Designs, Codes and Cryptography, 35, 311–335, 2005

Optimal Colored Threshold Visual Cryptography Schemes

STELVIO CIMATO cimato@dia.unisa.it
ROBERTO DE PRISCO* robdep@dia.unisa.it
ALFREDO DE SANTIS ads@dia.unisa.it
Dipartimento di Informatica ed Applicazioni, Universitá di Salerno, 84081 Baronissi (SA), Italy

Communicated by: H. Van Tilborg

Received July 11, 2002; Revised July 10, 2003; Accepted July 31, 2003

Abstract. Visual cryptography schemes allow the encoding of a secret image into n shares which are distributed to the participants. The shares are such that only qualified subsets of participants can "visually" recover the secret image. Usually the secret image consist of black and white pixels. In colored threshold visual cryptography schemes the secret image is composed of pixels taken from a given set of c colors. The pixels expansion and the contrast of a scheme are two measures of the goodness of the scheme.

In this paper, we study c-color (k,n)-threshold visual cryptography schemes and provide a characterization of contrast-optimal schemes. More specifically we prove that there exists a contrast-optimal scheme that is a member of a special set of schemes, which we call *canonical* schemes, and that satisfy strong symmetry properties.

Then we use canonical schemes to provide a constructive proof of optimality, with respect to the pixel expansion, of c-color (n,n)-threshold visual cryptography schemes.

Finally, we provide constructions of c-color $(2,n)$-threshold schemes whose pixels expansion improves on previously proposed schemes.

Keywords: visual crytography, secret sharing schemes

AMS Classification: 94A60

1. Introduction

A visual cryptography scheme for a set $\mathcal{P}$ of n participants is a method to encode a secret image into n shadow images in the form of transparencies, called shares, where each participant in $\mathcal{P}$ receives one share. Certain subsets of participants, called qualified sets, can "visually" recover the secret image, but other subsets of participants, called forbidden sets, have no information on the secret image. A "visual" recovery for a set $X \subseteq \mathcal{P}$ consists of stacking the shares (transparencies) given to the participants in X. The participants in a qualified set X will be able

*This author is also a member of the Akamai Faculty Group, Akamai Technologies, 8 Cambridge center, Cambridge, MA 02142, USA.

to see the secret image without any knowledge of cryptography and without performing any cryptographic computation. Forbidden sets of participants will have no information on the secret image.

This cryptographic paradigm was introduced by Naor and Shamir [6]. They analyzed the case of (k, n)-threshold visual cryptography schemes, in which a black and white secret image is visible if and only if any k transparencies are stacked together.

In order to implement a visual cryptography scheme, each pixel of the secret image is subdivided into a certain number m of subpixels. Hence, there is a loss of resolution proportional to m. The *pixel expansion* m is the most important measure of the goodness of a scheme. Obviously, schemes with smaller pixel expansion are better. Optimal schemes are those that have the minimum pixel expansion. Another important measure for the goodness of a scheme is the *contrast*, which is a measure of the quality of the reconstructed image.

The work of Naor and Shamir has sparkled the "visual cryptography" research vein, and a substantial amount of work has followed [6]. Most of the work done focused on black and white visual cryptography, where the secret image to be shared is composed of black and white pixels. Paper [2] is a recent work on black and white visual cryptography where the reader can find more references.

In this paper, we are concerned with colored visual cryptography. Verheul and Van Tilborg [7] were the first to consider colored visual cryptography, where the pixels in the secret image are taken from a given set of c colors. Their model assumes that, when superimposing pixels of different colors, one sees a special black color. This artificial property can be simulated by subdividing each pixel into c subpixels. Hence, in the model of [7] there is an additional loss of resolution of a factor of c. The construction provided in [7] yields (k, n)-threshold schemes.

In [3] constructions of (n, n)-threshold colored visual cryptography schemes have been provided. These schemes use the same model of [7] and improve the pixel expansion of the (n, n)-threshold scheme of [7], at least for the value of n for which a comparison is possible (the pixel expansion of the schemes in [7] is not explicitly computed for all values of n).

In [8] constructions for (k, n)-threshold colored visual cryptography schemes have been considered using a slightly different model: in order to avoid the additional loss of resolution due to the implementation of the artificial property described above, it is required that schemes be implemented in such a way that pixels of different colors are never superimposed.

For the case $k = n$, the constructions of [8] improve on those of [3, 7]. For other values of k, there are cases where the constructions of [8] have a better pixel expansion than those of [7] and also cases where the *vice versa* is true (we refer the reader to [8] for a comparison).

In this paper, we construct schemes where pixels of different colors are never superimposed. We provide a constructive proof of optimality for (n, n)-threshold schemes, that is, our proof establishes a lower bound on the pixel expansion and at the same time it gives schemes that achieve the lower bound. It turns out that

these schemes are the same as the (n, n)-threshold schemes of [8], though they are obtained with different techniques.

We also provide a characterization of (k, n)-threshold schemes with optimal contrast. More specifically we prove that there exists a scheme with optimal contrast that belongs to a particular class of schemes. Schemes of such a class will be called canonical schemes and they satisfy strong symmetry properties.

Finally, we provide new constructions of $(2, n)$-threshold schemes that improve on the pixel expansion of both [7] and [8].

2. The Model

2.1. *Definition of* (k, n)*-threshold colored schemes*

A secret image, consisting of colored pixels, has to be shared among a set $\mathcal{P} = \{1, \ldots, n\}$ of *participants*. A trusted party, which is called the *dealer* and is not a participant, knows the secret image. The dealer has to distribute *shares* to the n participants in the form of printed transparencies. The subsets of $\mathcal{P}$ consisting of at least k participants are called *qualified sets*. Participants in a qualified subset have to be able to "visually" recover the secret image, by stacking together their shares (transparencies) and holding the stacked set of transparencies to the light. All other subsets, that is, those which have less than k participants, are called *forbidden sets*. Participants in a forbidden set have not to be able to get any information on the secret image from their shares (neither by stacking together the transparencies nor by any other computation). Schemes where the forbidden and qualified sets are defined as above are called (k, n)-threshold schemes. Sometimes more general access structures are used, however, in this paper we are concerned only with (k, n)-threshold schemes.

From now on, we concentrate on how to deal with just one pixel of the image. In order to share the whole image, it is enough to repeat the sharing process for each pixel of the image.

Each secret pixel is divided into m subpixels. This implies a loss of resolution: the pixels of the reconstructed image will be m times bigger compared to the ones of the original image. A *share* is a "version" of the secret pixel consisting of a particular assignment of colors to the m subpixels.

Each pixel (either in the original image or in the shares) has one of c colors which we denote by $\{0, 1, \ldots, c-1\}$. We assume that there is a special black color that we denote with the symbol $\star$. So, the complete set of colors is $\{\star, 0, 1, \ldots, c-1\}$. We remark that we still have only c colors in the original image; the special black color is needed to cover up the noise introduced in the reconstructed image in order to not reveal information to forbidden sets of participants.

In the model proposed in [7], it is assumed that the subpixels have the following property: when two subpixels, of color i and color j, are put on top of each other and held to the light, one sees color i if $i = j$, otherwise, i.e., if $i \neq j$, one sees $\star$.

Clearly, this is not what happens in reality, but it is possible to "simulate" such a behavior by dividing each subpixel into c (sub)subpixels and representing

a subpixel of color i by coloring with color $\star$ each of the c (sub)subpixels except for the ith one which is colored with color i (see [7] for more details).

Encoding pixels as explained above the special property holds. However, this technique has two drawbacks: it requires a further loss of resolution and when all the superimposed pixels are of color i, we only see one (sub)subpixel of color i (which is a fraction of $1/c$ of the whole subpixel), while all the other (sub)subpixels are $\star$.

In order to avoid these problems, one can design schemes where the shares are such that pixels of different colors are never superimposed. That is pixels of a superposition are either equal to some color i or they are equal to the special black color $\star$. Hence, we assume a model that does not allow the superposition of pixels with different colors, except for the case where one of the colors is the special black color $\star$. This model is used also in [8].

The "generalized" or operator, defined in [7], takes two pixels of colors i and j and returns i if $i = j$, and $\star$ if one of the colors is $\star$. We denote this operator with gor. The gor operator is easily extended to (column) vectors of colors: it returns i if all the color of the vector are i otherwise it returns $\star$. We also extend it to matrices: given a matrix M the $\mathrm{gor}(M)$ is the (row) vector with elements in $\{\star, 0, 1, \ldots, c-1\}$ obtained by letting entry i be the gor of column i of M. We also use a generalized Hamming weight $w_i(\Psi)$ for a vector of colors Ψ, which gives the number of colors in Ψ that are equal to color i. Notice that $w_\star(\Psi)$ returns the number of components equal to the special $\star$ color.

Given a matrix M and a set X of natural numbers, which represent participants, we denote by $M|X$ the matrix consisting of only the rows of M corresponding to the integers in X, if they exists in M. For example, assuming that M has at least 6 rows, if $X = \{2, 3, 6\}$, then $M|X$ is the submatrix of M, consisting of the second, the third and the sixth row of M.

Next we provide the definition of a colored visual cryptography scheme.

Definition 2.1 [7]. Consider a set of c colors $\{0, 1, \ldots, c-1\}$ and let h and ℓ be integers such that $0 \le \ell < h \le m$. A c-color (k, n)-threshold visual cryptography scheme for a set of n participants, consists of c collections (multisets) of $n \times m$ matrices $\mathscr{C}^0, \ldots \mathscr{C}^{c-1}$, whose elements are colors or $\star$, satisfying:

1. Given a qualified set $X, |X| \ge k$, for any $M \in \mathscr{C}^i$, it holds that $w_i\ (\mathrm{gor}(M|X)) \ge h$ and $w_j(\mathrm{gor}(M|X)) \le \ell$ for any $j \ne i$.
2. Given a forbidden set $X, |X| < k$, the c collections of $|X| \times m$ matrices, $\mathscr{D}^i$, $i = 0, 1, \ldots, c-1$, consisting of $M|X$ for each $M \in \mathscr{C}^i$, are equal.

To share a secret pixel of color i, the dealer randomly chooses one of the matrices in $\mathscr{C}^i$ and distributes row j to participant j. Thus, the chosen matrix defines the m subpixels in each of the n transparencies.

Since matrices of $\mathscr{C}^i$ are used to share pixels of color i we say that i is the *primary* color for $\mathscr{C}^i$, while any other color $i' \ne i$ is a *secondary* color for $\mathscr{C}^i$.

Property 1 of Definition 2.1 is called the *contrast property* because it guarantees that the secret image will be reconstructed for a qualified set of participants. Property 2 is called the *security property* because it guarantees that a forbidden set of participants has no information has no information on the secret image. An alternative definition for the contrast property is the one that guarantees the reconstruction only for qualified sets X whose cardinality is exactly k:

1′ Given a qualified set $X, |X|=k$, for any $M \in \mathscr{C}^i$, it holds that $w_i\ (\text{gor}(M|X)) \geq h$ and $w_j\ (\text{gor}(M|X)) \leq \ell$ for any $j \neq i$.

This is without loss of generality since a qualified set of participants consisting of more than k members can anyway reconstruct the image by simply using only k shares and leaving out the remaining ones. When proving lower bounds, however the two definitions are not equivalent: a lower bound proved using definition 1′ holds also in a model that uses definition 1 while the opposite is not true. Our lower bounds hold in the model that uses definition 1′.

2.2. *Base Matrices*

Given a matrix B we denote by $\mathscr{C}(B)$ the set of matrices obtained by permuting in all possible ways the columns of B. In most schemes, the c collections $\mathscr{C}^i$ are obtained by fixing c matrices B^i and letting $\mathscr{C}^i = \mathscr{C}(B^i)$. The matrices B^i are called the "base matrices". Base matrices constitute an efficient representation of the scheme. Indeed, the dealer has to store only the base matrices and in order to randomly choose a matrix from $\mathscr{C}(B^i)$ he has to randomly choose a permutation of the columns of the base matrix B^i.

Notice that the security property for a base matrices scheme is equivalent to: Given a forbidden set X, the matrices $B^i|X$, for $i=0, 1, \ldots, c-1$ are the same up to a permutation of the columns.

2.3. *Efficiency of Schemes*

The goodness of a scheme is measured in terms of two parameters:

- m: *Pixel expansion.* The number of subpixels used to represent each pixel of the original image measures the loss of resolution from the original image to the reconstructed one. One would like to have m as small as possible.
- α: *Contrast.* The contrast is defined as $(h-\ell)/m$ and is a measure of the quality of the reconstructed image. One would like α to be as big as possible. (In an ideal, but impossible, reconstruction one would have $\alpha=1$, that is $h=m$ and $\ell=0$.)

Given a scheme $\mathscr{S}$ we denote with $m(\mathscr{S})$ the pixel expansion of $\mathscr{S}$, with $h(\mathscr{S})$, and $\ell(\mathscr{S})$ the thresholds h and ℓ of $\mathscr{S}$ and with $\alpha(\mathscr{S})$ the contrast of $\mathscr{S}$.

3. Contrast-optimal $(\mathbf{k}, \mathbf{n})$ Schemes

In this section, we are interested in (k, n)-threshold schemes with optimal (that is, maximal) contrast. We will characterize contrast-optimal schemes and give a linear program whose solution provides a scheme with optimal contrast. Contrast-optimal schemes will be instrumental in providing the proof of the lower bound on the pixel expansion in Section 4.

In order to find the optimal contrast we identify a subset of all the (k, n)-threshold schemes; schemes belonging to such subset will be called canonical schemes. We prove that there exists a canonical scheme with optimal contrast. Hence, in order to find the optimal contrast, it suffices to find the canonical scheme having the maximal contrast among the canonical schemes.

We start by providing a sequence of lemmas showing that there exist schemes with optimal contrast whose base matrices satisfy strong symmetry properties. Such a sequences of lemmas will culminate with Lemma 3.5, which characterizes the canonical schemes. We start with a simple lemma which is a trivial generalization of a result proved in Section 2.1 of [1].

LEMMA 3.1. *Let $\mathscr{S}$ be a c-color (k, n)-threshold scheme. There exists a c-color (k, n)-threshold scheme $\mathscr{S}'$, such that:*

1. *the c collections of $\mathscr{S}'$ have the same size;*
2. $\alpha(\mathscr{S}) = \alpha(\mathscr{S}')$;
3. $m(\mathscr{S}) = m(\mathscr{S}')$.

We omit the proof since the same proof of [1] for black and white schemes works for colored schemes with a trivial generalization. The next lemma shows that, given a scheme it is always possible to find a base matrices scheme with the same contrast. Given two matrices A and B with the same number of rows, we write $A \circ B$ to denote the concatenation of the two matrices.

LEMMA 3.2. *Let $\mathscr{S}$ be a c-color (k, n)-threshold scheme. There exists a c-color (k, n)-threshold schemes $\mathscr{S}'$, such that:*

1. *$\mathscr{S}'$ is a base matrices scheme;*
2. $\alpha(\mathscr{S}) = \alpha(\mathscr{S}')$.

Proof. By Lemma 3.1 we can assume, without loss of generality, that the collections of matrices of $\mathscr{S}$ have the same cardinality, say z. Let $\mathscr{C}^0 = \{C_1^0, C_2^0, \ldots, C_z^0\}, \mathscr{C}^1 = \{C_1^1, C_2^1, \ldots, C_z^1\}, \ldots, \mathscr{C}^{c-1} = \{C_1^{c-1}, C_2^{c-1}, \ldots, C_z^{c-1}\}$ be the collections of matrices of scheme $\mathscr{S}$. Construct a new scheme $\mathscr{S}'$ having the following base matrices: $B^i = C_1^i \circ C_2^i \circ \cdots \circ C_z^i$, for each $i = 0, 1, \ldots, c-1$. That is, the base matrix for color i is obtained by concatenating all the matrices of the collection $\mathscr{C}^i$.

Scheme $\mathscr{S}'$ satisfies the contrast property. Indeed, let X be a qualified set of participants. By definition, for each matrix $C \in \mathscr{C}^i$ we have that $w_i(\text{gor}(C|X)) \geqslant h(\mathscr{S})$. Hence $w_i(\text{gor}(B_i|X)) \geqslant h'$ where $h' = z \cdot h(\mathscr{S})$. By definition, for each matrix $C \in \mathscr{C}^i$ we have that $w_j(\text{gor}(M|X)) \leqslant \ell(\mathscr{S})$. Hence $w_j(\text{gor}(B^i)|X)) \leqslant \ell'$ where $\ell' = z \cdot \ell(\mathscr{S})$.

Scheme $\mathscr{S}'$ satisfies the security property. Indeed, let X be a forbidden set of participants. We have that $\mathscr{D}^i = \{C_0^i|X, \ldots, C_z^i|X\}$ is the same for all $i = 0, 1, \ldots, c-1$. Hence matrices $B^0|X, B^1|X, \ldots, B^{c-1}|X$ are the same up to a permutation of the columns.

Finally we have that

$$\alpha(\mathscr{S}') = \frac{h(\mathscr{S}') - \ell(\mathscr{S}')}{m(\mathscr{S}')} = \frac{z \cdot h(\mathscr{S}) - z \cdot \ell(\mathscr{S})}{z \cdot m(\mathscr{S})} = \alpha(\mathscr{S}).$$

■

The next lemma shows that given a scheme $\mathscr{S}$ with contrast $\alpha(\mathscr{S})$ it is always possible to find a scheme with the same contrast and with the property that the multiplicity of columns in the base matrices does not depend neither on the color nor on the position of the $\star$ color in the columns.

Before giving the lemma we introduce some notation useful to describe formally the above property. We denote by $\Psi^n(w, i, j)$, with $n, w, i, j \in \mathscr{N}$, where $0 \leqslant w \leqslant n$ and i is an integer whose binary representation has exactly w digits equal to 1, the column vector of size n constructed as follows: consider the binary vector corresponding to the binary representation of i, with the least significant bit on the first element of the column; then substitute each 1 with j and each 0 with $\star$. In the rest of the paper we will omit n since it is given by the context; so we write $\Psi(w, i, j)$ instead of $\Psi^n(w, i, j)$.

Let $n = 5$; the columns $\Psi(2, 17, 3), \Psi(1, 8, 0), \Psi(5, 31, 0)$, and $\Psi(0, 0, j)$ are shown in the following.

$$\begin{bmatrix} 3 \\ \star \\ \star \\ \star \\ 3 \end{bmatrix} \quad \begin{bmatrix} \star \\ \star \\ \star \\ 0 \\ \star \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} \star \\ \star \\ \star \\ \star \\ \star \end{bmatrix}.$$

Given a matrix M and a column $\Psi(w, i, j)$, we define $\mu^M(\Psi(w, i, j))$ as the number of times that $\Psi(w, i, j)$ appears in M, i.e., the multiplicity of $\Psi(w, i, j)$ in M. For brevity we also use $\mu^M(w, i, j) = \mu^M(\Psi(w, i, j))$.

Define I_w^n as the set of binary numbers with n digits, w of which are 1. For example, we have that $I_0^4 = \{0\}, I_1^4 = \{1, 2, 4, 8\}, I_2^4 = \{3, 5, 6, 9, 10, 12\}$, $I_3^4 = \{7, 11, 13, 14\}, I_4^4 = \{15\}$. Notice that, given n and w, it is possible to construct column $\Psi(w, i, j)$, for some j, only when $i \in I_w^n$.

We are now ready to present the lemma.

LEMMA 3.3. *Let $\mathscr{S}$ be a c-color (k, n)-threshold scheme. There exists a c-color (k, n)-threshold scheme $\mathscr{S}'$, such that:*

1. *$\mathscr{S}'$ is a scheme with base matrices $B^0, B^1, \ldots, B^{c-1}$;*
2. *$\alpha(\mathscr{S}) = \alpha(\mathscr{S}')$;*
3. *For any fixed weight w and colors j and j', we have that $\mu^{B^j}(w, i, j')$ is constant with respect to $i \in I_w^n$.*

Proof. By Lemma 3.2 we can assume, without loss of generality, that scheme $\mathscr{S}$ is a base matrices scheme. Let $C^0, C^1, \ldots, C^{c-1}$, be the base matrices of scheme $\mathscr{S}$. Let $\sigma_1, \sigma_2, \ldots, \sigma_{n!}$ be all the possible permutations of the set $\{1, 2, \ldots, n\}$. Let $C^j_{\sigma_z}$ be the matrix C^j with the rows permuted according to the permutation σ_z. Construct a new scheme $\mathscr{S}'$ having the following base matrices: $B^j = C^j_{\sigma_1} \circ C^j_{\sigma_2} \circ \cdots \circ C^j_{\sigma_{n!}}$, for each $j = 0, 1, \ldots, c-1$.

Let us first prove that scheme $\mathscr{S}'$ satisfies the contrast property. Let X be a qualified set of participants and let X' be the set of integers such that $C^j_{\sigma_z}|X = C^j|X'$. Since σ_z is a permutation, also X' is a qualified set of participants. By definition, matrix C^j satisfies $w_j(\mathrm{gor}(C^j|X')) \geqslant h(\mathscr{S})$. Hence, for any z, matrix $C^j_{\sigma_z}$ satisfies $w_j(\mathrm{gor}(C^j_{\sigma_z}|x)) \geqslant h(\mathscr{S})$. Thus we have that $w_j(\mathrm{gor}(B^j_X)) \geqslant h'$ where $h' = n! \cdot h(\mathscr{S})$. Similarly, we have that $w_{j'}(\mathrm{gor}(B_X)) \leqslant \ell'$ where $\ell' = n! \cdot \ell(\mathscr{S})$, for any $j' \neq j$. Thus the contrast property is satisfied.

Scheme $\mathscr{S}'$ satisfies the security property. Indeed, let X be a forbidden set of participants. Let j' and j'' be two colors. We have that $B^{j'}|X = C^{j'}_{\sigma_1}|X \circ C^{j'}_{\sigma_2}|X \circ \cdots \circ C^{j'}_{\sigma_{n!}}|X$ and $B^{j''}|X = C^{j''}_{\sigma_1}|X \circ C^{j''}_{\sigma_2}|X \circ \cdots \circ C^{j''}_{\sigma_{n!}}|X$. For the security property of $\mathscr{S}$, for all $z = 1, 2, \ldots, n!$, matrices $C^{j'}_{\sigma_z}|X$ and $C^{j''}_{\sigma_z}|X$ are the same up to a permutation of the columns. Hence, $B^{j'}|X$ and $B^{j''}|X$, for any j', j'', are the same up to a permutation of the columns. Thus, the security property holds also for $\mathscr{S}'$.

The two schemes have the same contrast, indeed we have that

$$\alpha(\mathscr{S}') = \frac{h' - \ell'}{m'} = \frac{n! \cdot h(\mathscr{S}) - n! \cdot \ell(\mathscr{S})}{n! \cdot m(\mathscr{S})} = \alpha(\mathscr{S}).$$

It remains to prove property 3. Fix $j, 0 \leqslant j \leqslant c-1$, and thus a base matrix B^j of the new scheme $\mathscr{S}'$ and a base matrix C^j of the initial scheme $\mathscr{S}$. Fix a weight w. The following reasoning is valid for any column of weight w of matrix C^j. Let ϕ be a column of C^j, whose weight is w and let $i \in I_w$ and j' be such that $\phi = \Psi(w, i, j')$. By construction, B^j contains exactly $n!$ columns that derive from ϕ, one for each permutation. Of these columns, exactly, $w! \cdot (n-w)!$ are equal to $\Psi(w, i', j')$ for each $i' \in I_w$. Hence, for each column ϕ in C^j there will be in B^j exactly $w! \cdot (n-w)!$ columns equal to $\Psi(w, i', j')$ for each $i' \in I_w$. Thus, fixed an $\bar{\imath} \in I_w$ we have that

$$\mu^{B^j}(w, \bar{\imath}, j') = |I_w| \cdot w! \cdot (n-w!) = \binom{n}{w} \cdot w! \cdot (n-w!)$$

which is constant with respect to $\bar{\imath}$. ∎

The next lemma tells us that given a scheme, if we permute the colors we obtain a new scheme for the permuted set of colors. For the sake of simplicity we give the lemma only for base matrices schemes[1], but it holds for any scheme.

LEMMA 3.4. *Let $\mathcal{S}$ be a c-color (k,n)-threshold scheme with base matrices $C^0, C^1, \ldots, C^{c-1}$. Let σ be a permutation of the colors. Let $\bar{\mathcal{S}}$ be the scheme whose base matrices are $\bar{C}^0, \bar{C}^1, \ldots, C^{\bar{c}-1}$, where $\bar{C}^{\sigma(j)}$ is obtained by letting $\bar{C}^{\sigma}(j)(\bar{\imath}, \bar{\jmath})$ be equal to $\sigma(C(\bar{\imath}, \bar{\jmath}))$, for any possible row $\bar{\imath}$ and column $\bar{\jmath}$. Scheme $\bar{\mathcal{S}}$ is a c-color (k,n)-threshold scheme. Moreover, $m(\mathcal{S}) = m(\mathcal{S}')$, $h(\mathcal{S}) = h(\mathcal{S}')$ and $\ell(\mathcal{S}) = \ell(\mathcal{S}')$.*

Proof. Trivial: we just renamed the colors. ■

Finally, the next lemma shows that given a scheme $\mathcal{S}$ with contrast $\alpha(\mathcal{S})$ it is always possible to find a scheme with the same contrast and with the property that the multiplicity of columns in the base matrices depends only on whether the color is primary or secondary. Recall that, for a base matrix C^j, color j is the primary color and any other color $j' \neq j$ is a secondary color.

LEMMA 3.5. *Let $\mathcal{S}$ be a c-color (k,n)-threshold scheme. There exists a c-color (k,n)-threshold scheme $\mathcal{S}'$, such that:*

1. *$\mathcal{S}'$ is a scheme with base matrices $B^0, B^1, \ldots, B^{c-1}$;*
2. *$\alpha(\mathcal{S}) = \alpha(\mathcal{S}')$;*
3. *For any fixed weight w, we have that $\mu^{C^j}(w,i,j)$ is constant with respect to any $i \in I_w^n$ and any color j;*
4. *For any fixed weight w, we have that $\mu^{C^j}(w,i,j')$ is constant with respect to any $i \in I_w^n$ and any colors j, j' such that $j \neq j'$.*

Proof. By Lemma 3.3 we can assume, without loss of generality, that scheme $\mathcal{S}$ is a base matrices scheme such that, in any base matrix, for any fixed w, j, j', we have that $\mu^{C^j}(w,i,j')$ is constant with respect to i.

Let $C^0, C^1, \ldots, C^{c-1}$, be the base matrices of scheme $\mathcal{S}$. Let $\sigma_1, \sigma_2, \ldots, \sigma_{c!}$ be all the possible permutations of the set $\{0, 1, \ldots, c-1\}$. Let $C^j_{\sigma_z}$ be the matrix C^j obtained by permuting the colors according to the permutation σ_z. Construct a new scheme $\mathcal{S}'$ having the following base matrices:

$$B^j = C^{\sigma_1^{-1}(j)}_{\sigma_1} \circ C^{\sigma_2^{-1}(j)}_{\sigma_2} \circ \cdots \circ C^{\sigma_{c!}^{-1}(j)}_{\sigma_{c!}}, \text{ for each } j = 0, 1, \ldots, c-1.$$

Observe that by Lemma 3.4, matrix $C^{\sigma_z^{-1}(j)}_{\sigma_z}$ is a base matrix for color i for a scheme having $h = h(\mathcal{S})$, $\ell = \ell(\mathcal{S})$ and $m = m(\mathcal{S})$. Using this observation, we can prove that scheme $\mathcal{S}'$ satisfies the contrast property. Indeed, for any qualified set of participants X, we have that:

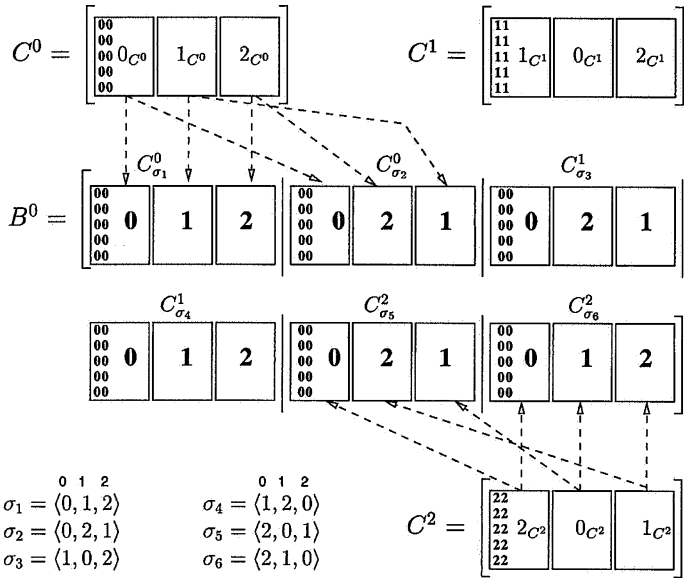

Figure 1. Example used in the proof of Lemma 3.5.

1. $w_j(\mathrm{gor}(B^j|X)) \geqslant h'$ where $h' = c! \cdot h(\mathscr{S})$, because each matrix $C_{\sigma_z}^{\sigma_z^{-1}(j)}$ satisfies, by definition, $w_j(\mathrm{gor}(C_{\sigma_z}^{\sigma_z^{-1}(j)}|X)) \geqslant h(\mathscr{S})$;
2. For $j' \neq j$, $w_{j'}(\mathrm{gor}(B|X)) \leq \ell'$ where $\ell' = c! \cdot \ell(\mathscr{S})$ because each matrix $C_{\sigma_j}^{\sigma_1^{-1}(j')}$ satisfies, by definition, $w_{j'}(\mathrm{gor}(C_{\sigma_z}^{\sigma_z^{-1}(j')}|X)) \leq \ell(\mathscr{S})$.

Scheme $\mathscr{S}'$ satisfies the security property. Indeed, let X be a forbidden set of participants. Let j' and j'' be two colors. We have that $B^{j'}|X = C_{\sigma_1}^{j'}|X \circ C_{\sigma_2}^{j'}|X \circ \cdots \circ C_{\sigma_{c!}}^{j'}|X$ and $B^{j''}|X = C_{\sigma_1}^{j''}|X \circ C_{\sigma_2}^{j''}|X \circ \cdots \circ C_{\sigma_{c!}}^{j''}|X$. For the security property of $\mathscr{S}$, for all $z = 1, 2, \ldots, c!$, matrices $C_{\sigma_z}^{j'}|X$ and $C_{\sigma_z}^{j''}|X$ are the same up to permutation of the columns. Hence matrices $B^{j'}|X$ and $B^{j''}|X$, for any j' and j'', are the same up to a permutation of the columns. Thus the security property holds also for $\mathscr{S}'$.

We have that

$$\alpha(\mathscr{S}') = \frac{h(\mathscr{S}') - \ell(\mathscr{S}')}{m(\mathscr{S}')} = \frac{c! \cdot h(\mathscr{S}) - c! \cdot \ell(\mathscr{S})}{c! \cdot m(\mathscr{S})} = \alpha(\mathscr{S}').$$

To complete the proof, we need to prove properties 3 and 4. These properties derive from the construction. To help the reader understand the argument we will refer to Figure 1, where a schematic construction of B^0 for the case of $c = 3$ is shown.

We are interested in computing $\mu^{B^j}(w,i,k)$. In the following, for the sake of simplicity, we assume that $j=0$, but the reasoning is valid for any j.

Recall that $B^0 = C_{\sigma_1}^{\sigma_1^{-1}(0)} \circ C_{\sigma_2}^{\sigma_2^{-1}(0)} \circ \cdots \circ C_{\sigma_{c!}}^{\sigma_{c!}^{-1}(0)}$. Observe that in the construction of B^0 we use $(c-1)!$ times each of the base matrices $C^0, C^1, \ldots, C^{c-1}$, and every time we use base matrix $C^{j'}$, the primary color j' is mapped to color (j which is) 0. In Figure 1, we use each matrix C^0, C^1 and C^2 exactly 2 times each since $c=3$; for example, in permutations σ_5 and σ_6 we use matrix C^2 since for these permutations color 2 is mapped to 0.

$$\mu^{B^0}(w,i,0) = \overbrace{\mu^{C^0}(w,i,0) + \cdots + \mu^{C^0}(w,i,0)}^{(c-1)!} + \cdots + \overbrace{\mu^{C^{c-1}}(w,i,c-1) + \cdots + \mu^{C^{c-1}}(w,i,c-1)}^{(c-1)!}$$

This number does not depend on 0, i.e., does not depend on j, hence it is the same for any B^j. This proves Property 3. Property 4 follows from the observation that the $(c-1)!$ times that we use a particular base matrix $C^{j'}$ (mapping the primary color j' to 0), all other colors are mapped to each other in all possible ways. In the example of Figure 1, we have only 2 other colors that are mapped in the 2 possible ways. For example, for matrix C^0 and permutations σ_1 and σ_2, the primary color 0 is mapped to 0; in σ_1 color 1 is mapped to color 1 and color 2 is mapped to color 2 while in σ_2 color 1 is mapped to color 2 and color 2 is mapped to color 1. The dotted arrows in Figure 1 show this mapping (the mapping is shown for C^0 and for C^2).

Hence, we have that

$$\begin{aligned}\mu^{B^0}(w,i,1) = {} & (c-1)!\cdot(\mu^{C^0}(w,i,1) + \mu^{C^0}(w,i,2) + \cdots + \mu^{C^0}(w,i,c-1)) \\ & + (c-1)!\cdot(\mu^{C^1}(w,i,0) + \mu^{C^1}(w,i,2) + \cdots + \mu^{C^1}(w,i,c-1)) \\ & + \cdots \\ & + (c-1)!\cdot(\mu^{C^{c-1}}(w,i,0) + \mu^{C^{c-1}}(w,i,1) + \cdots + \mu^{C^{c-1}}(w,i,c-2))\end{aligned}$$

However, if we compute $\mu^{B^0}(w,i,2)$ it will be the same as $\mu^{B^0}(w,i,1)$, and this is equal to $\mu^{B^0}(w,i,j')$ for any color $j' \neq 0$. Hence we have Property 4. ■

We refer to schemes satisfying Lemma 3.5 as *canonical* schemes. When finding a contrast optimal scheme we can restrict our attention only to canonical schemes: Indeed Lemma 3.5 guarantees that there exists a canonical scheme with optimal contrast.

Given the symmetry properties of a canonical scheme, in such a scheme there is no distinction among two secondary colors in the sense that if in a base matrix for primary color j there is a column for a secondary color j_1, then the base matrix also has the same column for any other secondary color j_2. Formally, we have that $\mu^{B^j}(w,i,j_1) = \mu^{B^j}(w,i,j_2)$ for any $j_1, j_2 \neq j$. Moreover, we also have that the position of the black color $\star$ is irrelevant in the sense that we have $\mu^{B^j}(w,i,j') = \mu^{B^j}(w,i',j')$ for any $i, i' \in I_w$. Finally we have that all these properties are valid

for any base matrix. It is also true that the number of columns of the same weight for the primary color is the same in all base matrices, that is $\mu^{B^j}(w,i,j) = \mu^{B^{j'}}(w,i,j')$, for any j and j'. Hence, to characterize a canonical scheme, we give the following definition.

Definition 3.6. In a canonical scheme we define the multiplicities $\mu(p,w)$ and $\mu(s,w)$ as follows:

- $\mu(p,w)$ is the number of columns having exactly w entries equal to the primary color, in any arbitrary but fixed positions, and the remaining ones equal to $\star$; Formally, $\mu(p,w) = \mu^{B^j}(w,i,j)$, for any i,j. This is well defined because of Property 3 of Lemma 3.5.
- $\mu(s,w)$ is the number of columns having exactly w entries equal to the secondary color, in any arbitrary but fixed positions, and the remaining ones equal to $\star$; Formally, $\mu(s,w) = \mu^{B^j}(w,i,j')$, for any i,j,j' such that $j' \neq j$. This is well defined because of Property 4 of Lemma 3.5.

In order to find the canonical scheme with optimal contrast, we will formulate a linear programming problem. The next lemma provides the objective function and the constraints used in this formulation.

LEMMA 3.7. *A set of integers* $\{\mu(p,r), \mu(s,r) | r = 0,1,\ldots,n\}$ *is the set of multiplicities of a c-color* (k,n)*-threshold scheme with pixel expansion* m *and contrast* α *if and only if the following properties are satisfied:*

1. $\sum_{r=0}^{n} \mu(p,r)\binom{n}{r} + (c-1)\sum_{r=0}^{n} \cdot \mu(s,r)\binom{n}{r} = m$
2. $\sum_{r=q}^{n-q+q'} \binom{n-q}{r-q'}(\mu(p,r) - \mu(s,r)) = 0$ *for any* q, q' *such that* $1 \leqslant q' \leqslant q \leqslant k-1$
3. $\sum_{r=0}^{n-k} \binom{n-k}{r}(\mu(p,k+r) - \mu(s,k+r)) = \alpha \cdot m$

Proof. We start by assuming that $\{\mu(p,r), \mu(s,r) | r = 0,1,\ldots,n\}$ are the multiplicities of a c-color (k,n)-threshold scheme with pixel expansion m and contrast α and we prove that Properties 1–3 are true.

The pixel expansion m is given by the number of columns in any base matrix. Fix a base matrix; the number of columns containing the primary color is $\sum_{r=0}^{n} \mu(p,r)\binom{n}{r}$, while for each of the secondary colors the number of columns in the base matrix is $\sum_{r=0}^{n} \cdot \mu(s,r)\binom{n}{r}$. Hence Property 1 holds.

Next, we prove Property 2. Let $C^0, C^1, \ldots, C^{c-1}$ be the base matrices of the scheme. Fix a color j and consider a column ϕ^q of size q, where $1 \leqslant q \leqslant k-1$ consisting of entries of color j and $\star$. Let $q' = w_j(\phi^q)$, that is the Hamming weight

of ϕ^q with respect to color j. Fix q rows of matrices $C^0, C^1, \ldots, C^{c-1}$. For the sake of simplicity, consider the first q rows, but the reasoning is valid for any q rows. Let X be the set of integers corresponding to these rows, that is $X = \{1, 2, \ldots, q\}$. For $j' = j$ the multiplicity of ϕ^q in $C_j|X$, is $\sum_{r=q}^{n-q+q'} \binom{n-q}{r-q'} \mu(p, r)$. Indeed, in a column of weight r in C^j, $r - q'$ entries of color j can be placed in the last $n - q$ rows in $\binom{n-q}{r-q'}$ ways. Similarly, for $j' \neq j$, the multiplicity of ϕ^q in $C_{j'}|X$ is $\sum_{r=q}^{n-q+q'} \binom{n-q}{r-q'} \mu(s, r)$.

To satisfy the security property, the above quantities must be equal, and thus Property 2 holds.

Now, we prove Property 3. Let X be a qualified set of participants. Fix a color i and consider the matrix $M = C^i|X$, where C^i is the base matrix for color i. The $\mathrm{gor}(M)$ contains

$$\sum_{r=0}^{n-k} \binom{n-k}{r} \mu(p, k+r)$$

pixels of the primary color i and

$$\sum_{r=0}^{n-k} \binom{n-k}{r} \mu(s, k+r)$$

pixels of any secondary color j.

By the contrast property it must hold that

$$\sum_{r=0}^{n-k} \binom{n-k}{r} (\mu(p, k+r) - \mu(s, k+r)) = \alpha \cdot m.$$

Now assume that Properties 1–3 are true. We have to prove that $\{\mu(x, r)|x = \text{“}p\text{”}, \text{“}s\text{”} \text{ and } r = 0, 1, \ldots, n\}$ are the multiplicities of a c-color (k, n)-threshold scheme with pixel expansion m and contrast α. By property 1, we have that the pixel expansion is m. By Property 2, we have that the security property is satisfied and by Property 3 we have that the contrast property is satisfied and that the contrast is α. ■

Using Lemma 3.7 we can formulate the problem of finding the optimal contrast of a canonical c-color (k, n)-threshold scheme in terms of a linear programming problem. We define the following variables: $x_i = \mu(p, i)/m$ and $y_i = \mu(s, i)/m$ for $i = 0, 1, \ldots, n$. Properties 1–3 of Lemma 3.7 give the following linear programming problem.

Maximize:

$$\alpha = \sum_{r=0}^{n-k} \binom{n-k}{r} (x_{k+r} - y_{k+r})$$

Subject to:

$$\sum_{r=0}^{n} x_r \binom{n}{r} + \sum_{r=0}^{n} (c-1) \cdot y_r \binom{n}{r} = 1$$

$$\sum_{r=q'}^{n-q+q'} \binom{n-q}{r-q'} (x_r - y_r) = 0 \quad \text{for any } q, q' \quad \text{such that}$$

$$1 \le q' \le q \le k-1$$

Notice that since the coefficients of the above linear programming problem are rational numbers (actually, they are integers), the values of the x_i's and the y_i's of an optimal solution are also rational numbers. Hence, given an optimal solution to the above linear programming problem, it is always possible to find a suitable m in order to get the μ's and thus a scheme with optimal contrast.

EXAMPLE 3.8. *The following linear programming problem is for the 3-color (3,4)-threshold canonical scheme with optimal contrast.*

Maximize:

$$\alpha = x_3 + x_4 - y_3 - y_4$$

Subject to:

$$x_0 + 4x_1 + 6x_2 + 4x_3 + x_4 + 2y_0 + 8y_1 + 12y_2 + 8y_3 + 2y_4 = 1$$
$$x_1 + 3x_2 + 3x_3 + x_4 - y_1 - 3y_2 - 3y_3 - y_4 = 0$$
$$x_1 + 2x_2 + x_3 - y_1 - 2y_2 - y_3 = 0$$
$$x_2 + 2x_3 + x_4 - y_2 - 2y_3 - y_4 = 0$$

The solution to the above linear programming problem gives $x_1 = y_3 = 1/14$, $x_4 = 2/14$, *all other variables equal to 0 and* $\alpha = 1/14$. *Setting* $m = 14$ *we obtain* $\mu(p,4) = 2, \mu(p,1) = 1, \mu(s,3) = 1$ *and the remaining* μ*'s equal to 0. The base matrices of the corresponding 3-color (3,4)-threshold canonical scheme are:*

$$C^0 = \begin{bmatrix} 0\,0\,1\,1\,1\,\star\,2\,2\,2\,\star\,\star\,\star\,0 \\ 0\,0\,1\,1\,\star\,1\,2\,2\,\star\,2\,\star\,\star\,0\,\star \\ 0\,0\,1\,\star\,1\,1\,2\,\star\,2\,2\,\star\,0\,\star\,\star \\ 0\,0\,\star\,1\,1\,1\,\star\,2\,2\,2\,0\,\star\,\star\,\star \end{bmatrix}$$

$$C^1 = \begin{bmatrix} 1\,1\,0\,0\,0\,\star\,2\,2\,2\,\star\,\star\,\star\,1 \\ 1\,1\,0\,0\,\star\,0\,2\,2\,\star\,2\,\star\,\star\,1\,\star \\ 1\,1\,0\,\star\,0\,0\,2\,\star\,2\,2\,\star\,1\,\star\,\star \\ 1\,1\,\star\,0\,0\,0\,\star\,2\,2\,2\,1\,\star\,\star\,\star \end{bmatrix}$$

Table 1. Optimal contrast values α obtained resolving the linear programming problem given above.

	n											
	3		4		5		6		7		8	
k	α	m	α	m	α	m	α	m	α	m	α	m
2	1/7	**7**(8)	2/15	15(11)	1/8	24(14)	3/25	50(17)	2/17	85(18)	16/133	133(20)
3	1/10	10(10)	1/14	**14**(18)	1/8	**18**(24)	1/20	60(30)	4/87	87(36)	5/119	119(42)
4	–	–	1/23	23(23)	1/42	**42**(45)	1/50	100(72)	3/190	190(105)	2/145	435(144)
5	–	–	–	–	1/46	46(46)	1/84	**84**(90)	1/132	**132**(144)	1/152	304(210)
6	–	–	–	–	–	–	1/95	95(95)	1/206	**206**(210)	2/579	579(384)
7	–	–	–	–	–	–	–	–	1/190	190(190)	1/412	**412**(420)
8	–	–	–	–	–	–	–	–	–	–	1/511	511(511)

The corresponding pixel expansion m are compared with the pixel expansion [8], which is reported in parentheses.

$$C^2 = \begin{bmatrix} 2\,2\,0\,0\,0\,\star\,1\,1\,1\,\star\,\star\,\star\,\star\,2 \\ 2\,2\,0\,0\,\star\,0\,1\,1\,\star\,1\,\star\,\star\,2\,\star \\ 2\,2\,0\,\star\,0\,0\,1\,\star\,1\,1\,\star\,2\,\star\,\star \\ 2\,2\,\star\,0\,0\,0\,\star\,1\,1\,1\,2\,\star\,\star\,\star \end{bmatrix}$$

■

Table 1 shows the optimal contrast values α and the corresponding values for the pixel expansion m obtained as solutions to the above linear programming problem, for the cases $k = 2, \ldots, 7$ and $k \leqslant n \leqslant 8$ and $c = 3$. It is worth to notice that, in some cases (reported in boldface in Table 1), the canonical schemes have better pixel expansion than the schemes proposed in [8], which in turn improved on the ones in [7].

4. Contrast-optimal (n, n)-Threshold Schemes and Optimal Pixel Expansion

In this section, we deal with the case $k = n$, for any $n \geq 2$. We first compute the optimal contrast and then use this result to prove a lower bound on the pixel expansion. The arguments used in the proof provide also a construction of schemes that achieve the lower bound on the pixel expansion. It turns out that these schemes are the same as the ones of [8]. Hence, we also prove that the schemes of [8] are optimal with respect to the pixel expansion.

The next lemma provides crucial properties of contrast-optimal schemes.

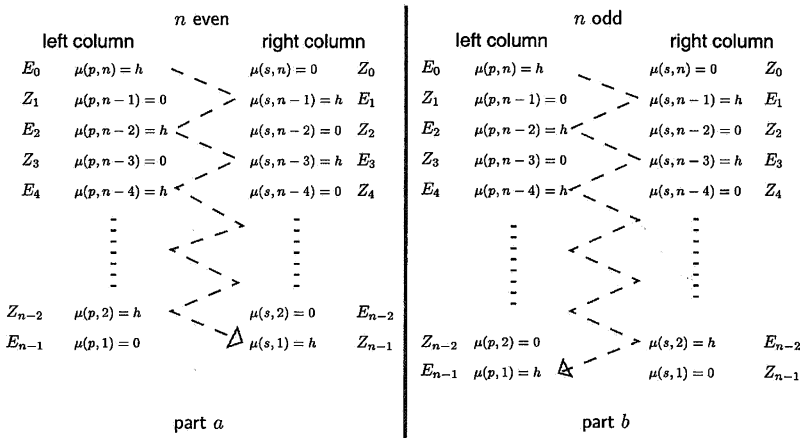

Figure 2. Submatrices R^i_j.

LEMMA 4.1. *For a canonical c-color (n, n)-threshold scheme $\mathscr{S}$ with optimal contrast, the following properties hold for $i = 0, 1, \ldots, \lfloor n/2 \rfloor$:*

1. $\mu(s, n-2i) = 0$,
2. $\mu(s, n-2i-1) = \mu(p, n)$
3. $\mu(p, n-2i-1) = 0$
4. $\mu(p, n-2i-2) = \mu(p, n)$. *Moreover* $\mu(p, n) = h(\mathscr{S})$.

Proof. Let $C^0, \ldots, C^{n-1}$ be the base matrices of scheme $\mathscr{S}$ and let $h = h(\mathscr{S})$. Assume that n is even and refer to Figure 2 part *a*; the figure provides an alternative way of looking at all the equations specified in Properties 1–4 of the lemma. Notice that for n odd the only thing that changes is the last equation in the sequence (see Figure 2 part *b*), but the reasoning is exactly the same, so we will only consider the case n even.

Let us first look at the equations on the dotted path in the figure; we have labeled these equations $E_0, \ldots, E_{n-1}$. We proceed by induction on the equation subscript number. The base case is equation E_0. Equation E_0 is $\mu(p, n) = h$ and this is true because each column consisting of n elements equal to the primary color reconstructs a pixel of the primary color for a qualified set of participants. Now assume that equation E_i is true, we need to prove that equation E_{i+1} is true. There are two possible cases: one is that equation E_i is in the left column, and the other is that equation E_i is in the right column (the reasoning however is the same). Let us consider the case when the equation is on the left column. This means that equation E_i is $\mu(p, n-i) = h$ and equation E_{i+1} is $\mu(s, n-i-1) = h$. By the inductive hypothesis we assume that $\mu(p, n-i) = h$. We need to prove that $\mu(s, n-i-1) = h$. This is true by the security property. Indeed consider a color j_1. Since $\mu(p, n-i) = h > 0$, matrix C^{j_1} contains h copies of column $\Psi(n-i, z, j_1)$, for any $z \in I_{n-1}$. Fix one such column ϕ (the reasoning applies to any column). A forbidden set must not be able to distinguish matrix C^{j_1} from another matrix C^{j_2}, for $j_2 \neq j_1$. This means that in C^{j_2} we

need to have all the columns that we can obtain by not considering one element equal to j_1 of ϕ, that is by substituting one element of ϕ with the special color $\star$. The columns so obtained consists of $n-i-1$ elements equal to j_1 and the remaining ones equal to $\star$. There are $\mu(p, n-i)$ such columns, hence $\mu(s, n-i-1)=\mu(p, n-i)$ and thus $\mu(s, n-i-1)=h$. The case when equation E_i is in the right column is symmetric (exchange p with s) and thus the proof is similar.

It remains to prove the equations of Figure 2 that are labeled with $Z_0, \ldots, Z_{n-1}$. For any $i=0, \ldots, n-1$ equation Z_i can be proved from equation E_i by using the following general argument: if a column is present in all base matrices, then it can be deleted from all base matrices obtaining a scheme with a better contrast. So, let us assume that equation E_i is true, we need to prove that equation Z_i is true. Again, we need to consider the two cases, one, where E_i is in the left column and the other where E_i is in the right column. Let us consider the case, when E_i is in the right column. Equation E_i is $\mu(s, n-i)=h$. Assume by contradiction that $\mu(p, n-i)=r$, with $r>0$. This means that any base matrix has columns with weight $n-i$ both for the primary color and for the secondary colors, which implies that these columns are present in all base matrices. The are $\min\{r, h\}$ such columns that can be deleted from all base matrices obtaining a scheme with a better contrast, which is impossible since the scheme we have started with, has optimal contrast. Hence it must be $\mu(p, n-i)=0$. The case when E_i is in the left column is symmetric and thus the proof is similar. ■

We are now able to compute the optimal contrast. In such a computation we will use the following equality. For any $n \geq 2$,

$$\sum_{s=0}^{n-1}(-1)^s \binom{n}{n-s} = (-1)^{n-1} \tag{1}$$

The above equality is derived from the following well known equality ([4], page 165), which holds for any integers, r, z, with $r > z$:

$$\sum_{s=0}^{z}\binom{r}{s}(-1)^s = (-1)^z \binom{r-1}{z}.$$

For $z=n-1$ and $r=n$, and using $\binom{n}{k}=\binom{n}{n-k}$ the above equality becomes (1).

LEMMA 4.2. *The optimal contrast of a c-color (n, n)-threshold scheme is*

$$\alpha_{\text{opt}} = \begin{cases} \frac{1}{c\cdot 2^{n-1}-1}, & \text{if } n \text{ is even} \\ \frac{1}{c\cdot 2^{n-1}-c+1}, & \text{if } n \text{ is odd} \end{cases}$$

Proof. Let $\mathcal{S}$ be a canonical c-color (n, n)-threshold scheme with optimal contrast. Let $m_{\alpha_{\text{opt}}} = m(\mathcal{S}), h_{\text{opt}} = h(\mathcal{S}), \ell_{\text{opt}} = \ell(\mathcal{S})$, and $\alpha_{\text{opt}} = \alpha(\mathcal{S})$.

By definition we have that $\alpha_{\text{opt}} = (h_{\text{opt}} - \ell_{\text{opt}})/(m_{\alpha_{\text{opt}}})$. By Lemma 4.1 we have that $\ell_{\text{opt}} = 0$ and since by definition we have $h_{\text{opt}} = \mu(p, n)$, it follows that

$$\alpha_{\text{opt}} = \frac{\mu(p, n)}{m_{\alpha_{\text{opt}}}}. \tag{2}$$

Next we compute $m_{\alpha_{\text{opt}}}$ and then we plug in the obtained value in the preceding equation in order to get the theorem.

By definition of the μ's we have that

$$m_{\alpha_{\text{opt}}} = \sum_{z=1}^{n} (\mu(p, z) + (c-1)\mu(s, z)) \binom{n}{z}$$

Using Lemma 4.1, we can rewrite $m_{\alpha_{\text{opt}}}$ as

$$\begin{aligned} m_{\alpha_{\text{opt}}} = \mu(p, n) \Bigg[&\binom{n}{n} + (c-1)\binom{n}{n-1} + \binom{n}{n-2} + (c-1)\binom{n}{n-3} \\ &+ \cdots + (c-1)^{(n-1) \bmod 2} \binom{n}{1} \Bigg] \end{aligned} \tag{3}$$

Next, we distinguish the two possible cases: n even and n odd. The proofs are similar but a few details change so for the sake of an easy reading we provide the two cases separately.

Case n even. We have that:

$$\sum_{j=0}^{n/2-1} \binom{n}{2j+1} = 2^{n-1} \tag{4}$$

Indeed, using the known equality $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ we have that:

$$\begin{aligned} \sum_{j=0}^{n/2-1} \binom{n}{2j+1} &= \sum_{j=0}^{n/2-1} \left[\binom{n-1}{2j+1} + \binom{n-1}{2j} \right] \\ &= \sum_{j=0}^{n-1} \binom{n-1}{j} = 2^{n-1} \end{aligned}$$

Since n is even, Equation (3) can be written as

$$\begin{aligned} m_{\alpha_{\text{opt}}} &= \mu(p, n) \left(\binom{n}{n} + c\binom{n}{n-1} - \binom{n}{n-1} + \binom{n}{n-2} + \cdots + \binom{n}{2} + c\binom{n}{1} - \binom{n}{1} \right) \\ &= \mu(p, n) \left(\sum_{s=0}^{n-1} (-1)^s \binom{n}{n-s} + c \sum_{s=0}^{n/2-1} \binom{n}{n-(2s+1)} \right) \end{aligned}$$

By using (1) we have

$$m_{\alpha_{\text{opt}}} = \mu(p,n)\left((-1)^{n-1} + c\cdot\sum_{s=0}^{n/2-1}\binom{n}{n-(2s+1)}\right)$$

By using (4) we have that

$$m_{\alpha_{\text{opt}}} = \mu(p,n)(-1+c2^{n-1})$$

By plugging in the above value of $m_{\alpha_{\text{opt}}}$ in Equation (2) we have the Lemma for the case of n even.

Case n odd. We have that

$$\sum_{j=0}^{\frac{n-1}{2}-1}\binom{n}{2j+1} = 2^{n-1}-1 \tag{5}$$

Indeed, using the known equality $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ we have that:

$$\begin{aligned}\sum_{j=0}^{\frac{n-1}{2}-1}\binom{n}{2j+1} &= \sum_{j=0}^{\frac{n-1}{2}-1}\left[\binom{n-1}{2j+1}+\binom{n-1}{2j}\right]\\ &= \sum_{j=0}^{n-2}\binom{n-1}{j} = 2^{n-1}-1\end{aligned}$$

Since n is odd, equation (3) can be written as

$$\begin{aligned}m_{\alpha_{\text{opt}}} &= \mu(p,n)\left(\binom{n}{n}+c\binom{n}{n-1}-\binom{n}{n-1}+\binom{n}{n-2}+\cdots+c\binom{n}{2}-\binom{n}{2}+\binom{n}{1}\right)\\ &= \mu(p,n)\left(\sum_{s=0}^{n-1}(-1)^s\binom{n}{n-s}+c\sum_{s=0}^{\frac{n-1}{2}-1}\binom{n}{n-(2s+1)}\right)\end{aligned}$$

By using (1) we have

$$m_{\alpha_{\text{opt}}} = \mu(p,n)\left((-1)^{n-1} + c\cdot\sum_{s=0}^{\frac{n-1}{2}-1}\binom{n}{n-(2s+1)}\right)$$

By using (5) we have

$$m_{\alpha_{\text{opt}}} = \mu(p,n)(1+c(2^{n-1}-1))$$

By plugging in the above value of $m_{\alpha_{\text{opt}}}$ in Equation (2) we have the Lemma for the case of n odd. ■

Finally, we are able to provide a lower bound on the pixel expansion.

THEOREM 4.3. *The pixel expansion of a c-color (n, n)-threshold scheme, for any c, $n \geqslant 2$, is lower bounded by*

$$m \geqslant \begin{cases} c \cdot 2^{n-1} - 1, & \text{if } n \text{ is even} \\ c \cdot 2^{n-1} - c + 1, & \text{if } n \text{ is odd} \end{cases}$$

Proof. Let α_{opt} be the contrast of a contrast-optimal c-color (n, n)-threshold scheme. Since for any c-color (n, n)-threshold scheme with contrast α, it holds that $\alpha \geqslant 1/m$ and $\alpha \leqslant \alpha_{\text{opt}}$, we have that $m \geqslant 1/\alpha_{\text{opt}}$. The lemma follows from Lemma 4.2. ■

Lemma 4.1 gives also a construction method for c-color (n, n)-threshold schemes. Indeed, once we have fixed an arbitrary value for $\mu(p, n)$, Lemma 4.1 gives the values for all other multiplicities of the scheme. In order to get the best pixel expansion we choose $\mu(p, n) = 1$. For such a choice, we can give the following construction of a c-color (n, n)-threshold. Such a scheme has optimal pixel expansion.

CONSTRUCTION 4.4. *The base matrices of a c-color (n, n)-threshold scheme with optimal pixel expansion can be constructed as follows. Fix any color i; base matrix C^i consists of the following columns:*

1. for $r = 0, 1, \ldots, \lceil n/2 \rceil - 1$ include the $\binom{n}{2r}$ columns having $2r$ entries equal to $\star$ and the remaining ones of color i;
2. for any color $j \neq i$, for $r = 0, 1, \ldots, \lceil \frac{n-1}{2} \rceil - 1$ include the $\binom{n}{2r-1}$ columns having $2r - 1$ entries equal to $\star$ and the remaining ones of color j;

EXAMPLE 4.5. *For $c = 3$ and $n = 4$ the base matrices of the scheme obtained with Construction 4.4 are provided below. For such a scheme $m = 23$ and $\alpha = 1/23$.*

$$C^0 = \begin{bmatrix} 0\,1\,1\,1\,\star\,2\,2\,2\,\star\,\star\,0\,0\,\star\,0\,\star\,\star\,\star\,\star\,1\,\star\,\star\,\star\,2 \\ 0\,1\,1\,\star\,1\,2\,2\,\star\,2\,\star\,0\,\star\,0\,\star\,0\,\star\,\star\,1\,\star\,\star\,\star\,2\,\star \\ 0\,1\,\star\,1\,1\,2\,\star\,2\,2\,0\,\star\,0\,\star\,\star\,0\,\star\,1\,\star\,\star\,\star\,2\,\star\,\star \\ 0\,\star\,1\,1\,1\,\star\,2\,2\,2\,0\,\star\,\star\,0\,0\,\star\,1\,\star\,\star\,\star\,2\,\star\,\star\,\star \end{bmatrix}$$

$$C^1 = \begin{bmatrix} 1\,0\,0\,0\,\star\,2\,2\,2\,\star\,\star\,1\,1\,\star\,1\,\star\,\star\,\star\,\star\,0\,\star\,\star\,\star\,2 \\ 1\,0\,0\,\star\,0\,2\,2\,\star\,2\,\star\,1\,\star\,1\,\star\,1\,\star\,\star\,0\,\star\,\star\,\star\,2\,\star \\ 1\,0\,\star\,0\,0\,2\,\star\,2\,2\,1\,\star\,1\,\star\,\star\,1\,\star\,0\,\star\,\star\,\star\,2\,\star\,\star \\ 1\,\star\,0\,0\,0\,\star\,2\,2\,2\,1\,\star\,\star\,1\,1\,\star\,0\,\star\,\star\,\star\,2\,\star\,\star\,\star \end{bmatrix}$$

$$C^2 = \begin{bmatrix} 2\,0\,0\,0\,\star\,1\,1\,1\,\star\,\star\,2\,2\,\star\,2\,\star\,\star\,\star\,\star\,0\,\star\,\star\,\star\,1 \\ 2\,0\,0\,\star\,0\,1\,1\,\star\,1\,\star\,2\,\star\,2\,\star\,2\,\star\,\star\,0\,\star\,\star\,\star\,1\,\star \\ 2\,0\,\star\,0\,0\,1\,\star\,1\,1\,2\,\star\,2\,\star\,\star\,2\,\star\,0\,\star\,\star\,\star\,1\,\star\,\star \\ 2\,\star\,0\,0\,0\,\star\,1\,1\,1\,2\,\star\,\star\,2\,2\,\star\,0\,\star\,\star\,\star\,1\,\star\,\star\,\star \end{bmatrix}$$

5. Construction of $(2, n)$ Threshold Schemes

In this section, we describe a new technique to construct c-color $(2, n)$-threshold schemes. The pixel expansion of our schemes is better than that of the schemes in [7,8].

Let us start by making some considerations on the structure of the base matrices $C^i, i = 0, 1, \ldots, c-1$, describing a $(2, n)$-threshold schemes. In any base matrix C^i we can identify c portions (submatrices), each corresponding to color j, for $j = 0, 1, \ldots, i, \ldots, c-1$, and consisting of all the columns that contain color j and possibly $\star$, i.e., columns equal to $\Psi(w, i', j)$ for some weight w, and $i' \in I_w^n$. Let us denote those submatrices by R_j^i. Figure 3 provides a schematic representation of such submatrices.

The construction we propose relies on the observation that the rows of the submatrices $R_j^i, j \neq i$, of C^i represent a Sperner family. A Sperner family $\mathcal{SF}$ over a ground set G is a family $\mathcal{SF} = \{A_1, \ldots, A_t\}$ of subsets of G such that A_j is not a subset of A_i for $i \neq j$ (for more information see [5]). Let $G = \{g_1, \ldots, g_{m_j}\}$ be a ground set of m_j elements. Each row $r, r = 1, 2, \ldots, n$, of R_j^i represents the subset $A_r = \{g_q | R_j^i(r, q) = j\}$ of G. To satisfy the security property, any two rows of R_j^i must contain the patterns $\left[\begin{smallmatrix} j \\ \star \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} \star \\ j \end{smallmatrix}\right]$ and thus the subsets A_r constitute a Sperner family over the ground set G. Therefore, the rows of R_j^i correspond to a Sperner family and thus we can construct the matrices R_j^i starting from Sperner families.

Next we provide a construction for $(2, n)$-threshold schemes, for $n \geq 2$.

CONSTRUCTION 5.1. *Let b be an integer $1 \leqslant b \leqslant n$, and let $s = \min\{s' : \binom{s'}{b} \geq n, 1 \leq s' \leq n\}$. Let $G = \{g_1, \ldots, g_s\}$ be a ground set of cardinality s. Let $\mathcal{SF} = \{A_1, \ldots, A_{\binom{s}{b}}\}$ be the Sperner family whose elements are all the subsets of G of size b. Let $B_1, \ldots, B_n$ be any n elements of $\mathcal{SF}$.*

For each $i = 0, 1, \ldots, c-1$, the constructions of the base matrices C^i are:

- *R_i^i consists of b columns with all i's, i.e., columns equal to $\Psi(n, 2^n - 1, i)$, and*
- *R_j^i has, for $r = 1, \ldots, n$ and $q = 1, \ldots, s$*

$$\begin{array}{cccc} & & R_i^i & \\ \end{array} \quad \begin{array}{ccc} & R_0^i & \end{array} \qquad \begin{array}{ccc} & R_{i-1}^i & \end{array} \quad \begin{array}{ccc} & R_{i+1}^i & \end{array} \qquad \begin{array}{ccc} & R_{c-1}^i & \end{array}$$

$$C^i = \left[\begin{array}{cccc|ccc|cc|ccc|ccc|cc|ccc}
i & \cdots & i & \cdots & \star & 0 & \cdots & \cdots & \cdots & i-1 & i-1 & \cdots & i+1 & \star & \cdots & \cdots & \cdots & \star & c-1 & \cdots \\
i & \cdots & \star & \cdots & 0 & 0 & \cdots & \cdots & \cdots & \star & i-1 & \cdots & i+1 & i+1 & \cdots & \cdots & \cdots & c-1 & \star & \cdots \\
i & \cdots & i & \cdots & 0 & \star & \cdots & \cdots & \cdots & \star & i-1 & \cdots & \star & \star & \cdots & \cdots & \cdots & c-1 & c-1 & \cdots \\
i & \cdots & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
i & \cdots & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
i & \cdots & \star & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & i-1 & \star & \cdots & \star & i+1 & \cdots & \cdots & \cdots & \star & \star & \cdots \\
i & \cdots & i & \cdots & 0 & \star & \cdots & \cdots & \cdots & \star & \star & \cdots & i+1 & \star & \cdots & \cdots & \cdots & c-1 & c-1 & \cdots \\
i & \cdots & i & \cdots & \star & 0 & \cdots & \cdots & \cdots & i-1 & i-1 & \cdots & i+1 & i+1 & \cdots & \cdots & \cdots & c-1 & \star & \cdots
\end{array}\right]$$

$$\underbrace{\qquad\qquad}_{m_i} \quad \underbrace{\qquad\qquad}_{m_0} \qquad\qquad \underbrace{\qquad\qquad}_{m_{i-1}} \quad \underbrace{\qquad\qquad}_{m_{i+1}} \qquad\qquad \underbrace{\qquad\qquad}_{m_{c-1}}$$

Figure 3. Equations of Lemma 4.1.

$$R_j^i(r,q)=\begin{cases} j, & if g_q \in B_r \\ \star, & otherwise \end{cases}$$

THEOREM 5.2. *Construction* 5.1 *gives a c-color* $(2,n)$*-threshold scheme with pixel expansion* $m=b+(c-1)\cdot s$

Proof. Let us fix the parameter b and construct the matrices $C^0, C^1, \ldots, C^{c-1}$ according to Construction 5.1.

Let us first prove that the obtained scheme statisfies the contrast property. Indeed any base matrix C^i has b columns with all entries of color i. Then, for any qualified set $X, |X| \geq 2$, consisting of at least two rows of C^i, it holds that $w_i(\text{gor}(C^i|X)) = b$. For the same X, and for any $j \neq i$, it holds that $w_j(\text{gor}(C^i|X)) \leq b-1)$. Indeed, the rows in $R_j^i|X$ have b entries of color j. Since they represent a Sperner family, any two rows of $R_j^i|X$ must contain the patterns $\left[\begin{smallmatrix} j \\ \star \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} \star \\ j \end{smallmatrix}\right]$ and thus $w_j(\text{gor}(C^i|X)) \leq b-1$. Thus, the contrast property is satisfied for $h=b$ and $\ell=b-1$.

Let us now prove that the scheme $\mathscr{S}$ satisfies the security property. For such a scheme, a forbidden set consists of at most a row of a base matrix C^i. By construction, for each color i, each row of C^i, consists of b entries of color j, $j=0,1,\ldots,i,\ldots,c-1$ and the remaining ones of color $\star$. Hence they are the same up to a permutation of the columns and thus the security property holds. ■

EXAMPLE 5.3. *Let us construct a* 3*-color,* (2,6)*-threshold scheme. Let* $b=2$*, then* $s=4$*. The scheme obtained with Construction* 5.1 *has pixel expansion* $m=2+2\cdot 4=10$ *and the base matrices are shown below.*

$$C^0=\begin{bmatrix} 0\,0\,1\,\star\,1\,\star\,2\,\star\,2\,\star \\ 0\,0\,1\,1\,\star\,\star\,2\,2\,\star\,\star \\ 0\,0\,\star\,1\,1\,\star\,\star\,2\,2\,\star \\ 0\,0\,\star\,\star\,1\,1\,\star\,\star\,2\,2 \\ 0\,0\,1\,\star\,\star\,1\,2\,\star\,\star\,2 \\ 0\,0\,\star\,1\,\star\,1\,\star\,2\,\star\,2 \end{bmatrix}$$

$$C^1=\begin{bmatrix} 1\,1\,0\,\star\,0\,\star\,2\,\star\,2\,\star \\ 1\,1\,0\,0\,\star\,\star\,2\,2\,\star\,\star \\ 1\,1\,\star\,0\,0\,\star\,\star\,2\,2\,\star \\ 1\,1\,\star\,\star\,0\,0\,\star\,\star\,2\,2 \\ 1\,1\,0\,\star\,\star\,0\,2\,\star\,\star\,2 \\ 1\,1\,\star\,0\,\star\,0\,\star\,2\,\star\,2 \end{bmatrix}$$

$$C^2 = \begin{bmatrix} 2\,2\,0\,\star\,0\,\star\,1\,\star\,1\,\star \\ 2\,2\,0\,0\,\star\,\star\,1\,1\,\star\,\star \\ 2\,2\,\star\,0\,0\,\star\,\star\,1\,1\,\star \\ 2\,2\,\star\,\star\,0\,0\,\star\,\star\,1\,1 \\ 2\,2\,0\,\star\,\star\,0\,1\,\star\,\star\,1 \\ 2\,2\,\star\,0\,\star\,0\,\star\,1\,\star\,1 \end{bmatrix}$$

Clearly, the pixel expansion of a scheme obtained with Construction 5.1 depends on the choice of b. As a particular case, it is worth to notice that fixing the parameter $b=1$ we obtain a family of c-color $(2,n)$-threshold schemes, with pixel expansion $m=(c-1)\cdot n+1$. In this case, each base matrix C^i has a very simple structure: R_i^i will have one column with all entries of color i, while for any color j, $j\neq i$, each R_j^i consists of the identity matrix containing color j on the diagonal and $\star$ elsewhere.

Construction 5.1 provides a family of schemes, one for each possible choice of $b, 1\leq b\leq n$. Once fixed a value for b, the pixel expansion of the corresponding scheme is $m=b+(c-1)s$ where $s=\min\{s' : \binom{s'}{b}\geq n, 1\leq s'\leq n\}$.

Since we are interested in optimizing the pixel expansion we can choose the value b that minimizes the resulting pixel expansion m. Table 2 shows the values of such b, together with the corresponding s and the pixel expansion m, for $c=3$ and $n\leq 200$. Table 3 shows the values of the best pixel expansion m obtained by varying b in Construction 5.1 for $n=2,\ldots,8$ participants and $c=3,4,5$ colors.

Table 2. Best values of parameters b and s, and corresponding pixel expansion m.

n	b	s	m
2	1	2	5
3	1	3	7
4	1	4	9
5	2	4	10
6	2	4	10
7–10	2	5	12
11–15	2	6	14
16–20	3	6	15
21	2	7	16
22–35	3	7	17
36–56	3	8	19
57–70	4	8	20
71–84	3	9	21
85–126	4	9	22
127–200	4	10	24

Table 3. Pixel expansion comparison of our construction with [8] and [7].

	$c=3$			$c=4$			$c=5$		
n	Our	[8]	[7]	Our	[8]	[7]	Our	[8]	[7]
2	5	5	9	7	7	12	9	9	15
3	7	8	12	10	11	12	13	14	15
4	9	11	15	13	15	15	17	19	15
5	10	14	21	14	19	21	18	24	21
6	10	17	21	14	23	21	18	29	21
7	12	18	24	17	25	24	22	32	24
8	12	20	27	17	28	27	22	36	27

Moreover the table contains a comparison with the pixel expansion of the schemes proposed in [8,7].

6. Conclusions

We have presented a characterization of contrast-optimal c-color (k, n)-threshold visual cryptography schemes. We have identified a special class of schemes, called *canonical*, that satisfy strong simmetry property. We proved that there exists a canonical scheme achieving optimal contrast. Then we used canonical schemes to provide a constructive proof of optimality, with respect to the pixel expansion, of c-color (n, n)-threshold visual cryptography schemes. Finally, we provided constructions of c-color $(2, n)$-threshold schemes whose pixel expansion improves on previously proposed schemes.

Several questions remain open. It would be interesting to find optimal (k, n)-threshold schemes for $k < n$. Perhaps a first step in this direction would be to find optimal schemes for the case $k = 2$. Another interesting direction of research is the exploration of new models which more realistically describe the superposition of different colors. Most of the research done (including the one presented in this paper) does not use the real properties of color superposition; it would be interesting to explore new models that appropriately describe such properties of colors.

Notes

1. In this paper, we need this lemma only for base matrices schemes.

References

1. G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Visual Cryptography for General Access Structures, *Information and Computation*, Vol. 129 No. 2 (1996) pp. 86–106.
2. G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Extended Schemes for Visual Cryptography, *Theoretical Computer Science*, Vol. 250 No. 1–2 (2001) pp. 143–161.

3. C. Blundo, A. De Bonis and A. De Santis, Improved Schemes for Visual Cryptography, *Designs, Codes, and Cryptography*, Vol. 24 (2001) pp. 255–278.
4. R. L. Grajam, D. E. Kunth and O. Patashnik, Concrete Mathematics, *A Foundation for Computer Science*, Addison Wesley, 1988.
5. J. H. van Lint and R. M. Wilson. *A Course in Combinatorics*, Cambridge University Press, Cambridge UK, 1992.
6. M. Naor and A. Shamir, Visual Cryptography, In *Advances in Cryptology – EUROCRYPT '94, LNCS* 950, pp. 1–12, 1995.
7. E. R. Verheul and H. C. A. van Tilborg, Constructions and Properties of k out of n Visual Secret Sharing Schemes. *Designs, Codes, and Cryptography*, Vol. 11 No. 2 (1997) pp. 179–196.
8. C. -N. Yang and C. -S. Laih, New Colored Visual Secret Sharing Schemes, *Designs, Codes and Cryptography*, No. 20, pp. 325–335, 2000.