Color Visual Cryptography Schemes Using Linear Algebraic Techniques over Rings

Sabyasachi Dutta[1(✉)], Md Kutubuddin Sardar[2], Avishek Adhikari[3], Sushmita Ruj[4], and Kouichi Sakurai[5]

[1] University of Calgary, Calgary, Canada
saby.math@gmail.com
[2] University of Calcutta, Kolkata, India
kutubpmath@gmail.com
[3] Presidency University, Kolkata, India
avishek.adh@gmail.com
[4] CSIRO, Data61, Sydney, Australia
sushmita.ruj@gmail.com, sushmita.ruj@csiro.au
[5] Kyushu University, Fukuoka, Japan
sakurai@inf.kyushu-u.ac.jp

Abstract. The research on color Visual Cryptographic Scheme (VCS) is much more difficult than that of the black and white VCS. This is essentially because of the fact that in color VCS, the rule for superimposition of two colors is not that simple as in black and white VCS. It was a long standing open issue whether linear algebraic technique in constructing Black and White visual cryptographic schemes could also be extended for color images. It was thought that such an extension was impossible. However, we resolve this issue by providing color VCS in same color model for the threshold access structures by extending linear algebraic techniques from the binary field $\mathbb{Z}_2$ to finite ring $\mathbb{Z}_c$ of integers modulo c. We first give a construction method based on linear algebra to share a color image for an (n, n)-threshold access structure. Then we give constructions for $(2, n)$-threshold access structures and in general (k, n)-threshold access structures. Existing methodology for constructing color VCS in same color model assumes the existence of black and white VCS, whereas our construction is a direct one. Moreover, we give closed form formulas for pixel expansion which is combinatorially a difficult task. Lastly, we give experimental results and propose a method to reduce pixel expansion.

S. Dutta—is grateful to the NICT, Japan for financial support under the NICT International Exchange Program during 2018-19 when the preliminary draft was prepared. Md K. Sardar—is thankful to the CSIR, Govt. of India for providing financial support (Award no. 09/028(0975)/2016-EMR-1).
A. Adhikari—Research of A. Adhikari is partially supported by DST-SERB Project MATRICS vide Sanction Order: MTR/2019/001573.

S. Kanhere et al. (Eds.): ICISS 2020, LNCS 12553, pp. 198–217, 2020.
https://doi.org/10.1007/978-3-030-65610-2_13

Keywords: Color visual secret sharing · Linear algebra · Pixel expansion · Relative contrast

1 Introduction

In a visual cryptographic scheme (VCS), on a set of n participants, a dealer who possesses a secret image encodes it into n shares and distributes these shares among n participants. Physically, each of the participants obtain a transparency on which his or her share is photocopied. Only a pre-specified collection of subsets of participants can visually recover the secret image. However, no subset of participants which are outside the above mentioned collection can recover the secret image – in fact, a stronger security condition is achieved viz. such subsets of participants obtain no information about the secret image. Eligible subsets are called "qualified" sets and ineligible subsets are termed as "forbidden" sets.

Main motivation to study visual cryptographic scheme is its simple recovery process. No participation of computing device is needed, the decoding process is done by the human visual system. Visual secret sharing has found its applications into several interesting areas - watermarking [15], application to QR-codes [11] etc. to name a few.

1.1 Related Works

Naor and Shamir [26] proposed the first visual cryptographic scheme and the concept has been further explored in [1,2,6,7,9,10] and extended to general access structures. Some recent works gave efficient constructions for few important and interesting access structures [5,16,17,20,28]. The work of Adhikari et al. [2] introduced an elegant linear algebraic technique to construct basis matrices for a black and white image - one only needs to solve systems of linear equations over the binary field $\mathbb{Z}_2$. The power of the technique was researched and resulted in a number of works - both in OR model [1,16,29,31] and XOR model [17,30] for B/W visual cryptography.

Verheul-Tilborg [33] for the first time, conceptualized color visual cryptography as an extension of the existing B/W visual cryptography model. They provided the model of color visual cryptographic scheme and constructed a color (n, n)-visual cryptographic scheme. Constructing color visual secret sharing depends on the underlying color-superposition principle. In B/W visual cryptography, color superposition principle is easy – two white pixels (when superposed) results in white pixel but if at least one of the two is a black pixel, the result is a black pixel. The situation gets complicated in case of color images – two different colors (when superposed) may result in a completely different third color. There are three major color models [14] conceptualized in the literature – *same color* (SC) model, *no darkening* (ND) model and *general* model. In the SC model, superposition of two different colored pixels is not allowed. However, there is an exception for the annihilator/masking "•" color which is different from the set of ingredient colors. In SC model, superposing two same colored pixels results in

a pixel with same color while superposing a colored pixel with "•" results in "•". However in this model the fact of darkening of reconstructed pixel is ignored – when two same colored pixels are superposed then in reality a darker version of that color is obtained. The premise is rather simplistic – superposition of two i colored pixels gives back one i colored pixel. The no-darkening model is similar to the same color model but in this case the problem of darkening is considered – when more than two same colored pixels are superimposed then the resulting pixel is a darker version of the color and therefore, to obtain "non-darkened" reconstructed pixel a colored pixel can only superpose with a white (transparent) pixel. The general model of color-superposition puts no restrictions on superposition principle - the color superposition satisfies real world color superposition principles.

Cimato et al. [13] considered no-darkening model and put forward construction of (k, n)-threshold color visual cryptographic scheme with the help of basis matrices of a $(k-1, k-1)$-threshold B/W visual cryptographic scheme. The resulting c-color VCS has a pixel expansion of $c\binom{n}{k}2^{k-2}$ and achieves "maximal contrast". The term maximal contrast loosely means that while recovering a secret pixel of some color i, no other false colored pixel j is reconstructed (see Definition 3). The authors [13] also provided c-color $(2, n)$-VCS with pixel expansion $c(n-1)$. Rijmen et al. [27] was the first to consider the general model of color superposition along with some of the follow up works [3,24]. Generic constructions of $(2, n)$-threshold color visual secret sharing schemes from B/W cryptographic schemes can be obtained using the techniques from [3,24]. A number of works [10,12,33,35] exist in the same color model. The main trick is in the encoding of color pixels – it is done in such a manner that during the implementing "superposition", same color model is satisfied. Verheul et al. [33] constructed c color (n, n)-threshold scheme, $(k, c-1)$-threshold scheme and (k, c)-scheme with the restriction that c is a prime power. For any value of c, Blundo et al. [10] gave constructions of c color $(2, n)$-schemes and (n, n)-schemes. Koga et al. [24] and Yang et al. [35] provided color visual cryptographic schemes for (k, n)-threshold access structures. Color VCS realizing general access structures was proposed in the work of Yang et al. [35]. Recently, Dutta et al. [19] gave a generic construction of color VCS realizing general access structure and an efficient scheme to realize $(k, n)^*$-access structure in the same-color model. Several other color visual cryptographic schemes with extra features have been proposed [21,23,25,32]. Iwamoto [22] introduced a "weaker notion of security" and used techniques of integer linear programming to obtain color VCS. For more literature one can refer to [14].

1.2 Our Contribution

Constructing visual cryptographic schemes using linear algebraic technique has long been proposed in the literature for B&W images [1,2]. It was a long standing open issue whether similar technique can be extended for color images. It was thought that such an extension was impossible. We resolve this issue by

providing color VCS for the threshold access structures by extending simple linear algebraic techniques from the binary field $\mathbb{Z}_2$ to finite ring $\mathbb{Z}_c$ of integers modulo c. In this work we consider the same-color model of color VCS. To the best our knowledge, all the generic constructions (except [19]) proposed so far to construct basis matrices for color VCS (in the same-color model) inherently assume the constructions of basis matrices for B&W images. More concretely, construction of basis matrices for color VCS used the basis matrices for B&W images realizing the same access structure. Novelty of our construction is that our methodology does not assume such existence of basis matrices for B&W images. Using our simple linear algebra based technique, one can build color VCS directly. This separates our work from [19] who assumed existence of a class of "basis matrices" to achieve their schemes. Furthermore, we give closed form formulas for pixel expansion which is combinatorially a difficult task. Lastly, we give experimental results and propose a method to reduce pixel expansion.

2 Prerequisites

We describe some basic definitions, fix color-superposition model and state some mathematical results on finite rings that are required for the paper.

2.1 The Color Model

We follow Verheul-Tilborg [33] 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 color superposition principle is described in 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 $\{0, 1, \ldots, c-1\}$, $z_i(V)$ denotes the number of coordinates in V equal to i where $i = 0, 1, \ldots, c-1$. For example, if $V = (0, 1, 0, 2, 2)$ with entries from the set $\{0, 1, 2\}$, then $z_0(V) = 2$, $z_1(V) = 1$ and $z_2(V) = 2$.

2.2 Color Visual Cryptographic Scheme

In a (k, n) threshold access structure subsets of size k or more are called "qualified" set and rest are "forbidden" sets which are subsets of size $k-1$ or less. We now define *unconditionally secure* c color (k, n)-threshold visual cryptographic

scheme and denote such a scheme by $(k,n)_c$-CVCS where c denotes the number of *true* colors. We require two conditions to be satisfied viz. the "contrast" condition and the "security" condition. The first condition guarantees that secret image is reconstructed by any set of k (or more) participants whereas the second is to ensure that no subset of size less than k can get any information about the image.

For defining $(k,n)_c$-CVCS in concrete terms, we require c *basis* matrices $S^0, S^1, \ldots, S^{c-1}$ where S^b corresponds to the color $b \in \{0,1,\ldots,c-1\}$. The entries of these matrices belong to the set of colors $\{0,1,\ldots,c-1\}$. To share a secret pixel $b \in \{0,1,\ldots,c-1\}$, the dealer in the *share generation* phase, chooses the matrix S^b and then applies a random column permutation on the matrix S^b. Share of participant P_i the i-th row of the resulting permuted matrix. To share a c-colored image, dealer repeatedly performs the above process (for every secret pixel) till all the pixels are shared. The formal definition is as follows.

Definition 1. *(adopted from [10,35]) 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 sequences of non-negative numbers $\{h_X\}$ and,$\{l_X\}$ with $l_X < h_X$ 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 $z_b(S^b_X) \geq h_X$; whereas, for $b' \neq b$ it results in $z_{b'}(S^b_X) \leq l_X$.*
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 $S^0[Y]$, $S^1[Y]$, ... , $S^{c-1}[Y]$ obtained by restricting S^0, S^1, ..., 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 suitably modified for any arbitrary access structure on a set of participants. Although in this paper we do not deal with general access structure, we discuss for sake of completeness. 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 $\mathcal{F}$. Basis matrices realizing a general access structure $(\mathcal{Q},\mathcal{F})$ with c many colors are defined as follows.

Definition 2. *(adapted from [35]) 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 $S^0[Y]$, $S^1[Y]$, ... , $S^{c-1}[Y]$ obtained by restricting S^0, S^1, ..., S^{c-1} respectively to rows indexed by the participants of Y, are identical up to column permutations.*

The *contrast* of reconstructed image in a color VCS [10,33] is defined as $\alpha = \frac{h-l}{h+l}$. The *loss in contrast* is measured by the quantity $\frac{h-l}{m(h+l)}$. On the other hand, [12] define the contrast to be the value $\frac{h-l}{m}$ keeping parity with the well-known definition of contrast given in [26]. A scheme is said to achieve *maximal contrast* if $l = 0$ [10]. In other words, maximal contrast guarantees that while reconstructing a secret pixel of color $i \in \{0, 1, \ldots, c-1\}$ no pixel of color $j(\neq i)$ is recovered. The formal definition is as follows.

Definition 3. *(adopted from [10]) With same notations described in Definition 2, the contrast is defined as* $\alpha = \frac{h-l}{h+l}$ *for a color visual cryptographic scheme. Furthermore, it is of maximal contrast if* $l = 0$.

2.3 Some Mathematical Results

We state some mathematical definitions and results [4] that will be needed through out this paper.

a. For any positive integer c, $(\mathbb{Z}_c, +, .)$ forms a finite *commutative ring* with *unity*. The addition "$+$" is addition modulo c and the multiplication "$.$" is multiplication modulo c. The elements of the set $\mathbb{Z}_c$ are denoted by $0, 1, \ldots, c-1$.
b. A *non-zero* element $x \in \mathbb{Z}_c$ is called a *zero-divisor* if there exists a *non-zero* element $y \in \mathbb{Z}_c$ such that $x.y = 0$. A *non-zero* element $x \in \mathbb{Z}_c$ is called a *unit* if there exists a *non-zero* element $y \in \mathbb{Z}_c$ such that $x.y = 1$. For example, $4 \in \mathbb{Z}_6$ is a zero-divisor as $4.3 = 0$ and $5 \in \mathbb{Z}_6$ is a unit as $5.5 = 1$.
c. Any non-zero element in $\mathbb{Z}_c$ is either a unit or a zero-divisor.
d. An element $x \in \mathbb{Z}_c$ is a unit if and only if $gcd(x, c) = 1$.
e. Every non-zero element $x \in \mathbb{Z}_c$ is a unit if and only if c is a prime. So when c is prime $\mathbb{Z}_c$ is said to form a *field* i.e. a commutative ring with unity where every non-zero element is unit.
f. Let $A\boldsymbol{x} = \boldsymbol{b}$ be a system of linear equations in n many unknowns $x_1, x_2, \ldots, x_n$ where the entries of the matrix A come from the ring $\mathbb{Z}_c$ and let $\boldsymbol{\alpha_0} = [\alpha_1, \alpha_2, \ldots, \alpha_n]^t$ be a particular solution to the above system. If $\boldsymbol{\beta} = [\beta_1, \beta_2, \ldots, \beta_n]^t$ be any solution to the homogeneous system $A\boldsymbol{x} = \boldsymbol{0}$ then $\boldsymbol{\alpha_0} + \boldsymbol{\beta}$ is a solution to $A\boldsymbol{x} = \boldsymbol{b}$.
g. For any prime power p^n there exists a field of size p^n.

3 Main Results

We propose a linear algebraic construction for obtaining basis matrices $S^0, \ldots, S^{c-1}$ for a $(k, n)_c$-CVCS, where $2 \leq k \leq n$. The methodology though simple, requires several involved results from algebra to prove correctness and security of such sharing scheme. First we give details of the underlying technique.

3.1 Constructing Color VCS from Smaller Schemes

In this section we present a construction for color visual cryptographic schemes using smaller schemes as building blocks. At this point we mention that we are considering the *same-color* model of color superposition to avoid any confusion. Let us consider a color image with c colors labeled by $0, 1, \ldots, c-1$.

Let (Q', F') and (Q'', F'') be two access structures defined on two sets $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively having cardinality n_1 and n_2 respectively, where the symbols have their usual meanings. Suppose there exist a (Q', F') color VCS with pixel expansion m' and a (Q'', F'') color VCS with pixel expansion m''. Also suppose $(R^0, R^1, \ldots, R^{c-1})$ denote the basis matrices for the first scheme and $(T^0, T^1, \ldots, T^{c-1})$ denote the same for the second scheme. We now describe how to construct a color-VCS for the access structure $(Q, F) = (Q' \cup Q'', F' \cap F'')$ on the set of participants $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_1$ containig n elements. Let us write $\mathcal{P} = \{1, 2, \ldots, n\}$.

From the given matrices we construct basis matrices $(S^0, S^1, \ldots, S^{c-1})$ realizing (Q, F) in Algorithm 1.

Algorithm 1 Construction of basis matrices from smaller schemes

procedure PREPARATION OF INTERMEDIATE MATRICES
for $\alpha = 0, \ldots, c-1$
    for $i = 1, \ldots, n$
        if the ith participant is not present in (Q', F')
            ith row of matrix $\hat{R}^\alpha$ = all $\bullet$ entries
        else it is the row corresponding to the ith party in R^α,

for $\alpha = 0, \ldots, c-1$
    for $i = 1, \ldots, n$
        if the ith participant is not present in (Q'', F'')
            ith row of matrix $\hat{T}^\alpha$ = all $\bullet$ entries
        else it is the row corresponding to the ith party in T^α,

procedure CONSTRUCTION OF BASIS MATRICES
for color $\alpha = 0, 1, \ldots, c-1$,
    construct the matrices $S^\alpha = \hat{R}^\alpha || \hat{T}^\alpha$, where $||$ denotes "concatenation" of matrices.

We now have the following theorem (a parallel version of it is proved for B & W image in Theorem 4.4 of [6]).

Theorem 1. *Let (Q', F') and (Q'', F'') be two access structures defined on two sets $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively having cardinality n_1 and n_2 respectively. Suppose there exist a (Q', F', m') color VCS and a (Q'', F'', m'') color VCS with basis matrices $(R^0, R^1, \ldots, R^{c-1})$ and $(T^0, T^1, \ldots, T^{c-1})$ respectively. Then Algorithm 1 yields a $(Q' \cup Q'', F' \cap F'', m' + m'')$ color VCS on the set of participants $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$.*

The above theorem can be extended to multiple access structures.

Corollary 1. *Let (Q, F) be an access structure such that $Q = Q_1 \cup \ldots \cup Q_r$ and $F = F_1 \cap \ldots \cap F_r$. If there exists (Q_i, F_i, m_i) color VCS for all $i = 1, \ldots, r$ then using Algorithm 1 repeatedly we get hold of a (Q, F, m) color VCS with $m = m_1 + \cdots + m_r$.*

On the basis of Corollary 1 we build our linear algebraic scheme for constructing basis matrices. We first give a high level idea of the entire methodology which consists of three main steps.

1. First, we partition the collection $\mathcal{Q}_{min}$ of *all minimal* qualified sets into groups $G_1, G_2, \ldots, G_t$ such that every group contains precisely two minimal qualified sets ($|G_i| = 2$ for all i), any two groups are disjoint ($G_i \cap G_j = \emptyset$ for $i \neq j$), union of the groups gives back the collection $\mathcal{Q}_{min}$ (i.e. $\cup G_i = \mathcal{Q}_{min}$). Moreover we want this grouping is done in such a way that two minimal qualified sets belonging in the same group have maximum intersection. This step corresponds to the decomposition of the given access structure into smaller access structures as stated in Corollary 1.
2. We associate a variable x_i to participant P_i for every i and formulate system of two linear equations for each group G_j. Thus we will have exactly those many systems of linear equations as the number of groups. For a system we will write all possible n-tuples of solutions of the variables as columns to construct a matrix. Here we emphasize that if a variable x_t is absent in a system we will set $x_t = \bullet$. In this scenario notice that every entry of the t-th row of the above-mentioned matrix is $\bullet$. We do this for every system of linear equations. This step merges the procedure of constructing basis matrices of smaller schemes (whose existence were assumed) in Corollary 1 and the procedure of "preparation of intermediate matrices" in Algorithm 1.
3. In the third step, we concatenate these matrices to get the basis matrices. This step corresponds to the procedure of "construction of basis matrices" of Algorithm 1.

3.2 Construction of $(n, n)_c$-CVCS

Let us assume for the time being that n and c are relatively prime i.e. $gcd(n, c) = 1$. Consider an (n, n)-threshold structure on the set of n many parties. There is only one qualified set namely, the set of participants $\mathcal{P}$ itself. Therefore there is only one group. Let us associate the variable x_i to the i-th participant, where $i = 1, 2, \ldots, n$.

Consider the linear equation over the ring $\mathbb{Z}_c$

$$x_1 + x_2 + \cdots + x_n = a \Big\}$$

where $a \in \mathbb{Z}_c$ and $+$ denotes the operation *addition modulo c*.
First we notice that we have a unique $r \in \mathbb{Z}_c$ such that $x_1 = x_2 = \cdots = x_n = r$ satisfying the above equation. This follows from the fact that $nr = a$ has a

unique solution $r = n^{-1}a$ since $(n, r) = 1$ implies n has a multiplicative inverse. It is easy to see that in the equation if we fix the values of any $n-1$ many variables then the value of the n-th one is automatically fixed. Thus there are c^{n-1} many solutions to the equation. If we write all the solutions as columns to form an $n \times c^{n-1}$ matrix then it has the following properties:

- exactly one column has all entries equal to $r \in \mathbb{Z}_c$,
- rest $c^{n-1} - 1$ columns contain at least two distinct entries from $\mathbb{Z}_c$.

Since the rows of this matrix are the shares of the n parties therefore superposition of all of them will yield the color r. Moreover any submatrix of size $(n-i) \times c^{n-1}$ contains all possible c^{n-i} columns each occurring exactly c^{i-1} times and thus revealing no information about r. Varying a over $\mathbb{Z}_c$ we get all the basis matrices $S^0, S^1, \ldots, S^{c-1}$ to realize an $(n, n)_c$-CVCS.

Theorem 2. *Suppose c and n are relatively prime. Then there exists an $(n, n)_c$-CVCS with pixel expansion c^{n-1} and $h = 1,\ l = 0$.*

Note 1. We note that the construction gives a maximal contrast (*see* Definition 3) color visual cryptographic scheme.

Example 1. Let us construct a $(2, 2)_5$-CVCS on the set of parties $\mathcal{P} = \{1, 2\}$. The five colors are identified as the elements of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Only minimal qualified set is $\{1, 2\}$. Following five matrices realize $(2, 2)_5$-CVCS.
$S^0 = \begin{bmatrix} 0\,1\,2\,3\,4 \\ 0\,4\,3\,2\,1 \end{bmatrix}$, $S^1 = \begin{bmatrix} 0\,1\,2\,3\,4 \\ 2\,1\,0\,4\,3 \end{bmatrix}$, $S^2 = \begin{bmatrix} 0\,1\,2\,3\,4 \\ 4\,3\,2\,1\,0 \end{bmatrix}$, $S^3 = \begin{bmatrix} 0\,1\,2\,3\,4 \\ 1\,0\,4\,3\,2 \end{bmatrix}$, $S^4 = \begin{bmatrix} 0\,1\,2\,3\,4 \\ 3\,2\,1\,3\,4 \end{bmatrix}$ which are obtained by solving (over $\mathbb{Z}_5$) the equations $x_1 + x_2 = 0$, $x_1 + x_2 = 2$, $x_1 + x_2 = 4$, $x_1 + x_2 = 1$, $x_1 + x_2 = 3$ respectively.

Remark 1. We emphasize that the fact $gcd(c, n) = 1$ is of immense importance. In the proof we have used that n has a multiplicative inverse in $\mathbb{Z}_c$. When $gcd(c, n) \neq 1$ then our method fails. Suppose we want to construct a $(2, 2)$-CVCS with 4 colors identified as the four elements $\{0, 1, 2, 3\}$ of $\mathbb{Z}_4$. Solving $x_1 + x_2 = 0$ we get $\begin{bmatrix} 0\,1\,2\,3 \\ 0\,3\,2\,1 \end{bmatrix}$ which does not satisfy the contrast condition of Definition 1 because of $[0, 0]^t$ and $[2, 2]^t$ appearing once each. We will discuss a method to fix the problem of non-coprime in Sect. 3.5.

3.3 Construction of $(2, n)_c$-CVCS

Let us now consider the case of $(2, n)$-threshold access structure and we have a secret image with c colors. The colors are identified as the elements of $\mathbb{Z}_c = \{0, 1, \ldots, c-1\}$. We give a detailed analysis of the construction method and proofs. This technique can essentially be generalized further to construct $(k, n)_c$-CVCS. We again make the following

Assumption: The numbers c and n are relatively prime, i.e. $gcd(2, c) = 1$.
We will show why this assumption is necessary for our construction.

Let $\mathcal{P} = \{1, 2, \ldots, n\}$ be the set of participants. Thus $\mathcal{Q}_{min} = \{Q \subset \mathcal{P} : |Q| = 2\}$ which implies $|\mathcal{Q}_{min}| = \binom{n}{2} = \frac{n(n-1)}{2}$. We will denote $\frac{n(n-1)}{2}$ by r. We arrange the elements of $\mathcal{Q}_{min}$ in the **lexicographic** order, say $B_1, B_2, \ldots, B_r$. We will collect these subsets to form groups $\{G\}_i$, such that when r is even

- each group G_i contains exactly two sets B_u, B_w with $|B_u \cap B_w| = 1$
- there are $\frac{r}{2}$ many groups

and when r is odd

- each group G_i for $i = 1, 2, \ldots, \frac{r-1}{2}$ contains exactly two sets B_u, B_w with $|B_u \cap B_w| = 1$
- the last group $G_{\frac{r+1}{2}}$ contains a single set B_r.

Let us attach variable x_i to participant i for $i = 1, 2, \ldots, n$. Let $f_{B_j} = \alpha$ denote the linear equation $\Sigma_{k \in B_j} x_k = \alpha$ over $\mathbb{Z}_c$ where $\alpha \in \mathbb{Z}_c$.
For each group $G_i = \{B_u, B_w\}$ consider the following systems of linear equations over $\mathbb{Z}_c$:

$$\left.\begin{matrix} f_{B_u} = 0 \\ f_{B_w} = 0 \end{matrix}\right\} \text{–i(0)} \quad , \quad \left.\begin{matrix} f_{B_u} = 1 \\ f_{B_w} = 1 \end{matrix}\right\} \text{–i(1)} \quad ,\ldots\ldots\ldots, \quad \left.\begin{matrix} f_{B_u} = c-1 \\ f_{B_w} = c-1 \end{matrix}\right\} \text{–i(c-1).}$$

When G_i is singleton $\{B_r\}$ then consider

$$f_{B_r} = 0 \,\} \text{–i(0)} \quad , \quad f_{B_r} = 1 \,\} \text{–i(1)} \quad ,\ldots\ldots\ldots, \quad f_{B_r} = c-1 \,\} \text{–i(c-1).}$$

We solve (for x_i s) these systems and if some variable(s) is(are) absent then we set the value of the variable to be $\bullet$.

Let $M_1^0, M_2^0, \ldots, M_{\lceil \frac{r}{2} \rceil}^0$ be the matrices whose columns are respectively the solutions of equations $1(0), 2(0), \ldots, \lceil \frac{r}{2} \rceil(0)$. Construct $S^0 = M_1^0 || M_2^0 || \ldots || M_{\lceil \frac{r}{2} \rceil}^0$, where $||$ denotes concatenation of the matrices. In general, we solve systems $1(\alpha), 2(\alpha), \ldots, \lceil \frac{r}{2} \rceil(\alpha)$ to get $M_1^{\lceil \frac{c}{2} \rceil \alpha}, M_2^{\lceil \frac{c}{2} \rceil \alpha}, \ldots, M_{\lceil \frac{r}{2} \rceil}^{\lceil \frac{c}{2} \rceil \alpha}$ and then concatenate them to obtain $S^{\lceil \frac{c}{2} \rceil \alpha}$ for every color $\alpha = 0, 1, \ldots, c-1$. We claim that these matrices $S^0, S^1, \ldots, S^{c-1}$ are basis matrices realizing the $(2, n)_c$-CVCS. Proof of the claim is given in Theorem 3. Before that we give a concrete example.

Example 2. Let $\mathcal{P} = \{1, 2, 3\}$ and we have three colors $0, 1, 2$. Thus, $\mathcal{Q}_{min} = \{12, 13, 23\}$, where 12 means the set $\{1, 2\}$ etc. We will sometimes denote a set in this form for brevity, when there is no scope for confusion. We form two groups $G_1 = \{12, 13\}$ and $G_2 = \{23\}$. Consider the following systems of equations over $\mathbb{Z}_3$:

$$\left.\begin{matrix} x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \end{matrix}\right\} \text{–1(0)} \quad , \quad \left.\begin{matrix} x_1 + x_2 = 1 \\ x_1 + x_3 = 1 \end{matrix}\right\} \text{-1(1)} \quad \text{and} \quad \left.\begin{matrix} x_1 + x_2 = 2 \\ x_1 + x_3 = 2 \end{matrix}\right\} \text{–1(2).}$$

and

$$x_2 + x_3 = 0 \,\}\text{–}2(0) \quad , \; x_2 + x_3 = 1 \,\}\text{–}2(1) \quad \text{and} \quad x_2 + x_3 = 2 \,\}\text{–}2(2).$$

Solving 1(0) and 2(0) we get, $S^0 = \begin{bmatrix} 012 & \bullet & \bullet & \bullet \\ 021 & 012 & & \\ 021 & 021 & & \end{bmatrix}$. Notice that the •s are present due to the absence of x_1 in Equation 2(0).

Solving 1(1) and 2(1) we get, $S^2 = \begin{bmatrix} 012 & \bullet & \bullet & \bullet \\ 102 & 012 & & \\ 102 & 102 & & \end{bmatrix}$.

Lastly, solving 1(2) and 2(2) we get, $S^1 = \begin{bmatrix} 012 & \bullet & \bullet & \bullet \\ 210 & 012 & & \\ 210 & 210 & & \end{bmatrix}$.

Theorem 3. *Let the numbers 2 and c are relatively prime, where c denote the number of colors. The matrices $S^0, S^1, \ldots, S^{c-1}$ constructed above are basis matrices realizing a $(2, n)_c$-CVCS. Moreover, the construction has pixel expansion $\lceil \frac{n(n-1)}{4} \rceil c$.*

Proof. First we prove the *security condition* in Definition 1. Let us take a forbidden set $X = \{i\}$ consisting of one single participant $\{i\}$. If we are able to prove that $M_k^0[i]$ and $M_k^j[i]$ are equal upto a column permutation for any $j = 0, 1, \ldots, c-1$ and for any $k = 1, 2, \ldots, \lceil \frac{r}{2} \rceil$ where $r = \binom{n}{2}$ then it is not hard to see the $S^0[i]$ and $S^j[i]$ are equal upto a column permutation. From this the proof will follow. We recall that the kth blocks are obtained by solving the simultaneous linear equations corresponding to the kth group $G_k = \{B, C\}$, say. Note that if i is not present in group G_k then $M_k^0[i] = [\bullet \bullet \ldots \bullet]_{1 \times c} = M_k^j[i]$ and hence they are equal.

If i is present in $G_k = \{B, C\}$ then $i \in B - C$ or $i \in C - B$ or belongs to both.

Suppose $i \in B - C$, then there exists a party μ such that $\mu \in B \cap C$ (our algorithm ensures that there is always such a party) and another party $\beta \in C - B$. Thus $B = \{i, \mu\}$ and $C = \{\mu, \beta\}$.

Let the equations we solved to obtain M_k^0 and M_k^j be respectively

$$\left.\begin{matrix} x_i + x_\mu = 0 \\ x_\beta + x_\mu = 0 \end{matrix}\right\} \text{–k(0)} \quad \text{and} \quad \left.\begin{matrix} x_i + x_\mu = a \\ x_\beta + x_\mu = a \end{matrix}\right\} \text{–k(a).}$$

where $2j = a (mod\ c)$. A particular solution to the system $k(a)$ is given by $x_i = 0 = x_\beta$ and $x_\mu = a$ and every solution to this system is obtained by adding this particular solution to every solution of $k(0)$. That is, there is a particular solution which assigns 0 to the variable x_i and that is all we need. Now it is easy to see that $M_k^0[i]$ and $M_k^j[i]$ are equal upto a column permutation. The case when $i \in C - B$ is handled similarly.

Lastly, when $i \in B \cap C$, it is easy to see that there exist parties $\alpha \in B$ and $\gamma \in C$ so that $B = \{i, \alpha\}$ and $C = \{i, \gamma\}$. Then, $x_\alpha = a = x_\gamma$ and $x_i = 0$ is

a particular solution to $k(a)$. Again we can conclude that $M_k^0[i]$ and $M_k^j[i]$ are equal upto a column permutation.

Therefore, in any case we see that $M_k^0[i]$ and $M_k^j[i]$ are equal upto a column permutation for any $j = 0, 1, \ldots, c-1$ and for all $k = 1, 2, \ldots, \lceil \frac{r}{2} \rceil$. This implies that the matrices $S^0[i]$ and $S^j[i]$ are equal upto a column permutation. The proof now follows.

To prove the *contrast condition* let us first choose a minimal qualified set $B = \{i_1, i_2\}$. Let j be any color from the set of colors $\{0, 1, \ldots, c-1\}$. Also let the corresponding matrix S^j is obtained by solving the systems in which the right hand side is equal to the constant a. Thus we know $2j = a(mod\ c)$. Now since B is a minimal qualified set therefore it belongs to a group G_k (possibly) together with another minimal qualified set. Thus the equation $x_{i_1} + x_{i_2} = a$ appears in the system $k(a)$ and solving this system we obtain M_k^j. Note that $x_{i_1} = j = x_{i_2}$ is a solution to this system.

Let us restrict our view to $M_k^j[B]$ which is the restriction of M_k^j to the rows indexed by B. We observe that the column vector $[j\ j]^t$ occurs exactly once in this restricted matrix and no other $[l\ l]^t$ type column occurs in $M_k^j[B]$. The reason for this is the equation $2x = a$ has a unique solution in $\mathbb{Z}_c$ as 2 being relatively prime to c, has a unique multiplicative inverse in $\mathbb{Z}_c$. Moreover the unique solution is j. Thus the G-OR of the rows i_1, i_2, when restricted to the block M_k^j gives *one* j and the rest are equal to $\bullet$.

On the other hand, it is possible that i_1 and i_2 occur in another group say, $G_t = \{\{i_1, \mu\}, \{i_2, \mu\}\}$. We obtain the block M_t^j by solving the system

$$\left.\begin{array}{l} x_{i_1} + x_\mu = a \\ x_{i_1} + x_\mu = a \end{array}\right\} \text{------t(a)} \quad .$$

We notice that in the above system if we fix any value from $\{0, 1, \ldots, c-1\}$ for x_μ then the values of x_{i_1} and x_{i_2} are equal. Thus, we have $M_t^j[B] = \begin{bmatrix} 0\ 1\ \ldots\ c-1 \\ 0\ 1\ \ldots\ c-1 \end{bmatrix}$ which shows that the G-OR of the rows i_1, i_2, when restricted to the block M_t^j gives every color α exactly once.

Lastly, if at least one of i_1 and i_2 is absent in any group say, G_s then the absent variable assumes $\bullet$. Thus, in the block M_s^j at least one of i_1 and i_2-th row has all its entries equal to $\bullet$. Hence G-OR of i_1 and i_2-th rows when restricted to the block M_s^j gives $\bullet$ in all entries.

Combining the above three cases we can easily see that the G-OR of the two rows of restricted matrix $S^j[\{i_1, i_2\}]$ has at least one more j than any other color $l \in \mathbb{Z}_c - \{j\}$. Thus the contrast condition is satisfied.

We notice that in any system of the linear equations if we fix the value of one variable then the values of other variables are uniquely determined. This gives the pixel expansion of the scheme to be $\lceil \frac{n(n-1)}{4} \rceil c$.

Thus we have a $(2, n)_c$-CVCS when $gcd(2, c) = 1$.

□

Remark 2. We note that in light of Remark 1 the assumption $gcd(2, c) = 1$ plays a crucial role in the correctness of construction method. However the grouping

technique does not play any role whatsoever in the construction of $(2, n)_c$-CVCS. Our pairing algorithm gives a closed form of pixel expansion and it is the minimum pixel expansion one can get while using the linear algebraic technique. But any type of pairing of the minimal qualified sets will admit a $(2, n)_c$-CVCS, only with higher pixel expansion.

3.4 Construction of $(k, n)_c$-CVCS

Taking cue from Remark 2 we now construct a color visual secret sharing scheme on (k, n)-threshold access structure. Again we assume that $gcd(k, c) = 1$. The method of construction remains the same - we first pair the minimal qualified sets to form groups, form and solve corresponding systems of linear equations and collect the solutions to construct basis matrices. The proofs of correctness and secrecy follow an essentially same line of argument that has been used in Theorem 3.

We note that size of any minimal qualified set is k and therefore every system of linear equations contains $2k$ many variables. If $2k \leq n$ then there is a possibility that these $2k$ variables occurring in a system can be all different. In order to solve such a system of linear equations we need to fix the values of $2k - 2$ variables which results in c^{2k-2} many solutions for that system.

Theorem 4. *If $gcd(k, c) = 1$, $2 \leq k \leq n$ and m denotes the pixel expansion of a $(k, n)_c$-CVCS then $m \leq \lceil \frac{l}{2} \rceil c^{2k-2}$, where $l = \binom{n}{k}$.*

If we can adopt a technique for grouping such that in every group the pair of minimal qualified sets have $k - 1$ common participants then we have a $(k, n)_c$-CVCS with much better pixel expansion. Such a pairing technique is possible, *see* [8]. We now have the following theorem.

Theorem 5. *If $gcd(k, c) = 1$ and $2 \leq k \leq n$ then we have a $(k, n)_c$-CVCS with pixel expansion $\lceil \frac{l}{2} \rceil c^{k-1}$, where $l = \binom{n}{k}$.*

3.5 Modification of the Technique

We have noticed that the condition $\gcd(k, c) = 1$ plays a crucial role in the construction where k denotes the threshold value and c is the number of colors. In fact, the methodology fails if c, k are not relatively prime (*see* Remark 1). To overcome the difficulty when the numbers are not relatively prime, we can introduce some *dummy* colors $c, \ldots, r$ such that r is the least positive integer which is greater than c and also relatively prime with k. We can now work with the ring $\mathbb{Z}_r$ of colors where the last $r - c$ colors are dummy. Basis matrices for each of the first c colors can now be constructed using linear algebraic technique. Then we get rid of the dummy colors by replacing them with $\bullet$. It can be easily checked that after this replacement the resulting matrices constitute the basis matrices realizing the original $(k, n)_c$-CVCS according to Definition 1.

To gain clarity into the above discussion we describe construction of basis matrices of a $(3,4)$-CVCS with 3 colors $\{0,1,2\}$. As we have observed earlier, number of colors and the threshold value are not relatively prime. We will introduce one *dummy* color to make number of colors and threshold value relatively prime. Thus, the new color set can be thought of as $\mathbb{Z}_4 = \{0,1,2,3\}$. Following the same (usual) notations, the system of equations over $\mathbb{Z}_4$

$$\left.\begin{matrix} x_1+x_2+x_3=0 \\ x_1+x_2+x_4=0 \end{matrix}\right\} -1(0)\ ,\ \left.\begin{matrix} x_1+x_2+x_3=1 \\ x_1+x_2+x_4=1 \end{matrix}\right\} -1(1)\ \ \&\ \left.\begin{matrix} x_1+x_2+x_3=2 \\ x_1+x_2+x_4=2 \end{matrix}\right\} -1(2)\ \ .$$

and

$$\left.\begin{matrix} x_1+x_3+x_4=0 \\ x_2+x_3+x_4=0 \end{matrix}\right\} -2(0)\ ,\ \left.\begin{matrix} x_1+x_3+x_4=1 \\ x_2+x_3+x_4=1 \end{matrix}\right\} -2(1)\ \ \&\ \left.\begin{matrix} x_1+x_3+x_4=2 \\ x_2+x_3+x_4=2 \end{matrix}\right\} -2(2)\ \ .$$

Solving the above systems over $\mathbb{Z}_4$ and using the concatenation technique (Subsect. 3.1) we get

$$U^0 = \begin{bmatrix} 0000\ 1111\ 2222\ 3333\ 0321\ 3210\ 2103\ 1032 \\ 0123\ 0123\ 0123\ 0123\ 0321\ 3210\ 2103\ 1032 \\ 0321\ 3210\ 2103\ 1032\ 0123\ 0123\ 0123\ 0123 \\ 0321\ 3210\ 2103\ 1032\ 0000\ 1111\ 2222\ 3333 \end{bmatrix},$$

$$U^1 = \begin{bmatrix} 3333\ 0000\ 1111\ 2222\ 0321\ 3210\ 2103\ 1032 \\ 0123\ 0123\ 0123\ 0123\ 0321\ 3210\ 2103\ 1032 \\ 0321\ 3210\ 2103\ 1032\ 0123\ 0123\ 0123\ 0123 \\ 0321\ 3210\ 2103\ 1032\ 3333\ 0000\ 1111\ 2222 \end{bmatrix},$$

$$U^2 = \begin{bmatrix} 2222\ 3333\ 1111\ 0000\ 0321\ 3210\ 2103\ 1032 \\ 0123\ 0123\ 0123\ 0123\ 0321\ 3210\ 2103\ 1032 \\ 0321\ 3210\ 2103\ 1032\ 0123\ 0123\ 0123\ 0123 \\ 0321\ 3210\ 2103\ 1032\ 2222\ 3333\ 1111\ 0000 \end{bmatrix}.$$

We observe that U^0, U^1, U^2 are the basis matrices for the colors $0,1,2$ respectively when we consider $(3,4)_4$-CVCS with 4 colors. But in the original image the fourth color 3 was not present. It is the dummy color that we have introduced. Therefore we replace this dummy color by $\bullet$ to obtain the following three matrices. It is now easy to check that the following three are basis matrices realizing a $(3,4)_3$-CVCS.

$$S^0 = \begin{bmatrix} 0000\ \ 1111\ 2222\ \bullet\bullet\bullet\bullet\ 0\bullet 21\ \bullet 210\ 210\bullet\ 10\bullet 2 \\ 012\bullet\ \ 012\bullet\ 012\bullet\ \ 012\bullet\ \ 0\bullet 21\ \bullet 210\ 210\bullet\ 10\bullet 2 \\ 0\bullet 21\ \bullet 210\ 210\bullet\ 10\bullet 2\ \ 012\bullet\ \ 012\bullet\ 012\bullet\ \ 012\bullet \\ 0\bullet 21\ \bullet 210\ 210\bullet\ 10\bullet 2\ \ 0000\ \ 1111\ 2222\ \bullet\bullet\bullet\bullet \end{bmatrix},$$

$$S^1 = \begin{bmatrix} \bullet\bullet\bullet\bullet\ 0000\ 1111\ \ 2222\ \ 0\bullet 21\ \bullet 210\ 210\bullet\ 10\bullet 2 \\ 012\bullet\ \ 012\bullet\ 012\bullet\ \ 012\bullet\ \ 0\bullet 21\ \bullet 210\ 210\bullet\ 10\bullet 2 \\ 0\bullet 21\ \bullet 210\ 210\bullet\ 10\bullet 2\ \ 012\bullet\ \ 012\bullet\ 012\bullet\ \ 012\bullet \\ 0\bullet 21\ \bullet 210\ 210\bullet\ 10\bullet 2\ \bullet\bullet\bullet\bullet\ 0000\ 1111\ \ 2222 \end{bmatrix},$$

$$S^2 = \begin{bmatrix} 2222 & \bullet\bullet\bullet\bullet & 1111 & 0000 & 0\bullet 21 & \bullet 210 & 210\bullet & 10\bullet 2 \\ 012\bullet & 012\bullet & 012\bullet & 012\bullet & 0\bullet 21 & \bullet 210 & 210\bullet & 10\bullet 2 \\ 0\bullet 21 & \bullet 210 & 210\bullet & 10\bullet 2 & 012\bullet & 012\bullet & 012\bullet & 012\bullet \\ 0\bullet 21 & \bullet 210 & 210\bullet & 10\bullet 2 & 2222 & \bullet\bullet\bullet\bullet & 1111 & 0000 \end{bmatrix}.$$

4 Discussions and Experimental Results

In this section we discuss some experimental results and consider the problem of reducing share size.

In Fig. 1 we implement a $(2, 2)$-threshold visual cryptographic scheme for a color image. The secret image is a picture with three colors and we use the construction technique shown in Subsect. 3.2. We observe that since the scheme is of maximal contrast, corresponding to one secret pixel three subpixels are reconstructed - one true color pixel and two $\bullet$. Presence of two $\bullet$'s makes the reconstructed image dark.

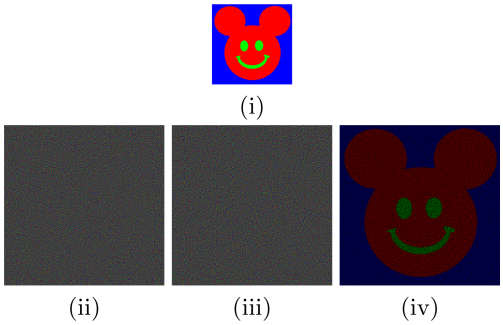

Fig. 1. $(2, 2)$-CVCS with 3 colors using Subsect. 3.2 (i) secret image, (ii)–(iii) shares of P_1, P_2 respectively, (iv) GOR(share1, share2) (Color figure online)

In Fig. 2 we implement a $(2, 3)$-threshold visual cryptographic scheme using the construction technique described in Example 2.

The main issue with deterministic GOR based color visual cryptographic scheme is its pixel expansion which is the share size of the scheme. Same problem occurs in the deterministic OR based black and white visual cryptographic scheme. To reduce share size, Yang [34] introduced a novel idea for B&W visual cryptographic scheme. Instead of distributing rows of a basis matrix to the participants as their shares, the dealer chooses randomly one column from a basis matrix and distribute the corresponding entries to the parties. Although the pixel expansion is reduced to 1, which implies the share size is equal to secret image size, but the deterministic recovery of the secret pixel is hampered. An error probability of correct reconstruction of secret pixel is automatically introduced. For black and white image there are only two choices for every reconstructed

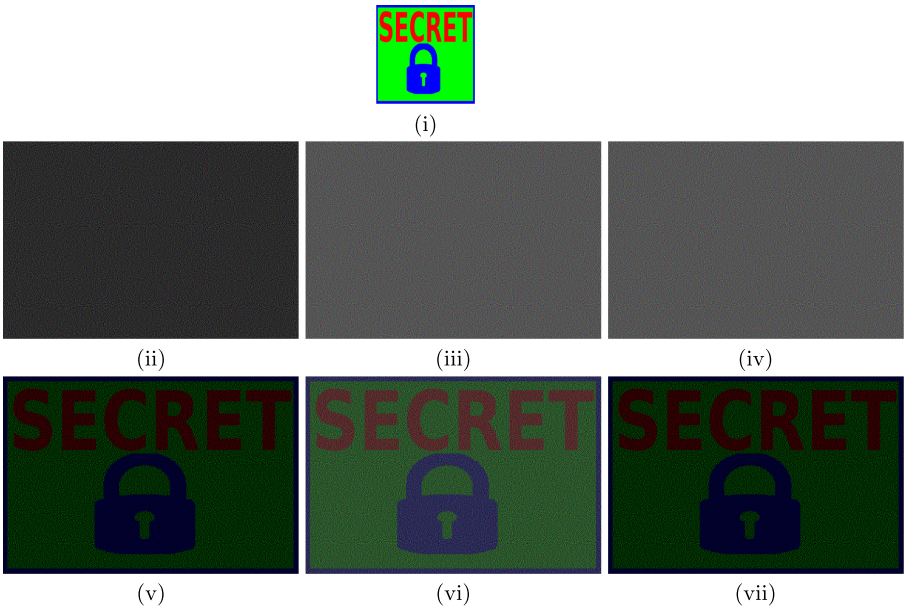

Fig. 2. $(2, 3)$-CVCS with 3 colors using Subsect. 3.3 (i) secret image, (ii)-(iv) shares of P_1, P_2, P_3 respectively, (v) GOR(share1, share2), (vi) GOR(share2, share3), (vii) GOR(share1, share2, share3)

pixel- either black or white and this can be directly translated to "either correct or incorrect". The problem with color visual secret sharing is more tricky. Although the meaning of "correct reconstruction" of a colored pixel remains the same but "incorrect reconstruction" now perhaps includes more options.

Let us consider the basis matrix S^0 of Example 2. The discussion for S^1, S^2 will be similar. First let us focus on shares of P_2, P_3. If a column from S^0 is randomly selected and the entries are given as shares then incorrect reconstruction can happen in three different manner- reconstruction of $\bullet$ or 1 or 2. If a $\bullet$ is observed then it is not possible to guess the actual color of the corresponding pixel but if 1 or 2 is reconstructed then there is problem of misinterpreting the true color of the original pixel. It is easily seen that the probability of reconstructing color 1 is $\frac{1}{6}$ and that of color 2 is also $\frac{1}{6}$. However, probability of reconstructing true color 0 is higher viz. $\frac{2}{6}$. On the other hand, if we consider the shares of P_1, P_2 it can be easily seen that there is no possibility of misinterpretation of the recovered color - either it is the pixel of color 0 or $\bullet$. In other words, these two shares satisfy the conditions of maximal contrast (see Definition 3).

In Fig. 3 we implement a probabilistic color visual cryptographic scheme using the basis matrices given in Example 2 and then choosing columns of S^c randomly to share a pixel of color c. The recovered images from the shares of P_2 and P_3 are brighter [item (vi) in Fig. 2 and Fig. 3]. This matches with our theory because for the shares P_2, P_3 the recovery of $\bullet$ is less (probable). On the other hand, share of P_1 contributes more $\bullet$s into the recovered images and thereby resulting in more darker versions of recovered images [(v) & (vii) of Fig. 2 and Fig. 3].

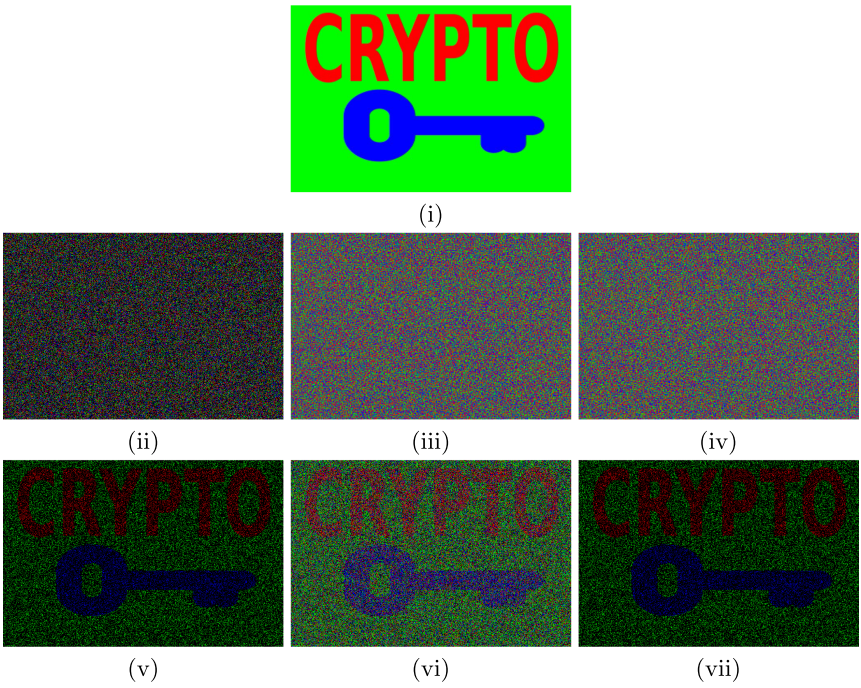

Fig. 3. $(2, 3)$-PCVCS with 3 colors using Subsect. 3.3 (i) secret image, (ii)-(iv) shares of P_1, P_2, P_3 respectively, (v) GOR(share1, share2), (vi) GOR(share2, share3), (vii) GOR(share1, share2, share3) (Color figure online)

4.1 Comparison

In Table 1 and Table 2 we compare our results (from Sect. 3) with the existing works of Yang-Laih [35] and Verheul-Tilborg [33].

Table 1. Comparison of pixel expansions among our proposed scheme, Yang et al. [35] & Verheul-Tilborg [33] with three colors.

Schemes	Pixel expansion		
	Our	Yang-Laih[35]	Verheul-Tilborg [33]
(2,2)	3	5	9
(2,3)	6	8	12
(2,4)	9	11	15
(3,3)	16	12	27
(3,4)	32	18	75
(4,4)	27	23	81

Table 2. Comparison of pixel expansions among our proposed scheme, Yang et al. [35] & Verheul-Tilborg [33] with four colors.

Schemes	Pixel expansion		
	Our	Yang-Laih [35]	Verheul-Tilborg [33]
(2,2)	5	7	12
(2,3)	10	11	12
(2,4)	15	15	15
(3,3)	16	13	48
(3,4)	32	24	75
(4,4)	125	31	142

5 Conclusion

We have given a linear algebraic method for constructing basis matrices realizing color visual cryptographic scheme for threshold access structures. Using the same technique to construct general access structures have some inherent difficulties e.g. the number of colors and number of parties in every minimal qualified set have to be relatively prime. Introducing *dummy* colors we may fix the problem but that will incur in huge pixel expansion. Efficient solution to this question can be a direction for further research.

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 Crypt. **73**(3), 865–895 (2013). https://doi.org/10.1007/s10623-013-9832-5

2. Adhikari, A., Dutta, T.K., Roy, B.: A new black and white visual cryptographic scheme for general access structures. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 399–413. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30556-9_31
3. Adhikari, A., Sikdar, S.: A new $(2,n)$-visual threshold scheme for color images. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 148–161. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-24582-7_11
4. Adhikari, M.R., Adhikari, A.: Basic Modern Algebra with Applications. Springer, New Delhi (2014). https://doi.org/10.1007/978-81-322-1599-8_9
5. Arumugam, S., Lakshmanan, R., Nagar, A.K.: On $(k,n)^*$-visual cryptography scheme. Des. Codes Crypt. **71**(1), 153–162 (2014). https://doi.org/10.1007/s10623-012-9722-2
6. Ateniese, G., Blundo, C., Santis, A.D., Stinson, D.R.: Visual Cryptography for General Access Structures. Inf. Comput. **129**, 86–106 (1996)
7. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Constructions and bounds for visual cryptography. In: Meyer, F., Monien, B. (eds.) ICALP 1996. LNCS, vol. 1099, pp. 416–428. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-61440-0_147
8. Bitner, J.R., Ehrlich, G., Reingold, E.M.: Efficient generation of the binary reflected Gray code. Commun. ACM **19**(9), 517–521 (1976)
9. Blundo, C., D'arco, P., Santis, A.D., Stinson, D.R.: Contrast optimal threshold visual cryptography. SIAM J. Discrete Math. **16**(2), 224–261 (2003)
10. Blundo, C., Bonis, A.D., Santis, A.D.: Improved schemes for visual cryptography. Des. Codes Crypt. **24**(3), 255–278 (2001)
11. Cheng, Y., Fu, Z., Yu, B.: Improved visual secret sharing scheme for QR code applications. IEEE Trans. Inf. Forensics Secur. **13**(9), 2393–2403 (2018)
12. Cimato, S., Prisco, R.D., Santis, A.D.: Optimal colored threshold visual cryptography schemes. Des. Codes Crypt. **35**(3), 311–335 (2005). https://doi.org/10.1007/s10623-003-6741-z
13. Cimato, S., Prisco, R.D., Santis, A.D.: Colored visual cryptography without color darkening. Theor. Comput. Sci. **374**(1–3), 261–276 (2007)
14. Cimato, S., Yang, C.N.: Visual Cryptography and Secret Image Sharing. Taylor & Francis, CRC Press (2011)
15. Cimato, S., Yang, J.C.N., Wu, C.-C.: Visual cryptography based watermarking. In: Shi, Y.Q., Liu, F., Yan, W. (eds.) Transactions on Data Hiding and Multimedia Security IX. LNCS, vol. 8363, pp. 91–109. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55046-1_6
16. 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 Crypt. **80**(1), 165–196 (2016)
17. Dutta, S., Adhikari, A.: XOR based non-monotone $t-(k,n)^*$ -visual cryptographic schemes using linear algebra. ICICS **2014**, 230–242 (2014)
18. Dutta, S., Adhikari, A.: Contrast optimal XOR based visual cryptographic schemes. In: Shikata, J. (ed.) ICITS 2017. LNCS, vol. 10681, pp. 58–72. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-72089-0_4
19. Dutta, S., Adhikari, A., Ruj, S.: Maximal contrast color visual secret sharing schemes. Des. Codes Crypt. **87**(7), 1699–1711 (2018). https://doi.org/10.1007/s10623-018-0570-6
20. Guo, T., Liu, F., Wu, C.K., Ren, Y.W., Wang, W.: On (k,n) visual cryptography scheme with t essential parties. In: Padró, C. (ed.) ICITS 2013. LNCS, vol. 8317, pp. 56–68. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-04268-8_4

21. Hou, Y.-C.: Visual cryptography for color images. Pattern Recogn. **36**(7), 1619–1629 (2003)
22. Iwamoto, M.: A weak security notion for visual secret sharing schemes. IEEE Trans. Inf. Forensics Secur. **7**(2), 372–382 (2012)
23. Jin, D., Yan, W.-Q., Kankanhalli, M.S.: Progressive color visual cryptography. J. Electron. Imaging **14**(3), 033019 (2005)
24. Koga, H., Yamamoto, H.: Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. IEICE Trans. Fund. Electron. Commun. Comput. Sci. **81**(6), 1262–1269 (1998)
25. Liu, F., Wu, C.K., Lin, X.J.: Colour visual cryptography schemes. IET Inf. Secur. **2**(4), 151–165 (2008)
26. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995). https://doi.org/10.1007/BFb0053419
27. Rijmen, V., Preneel, B.: Efficient colour visual encryption or Shared colors of benetton. EUROCRYPT 1996 Rump Section (1996). http://www.iacr.org/conference/ec96/rump/preneel.ps.gz
28. Praveen, K., Rajeev, K., Sethumadhavan, M.: On the extensions of (k, n)*-visual cryptographic schemes. In: Martínez Pérez, G., Thampi, S.M., Ko, R., Shu, L. (eds.) SNDS 2014. CCIS, vol. 420, pp. 231–238. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54525-2_21
29. Shen, G., Liu, F., Fu, Z., Yu, B.: New insight into linear algebraic technique to construct visual cryptography scheme for general access structure. Multimedia Tools Appl. **76**(12), 14511–14533 (2017)
30. Shen, G., Liu, F., Fu, Z., Yu, B.: Perfect contrast XOR-based visual cryptography schemes via linear algebra. Des. Codes Crypt. **85**(1), 15–37 (2016). https://doi.org/10.1007/s10623-016-0285-5
31. Shen, G., Liu, F., Fu, Z., Yu, B.: Visual cryptograms of random grids via linear algebra. Multimedia Tools Appl. **77**(10), 12871–12899 (2017). https://doi.org/10.1007/s11042-017-4921-5
32. Shyu, S.J.: Efficient visual secret sharing scheme for color images. Pattern Recogn. **39**(5), 866–880 (2006)
33. Verheul, E.R., Tilborg, H.C.A.: Constructions and properties of k out of n visual secret sharing schemes. Des. Codes Crypt. **11**(2), 179–196 (1997). https://doi.org/10.1023/A:1008280705142
34. Yang, C.-N.: New visual secret sharing schemes using probabilistic method. Pattern Recogn. Lett. **25**, 481–494 (2004)
35. Yang, C.-N., Laih, C.-S.: New colored visual secret sharing schemes. Des. Codes Crypt. **20**(3), 325–336 (2000)