}^*_{min} = \{B \subseteq \mathcal{P} : 1 \in B \text{ and } |B| = k\}$. It is easy to see that the collection of all maximal *forbidden* sets is $\mathcal{F}^*_{max} = \{F \subseteq \mathcal{P} : F = \{2, \ldots, n\} \text{ or } 1 \in F \text{ and } |F| = k - 1\}$. Let us begin with an example of $(2, 5)^*_4$-CVCS.

Example 3 The collection of minimal qualified sets for the $(2, 5)^*_4$-access structure on $\mathcal{P} = \{1, 2, 3, 4, 5\}$ is given by $\mathcal{Q}^*_{min} = \{12, 13, 14, 15\}$. The following matrices S^0, S^1, S^2, S^3 are basis matrices of a $(2, 5)^*_4$-CVCS.

$$S^0 = \begin{bmatrix} 0231 \\ 0123 \\ 0123 \\ 0123 \\ 0123 \end{bmatrix}, S^1 = \begin{bmatrix} 2131 \\ 0123 \\ 0123 \\ 0123 \\ 0123 \end{bmatrix}, S^2 = \begin{bmatrix} 1321 \\ 0123 \\ 0123 \\ 0123 \\ 0123 \end{bmatrix} \& S^3 = \begin{bmatrix} 2013 \\ 0123 \\ 0123 \\ 0123 \\ 0123 \end{bmatrix}.$$

Clearly $S^0[F]$, $S^1[F]$, $S^2[F]$, $S^3[F]$ are equal upto a column permutation for all forbidden set F. Also $z_b(S^b_X) \geq 1$ and $z_{b'}(S^b_X) = 0$ for all qualified sets X, for all colors $b, b' \in \{0, 1, 2, 3\}$ with $b \neq b'$. In other words, we have a $(2, 5)^*_4$-CVCS with $h = 1, l = 0$.

For $n \geq k \geq 2$ we now propose a construction method for $(k, n)^*_c$-CVCS from a $(k - 1, n - 1)_c$-CVCS.

Let us consider a c color visual secret sharing scheme for the $(k - 1, n - 1)$-threshold access structure on $\mathcal{P}'$ with pixel expansion m. Let $T^0, T^1, \ldots, T^{c-1}$ be the corresponding basis matrices whose sizes are $(n - 1) \times m$ each. Choose c permutations $\sigma_0, \sigma_1, \ldots, \sigma_{c-1}$ such that

1. σ_i is a permutation on the set $\{0, 1, \ldots, c - 1\}$ for all $i = 0, 1, \ldots, c - 1$.
2. For every $0 \leq i \leq c - 1$, $\sigma_i(i) = i$ and $\sigma_i(j) \neq j$ for every $0 \leq j \leq c - 1$ where $i \neq j$.

Let $\boldsymbol{\sigma_b(i)}$ denote an $1 \times m$ row vector each of its entries being equal to $\sigma_b(i)$.

We now define c many $n \times cm$ matrices $S^0, S^1, \ldots, S^{c-1}$ by the following concatenation: $S^b = \left[\begin{array}{c|c|c|c|c|c|c} \boldsymbol{\sigma_b(0)} & \boldsymbol{\sigma_b(1)} & \ldots & \boldsymbol{\sigma_b(b)} & \ldots & \boldsymbol{\sigma_b(c-1)} \\ T^0 & T^1 & \ldots & T^b & \ldots & T^{c-1} \end{array}\right]$, where $0 \leq b \leq c - 1$ and "||" stands for the concatenation of two matrices.

We claim that the matrices $S^0, S^1, \ldots, S^{c-1}$ are the basis matrices for the $(k, n)^*$-access structure with pixel expansion cm. First we give an example to understand the construction.

Example 4 Let us consider a $(3, 4)^*$-access structure on a set of 4 participants $\{1, 2, 3, 4\}$. Thus the minimal qualified sets are $\{123, 124, 134\}$. Suppose we want to construct a $(3, 4)^*_5$-CVCS with 5 colors $\{0, 1, 2, 3, 4\}$. So first we consider the basis matrices of $(2, 3)_5$-CVCS.

$$T^0 = \begin{bmatrix} 01234 \\ 02341 \\ 03412 \end{bmatrix}, T^1 = \begin{bmatrix} 10234 \\ 12340 \\ 13402 \end{bmatrix}, T^2 = \begin{bmatrix} 21034 \\ 20341 \\ 23410 \end{bmatrix}, T^3 = \begin{bmatrix} 31204 \\ 32041 \\ 30412 \end{bmatrix}$$
$$\& T^4 = \begin{bmatrix} 41230 \\ 42301 \\ 43012 \end{bmatrix}.$$

In order to construct the basis matrix S^0 for $(3, 4)^*$-access structure we first choose a permutation σ_0 such that $\sigma_0(0) = 0$ and $\sigma_0(j) \neq j$ for any $j \in \{1, 2, 3, 4\}$. Such a permutation is $\sigma_0(0) = 0$, $\sigma_0(1) = 2$, $\sigma_0(2) = 3$, $\sigma_0(3) = 4$ and $\sigma_0(4) = 1$. So according to the

construction method

$$S^0 = \left[\begin{array}{c|c|c|c|c} 00000 & 22222 & 33333 & 44444 & 11111 \\ 01234 & 10234 & 21034 & 31204 & 41230 \\ 02341 & 12340 & 20341 & 32041 & 42301 \\ 03412 & 13402 & 23410 & 30412 & 43012 \end{array}\right].$$

Similarly the other basis matrices can be constructed as

$$S^1 = \left[\begin{array}{c|c|c|c|c} 22222 & 11111 & 33333 & 44444 & 00000 \\ 01234 & 10234 & 21034 & 31204 & 41230 \\ 02341 & 12340 & 20341 & 32041 & 42301 \\ 03412 & 13402 & 23410 & 30412 & 43012 \end{array}\right],$$

$$S^2 = \left[\begin{array}{c|c|c|c|c} 11111 & 00000 & 22222 & 44444 & 33333 \\ 01234 & 10234 & 21034 & 31204 & 41230 \\ 02341 & 12340 & 20341 & 32041 & 42301 \\ 03412 & 13402 & 23410 & 30412 & 43012 \end{array}\right],$$

$$S^3 = \left[\begin{array}{c|c|c|c|c} 11111 & 00000 & 44444 & 33333 & 22222 \\ 01234 & 10234 & 21034 & 31204 & 41230 \\ 02341 & 12340 & 20341 & 32041 & 42301 \\ 03412 & 13402 & 23410 & 30412 & 43012 \end{array}\right]$$

and

$$S^4 = \left[\begin{array}{c|c|c|c|c} 11111 & 00000 & 33333 & 22222 & 44444 \\ 01234 & 10234 & 21034 & 31204 & 41230 \\ 02341 & 12340 & 20341 & 32041 & 42301 \\ 03412 & 13402 & 23410 & 30412 & 43012 \end{array}\right].$$

We now prove the following.

Theorem 2 *Let us consider* $(\mathcal{Q}, \mathcal{F})$*, a* $(k-1, n-1)$*-threshold access structure on* $\mathcal{P}' = \{2, 3, \ldots, n\}$*. Let* $(\mathcal{Q}^*, \mathcal{F}^*)$ *be the corresponding* $(k, n)^*$*-access structure on* $\mathcal{P} = \{1, 2, \ldots, n\}$*. Given a* $(k-1, n-1)_c$*-CVCS with pixel expansion m, there exists a* $(k, n)_c^*$*-CVCS with pixel expansion cm.*

Proof First we prove the *security condition* i.e. if F is a maximal forbidden set then $S^0[F], S^1[F], \ldots, S^{c-1}[F]$ are equal upto column permutations. In a $(k, n)^*$-access structure there are two types of maximal forbidden sets. In the first type, $1 \in F$ but $|F| = k-1$ i.e. F contains the essential participant but $k-2$ regular parties. In the second type, there is only one maximal forbidden set F namely, the set $\{2, 3, \ldots, n\}$.

If $F = \{2, 3, \ldots, n\}$ then $S^0[F], S^1[F], \ldots, S^{c-1}[F]$ all are equal (up to column permutations) to the concatenation $T^0||T^1||\cdots||T^{c-1}$.

Let F be of the first type. Without loss of generality, let $F = \{1, 2, \ldots, k-1\}$, i.e. F contains the essential party 1 and $k-2$ regular parties. We show that $S^\alpha[F]$ and $S^\beta[F]$ are equal up to column permutations for any two distinct colors $\alpha, \beta \in \{0, 1, \ldots, c-1\}$. From the construction, it is easy to see that for every block $\left[\begin{array}{c} \boldsymbol{\sigma_\alpha(i)} \\ T^i \end{array}\right]$ in S^α there is exactly one block $\left[\begin{array}{c} \boldsymbol{\sigma_\beta(j)} \\ T^j \end{array}\right]$ in S^β such that $\boldsymbol{\sigma_\alpha(i)} = \boldsymbol{\sigma_\beta(j)} = [\lambda, \lambda, \ldots, \lambda]_{1\times m} = \boldsymbol{\lambda}$ for some $0 \le \lambda \le c-1$. Since T^i and T^j are basis matrices of a $(k-1, n-1)_c$-CVCS on $\mathcal{P}' = \{2, 3, \ldots, n\}$ therefore $T^i[\{2, 3, \ldots, k-1\}]$ and $T^j[\{2, 3, \ldots, k-1\}]$ are equal upto column permutation. Thus,

the blocks $\begin{bmatrix} \boldsymbol{\lambda} \\ T^i \end{bmatrix}$ and $\begin{bmatrix} \boldsymbol{\lambda} \\ T^j \end{bmatrix}$ when restricted to $F = \{1, 2, \ldots, k-1\}$ are equal up to column permutation. Varying over all the blocks it follows that $S^{\alpha}[F]$ and $S^{\beta}[F]$ are equal upto column permutations. Hence, the security follows.

In order to prove the *contrast* condition let us consider a minimal qualified set B. Again, without loss of generality, let $B = \{1, 2, \ldots, k\}$. Let us consider any color $b \in \{0, 1, \ldots, c-1\}$. We will show that there exists two non-negative integers l, h with $h > l$ such that:

1. $z_b(S_B^b) \geq h$ and
2. $z_{b'}(S_B^b) \leq l$ for all $b' \neq b$.

That is, while recovering color b, the GOR of the shares corresponding to the participants in B, the number of subpixels corresponding to the true color b must be strictly greater the number of subpixels of any falsely recovered color.

Observe that, there is a block $\begin{bmatrix} \boldsymbol{\sigma_b(b)} \\ T^b \end{bmatrix}$ occurring in S^b. Now $\boldsymbol{\sigma_b(b)} = [b, b, \ldots, b]_{1\times m}$. Hence if the underlying $(k-1, n-1)_c$-CVCS has parameters h', l' then $z_b(S_B^b) \geq h'$. For any other block $\begin{bmatrix} \boldsymbol{\sigma_b(i)} \\ T^i \end{bmatrix}$ since $\sigma_b(i) \neq i$ therefore at most l' many $\sigma_b(i)$ colored subpixels can be recovered. Varying over all i's with $i \neq b$ it is not hard to see $\sigma_b(i)$ varies over all colors not equal to b. We can therefore conclude that $z_{b'}(S_B^b) \leq l'$ for all $b' \neq b$. Hence if we set $h = h'$ and $l = l'$ then we have the contrast condition.
This concludes the proof of the theorem. □

Note 2 We observe that if the underlying $(k-1, n-1)_c$-CVCS has maximal contrast then the construction of $(k, n)_c^*$-CVCS also has maximal contrast.

Corollary 2 *There exists $(2, n)_c^*$-CVCS with pixel expansion c which is independent of the number of participants n. Moreover, the scheme has maximal contrast (see Example 3).*

Corollary 3 *Let m, h, l be the parameters of an optimal $(k-1, n-1)_c$-CVCS. Let m^*, h^*, l^* be the parameters of an optimal $(k, n)_c^*$-CVCS. Then $m^* \leq cm$, $h^* = h$ and $l^* \leq l$.*

4 Comparison and experimental results

We now show that our scheme provides better pixel expansion than the existing schemes. To the best of our knowledge, there is only one paper [28] that gives color visual cryptographic schemes for general access structures. The authors in [28] first considered the basis matrices of visual cryptographic schemes for black & white images and then transformed them into the basis matrices of the color visual cryptographic schemes. For $(t, t)_c$-CVCS their pixel expansion turns out to be $m_{(t,t)}^{YL} = c.2^{t-1}$. For any general access structure $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ with $|\mathcal{F}_{max}| = t$ their construction method gives a pixel expansion of $m_{Gen}^{YL} = c2^{t-1}$. Blundo et al. [10] gave direct constructions for only $(2, t)_c$-CVCS and $(t, t)_c$-CVCS. Their $(t, t)_c$-CVCS has the following pixel expansion:

$$m_{(t,t)_c}^{BBS} = \begin{cases} (c-1)2^{t-1} - c + 2 & \text{for } odd\ t \geq 3 \\ c(c-1)2^{t-2} - c & \text{for } even\ t \geq 4. \end{cases}$$

Our generic construction method (Theorem 1) constructs c-color visual cryptographic schemes for any monotone access structure $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ having $|\mathcal{F}_{max}| = t$ with the help of *any* $(t, t)_c$-CVCS (e.g. [10] or [28]).

Table 1 Pixel Expansions for $(k, n)^*$-access structures with 3 colors

Acc. Str.	m_{Gen}^{YL}	m_{our}^{YL}(Thm1)	m_{our}^{BBS}(Thm1)	m_{our}^{*}(Thm 2)
$(2, 4)^*$	6	6	–	3
$(3, 4)^*$	24	24	21	24
$(2, 5)^*$	6	6	–	3
$(3, 5)^*$	48	48	31	33
$(4, 5)^*$	192	192	127	54
$(2, 6)^*$	6	6	–	3
$(3, 6)^*$	96	96	93	45
$(4, 6)^*$	3.2^{10}	3.2^{10}	$2^{11} - 1$	72
$(5, 6)^*$	3.2^{10}	3.2^{10}	$2^{11} - 1$	135

If we take the underlying $(t, t)_c$-CVCS of [28] then using Theorem 1 we have the pixel expansion of a c-color VCS on $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ as $m_{our}^{YL} = c.2^{t-1}$ which is exactly equal to m_{Gen}^{YL}.

On the other hand, if we use $(t, t)_c$-CVCS of [10] then the pixel expansion becomes

$$m_{our}^{BBS} = \begin{cases} (c-1)2^{t-1} - c + 2 & \text{for } odd\ t \geq 3 \\ c(c-1)2^{t-2} - c & \text{for } even\ t \geq 4. \end{cases}$$

Now for meaningful color visual secret sharing schemes on access structures $t \geq 1$ and $c \geq 3$. It is now easy to see that $m_{our}^{BBS} \leq m_{Gen}^{YL}$ when t is odd. When t is even then we can shift between [10] and [28] for choosing $(t, t)_c$-CVCS to achieve better or equal pixel expansion.

The construction given in Theorem 2 significantly improves the pixel expansion over the generic techniques. In Table 1 we give some comparisons of the pixel expansions for different $(k, n)^*$-access structures across different construction methods when there are 3 colors. The notations m_{Gen}^{YL} denotes the pixel expansion corresponding to *Construction* 2 of [28], m_{our}^{YL} denotes pixel expansion corresponding to Corollary 1 of this paper and *Construction* 1 of [28], m_{our}^{BBS} denotes pixel expansion corresponding to Corollary 1 of this paper and *Theorems* 6.8 & 6.9 of [10]. Lastly, m_{our}^{*} denotes the pixel expansion corresponding to Theorem 2 while using pixel expansions from Table 1 of [28].

Figure 1 shows three shares *Share* 1, *Share* 2, *Share* 3 for a $(2, 3)_3^*$-CVCS using Corollary 2 where the secret image consists of three colors Red, Green and Blue. To maintain the aspect ratio we have introduced an all $\bullet$ column to each of the basis matrices. Superposition of shares corresponding to a minimal qualified sets $\{1, 2\}$ and $\{1, 3\}$ retrieve the secret image. But $\{2, 3\}$ being a forbidden set, superposition of the corresponding shares reveals no information whatsoever.

5 Conclusion

In this work first we have presented information theoretic color visual cryptographic scheme realizing general access structure and our construction achieves maximal contrast. Then we have given a direct construction of color visual cryptographic scheme to realize a very

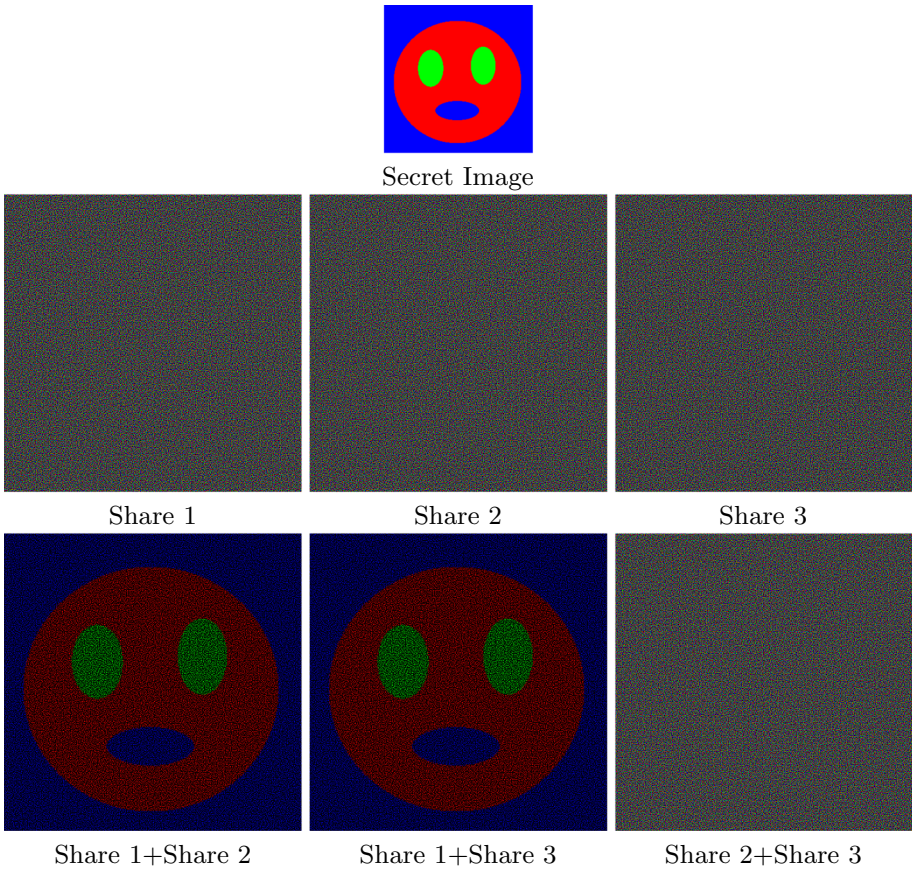

Fig. 1 Implementation of (2, 3)*-CVCS with 3 colors (Color figure online)

important class of access structure known as (k, n)*-access structure. Last, we show that our construction methods outperform the existing methods in terms of pixel expansion.

Acknowledgements The authors are thankful to the anonymous reviewers for their comments and suggestions. The authors are also thankful to Md. Kutubuddin Sardar of Department of Pure Mathematics, University of Calcutta for fruitful discussions and implementations during the preparation of manuscript. Research of Dr. Adhikari is partially supported by National Board for Higher Mathematics, Department of Atomic Energy, Government of India (No 2/48(10)/2013/NBHM(R.P.)/R & D II/695).

References

1. Adhikari A.: Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images. Des. Codes Cryptogr. **73**(3), 865–895 (2014).
2. Adhikari A., Bose M.: A new visual cryptographic scheme using latin squares. In: IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **87**(5), 1198–1202 (2004).
3. Adhikari A., Dutta T.K., Roy B.: A New Black and White Visual Cryptographic Scheme for General Access Structures. In: INDOCRYPT'04. LNCS **3348**, 399–413 (2004).
4. Adhikari A., Sikdar S.: A New $(2, n)$-Visual Threshold Scheme for Color Images. In: INDOCRYPT'03. LNCS **2904**, 148–161 (2003).

5. Adhikari A., Bose M., Kumar D., Roy B.K.: Applications of partially balanced incomplete block designs in developing (2, n) visual cryptographic schemes. In: IEICE Transactions **90–A**(5), 949–951 (2007).
6. Arumugam S., Lakshmanan R., Nagar A.K.: On (k, n)*-visual cryptography scheme. Des. Codes Cryptogr. **71**(1), 153–162 (2014).
7. Ateniese G., Blundo C., De Santis A., Stinson D.R.: Visual cryptography for general access structures. Inf. Comput. **129**, 86–106 (1996).
8. Ateniese G., Blundo C., De Santis A., Stinson D.R.: Constructions and Bounds for Visual Cryptography. In: ICALP'96. LNCS **1099**, 416–428 (1996).
9. Blundo C., D'arco P., De Santis A., Stinson D.R.: Contrast optimal threshold visual cryptography. SIAM J. Discret. Math. **16**(2), 224–261 (2003).
10. Blundo C., De Bonis A., De Santis A.: Improved schemes for visual cryptography. Des. Codes Cryptogr. **24**(3), 255–278 (2001).
11. Cimato S., De Prisco R., De Santis A.: Optimal colored threshold visual cryptography schemes. Des. Codes Cryptogr. **35**(3), 311–335 (2005).
12. Cimato S., De Prisco R., De Santis A.: Colored visual cryptography without color darkening. Theor. Comput. Sci. **374**(1–3), 261–276 (2007).
13. Cimato S., Yang C.N.: Visual Cryptography and Secret Image Sharing. Taylor & Francis, CRC Press, Boca Raton (2011).
14. Dutta S., Rohit R.S., Adhikari A.: Constructions and analysis of some efficient $t-(k,n)^*$-visual cryptographic schemes using linear algebraic techniques. Des. Codes Cryptogr. **80**(1), 165–196 (2016).
15. Dutta S., Adhikari A.: XOR based non-monotone $t-(k,n)^*$-visual cryptographic schemes using linear algebra. ICICS **2014**, 230–242 (2014).
16. Dutta S., Adhikari A.: Contrast optimal XOR based visual cryptographic schemes. ICITS **2017**, 58–72 (2017).
17. Guo T., Liu F., Wu C.K., Ren Y.W., Wang W.: On (k, n) Visual Cryptography Scheme with t Essential Parties. In: ICITS'13. LNCS **8317**, 56–68 (2014).
18. Hou Y.-C.: Visual cryptography for color images. Pattern Recognit. **36**(7), 1619–1629 (2003).
19. Iwamoto M.: A weak security notion for visual secret sharing schemes. IEEE Trans. Inf. Forensics Secur. **7**(2), 372–382 (2012).
20. Jin D., Yan W.-Q., Kankanhalli M.S.: Progressive color visual cryptography. J. Electron. Imaging **14**(3), 033019 (2005).
21. Koga H., Yamamoto H.: Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. In: IEICE Transactions on Fundamentals of Electronics, Communications & Computer Sciences **E81–A**(6), 1262–1269 (1998).
22. Liu F., Wu C.K., Lin X.J.: Colour visual cryptography schemes. IET Inf. Secur. **2**(4), 151–165 (2008).
23. Naor M., Shamir A.: Visual Cryptography. In: EUROCRYPT'94. LNCS **950**, 1–12 (1994).
24. Rijmen, V., Preneel, B.: Efficient colour visual encryption or shared colors of benetton. EUROCRYPT'96 Rump Section. http://www.iacr.org/conference/ec96/rump/preneel.ps.gz
25. Praveen K., Rajeev K., Sethumadhavan M.: On the Extensions of $(k,n)^*$-Visual Cryptographic Schemes. In: SNDS'14, CCIS **420**, 231–238 (2014).
26. Shyu S.J.: Efficient visual secret sharing scheme for color images. Pattern Recognit. **39**(5), 866–880 (2006).
27. Verheul E.R., Tilborg H.C.A.: Constructions and properties of k out of n visual secret sharing schemes. Des. Codes Cryptogr. **11**(2), 179–196 (1997).
28. Yang C.-N., Laih C.-S.: New colored visual secret sharing schemes. Des. Codes Cryptogr. **20**(3), 325–336 (2000).