Theoretical Computer Science 510 (2013) 62–86

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Color visual cryptography schemes for black and white secret images ☆

Roberto De Prisco *, Alfredo De Santis

Dipartimento di Informatica, Università di Salerno, 84084 Fisciano (SA), Italy

ARTICLE INFO

Article history:
Received 2 April 2013
Received in revised form 28 August 2013
Accepted 3 September 2013
Communicated by G. Ausiello

Keywords:
Secret sharing
Visual cryptography
Threshold schemes
b&w secret images
Colored shares

ABSTRACT

In this paper we propose the use of colors to improve visual cryptography schemes for black-and-white secret images. The resulting model is called colored-black-and-white visual cryptography (CBW-VC) model.

Using this new model we exploit colors to obtain schemes to share b&w images using a smaller pixel expansion. In particular we provide $(2, n)$-threshold schemes with pixel expansion $m = \lceil \log_3 n \rceil$, improving on the best pixel expansion attainable in the normal b&w model (BW-VC).

For the case of schemes with perfect reconstruction of black pixels we provide a general construction that allows us to transform any BW-VC scheme into a CBW-VC scheme whose pixel expansion is 1/3 of the pixel expansion of the starting BW-VC scheme.

We prove that, in the CBW-VC model, it is not possible to construct $(2, n)$-threshold schemes, for $n \geqslant 4$, and (k, n)-threshold schemes, for $k \geqslant 3$, without pixel expansion.

We also prove that there exist schemes with optimal contrast in the subset of schemes that use only full intensity colors; this is a direct consequence of the definition of contrast which distinguishes only black and non-black pixels. We discuss an alternative measure of contrast that takes into account the "distance" between colors. We conjecture that also with this definition of contrast there exist schemes that use only full intensity colors and achieve optimal contrast.

1. Introduction

A visual cryptography scheme, or vcs for short, is a special type of secret sharing that allows to share a secret image in such a way that the reconstruction of the secret can be performed by the human visual system. The sharing process produces a share for each participant. Each share is an image printed on a transparency. We will denote with $\mathcal{P}$ the set of participants and with n the cardinality of $\mathcal{P}$. The secret image is known by a trusted party, called the dealer. The dealer constructs the n shares and distributes one share to each participant. Certain qualified subsets of participants can "visually" recover the secret image. All other sets of participants, called forbidden, have no information on the secret image. A "visual" recovery for a set $X \subseteq \mathcal{P}$ consists in superposing the shares (transparencies) given to the participants in X. The participants in a qualified set X will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation. In most cases the qualified set of participants are all the sets with at least k participants, while all the sets with less than k participants are forbidden. In such cases the schemes are called (k, n)-threshold. For the

☆ A preliminary version of this paper appears in the proceedings of ICITS 2011 [10].

* Corresponding author.
E-mail addresses: robdep@dia.unisa.it (R. De Prisco), ads@dia.unisa.it (A. De Santis).

0304-3975/$ – see front matter
http://dx.doi.org/10.1016/j.tcs.2013.09.005

sake of simplicity, in this paper we consider only (k, n)-threshold schemes, although the results can be easily extended to any access structure.

Visual cryptography has been devised by Naor and Shamir [20]. We note that a previous paper by Kafri and Keren [15] provides a similar idea. The model used in [20] considers black and white visual cryptography. In b&w visual cryptography the secret image is a b&w image and also the shares are b&w images. The reconstructed image is also a b&w image. The idea is the following: each pixel of the secret image is expanded into some number m of pixels. Sometimes we call such m pixels "subpixels", even though they are regular pixels (a pixel cannot be subdivided). Parameter m is the *pixel expansion* of the scheme. The shares are constructed in such a way that when we superpose the shares of a qualified set of participants, among the m subpixels that represent a secret pixel we will find at most ℓ black subpixels, if the secret pixel is white, and at least h black subpixels if the secret pixel is black, with $0 \leqslant \ell < h \leqslant m$. The far apart are ℓ and h the better will be the reconstructed image. Parameters ℓ and h are used to define the *contrast* of the scheme.

The size of the reconstructed image is m times the size of the secret image. The pixel expansion m is a crucial characteristic of the scheme. When the pixel expansion is too large it might be impracticable to use the scheme because the physical size of the shares and the reconstructed image can become too large. For this reason it is important that m be as small as possible. The contrast is also important because it determines the overall quality of the reconstructed image.

Many papers have tackled the problem of finding BW-VC schemes with optimal (minimum) pixel expansion and several results are known, including both lower bounds on the pixel expansion and schemes achieving the lower bounds. Clearly we cannot improve on those schemes if we use the BW-VC model. However by allowing the shares to use colors we can construct schemes with smaller pixel expansion. For very specific cases we are able to construct schemes with no pixel expansion. We remark that the probabilistic model [25] also allows schemes with no pixel expansion, however the reconstruction is only probabilistic, that is, pixels are correctly reconstructed only with some given probability and such a probability decreases when the pixel expansion m increases. In [6] it has been shown that a decrease of the pixel expansion of a probabilistic scheme is payed off with an increase of the probability of an incorrect reconstruction. In this paper we are concerned with deterministic schemes in which there are no errors in the reconstruction of the secret image.

Some papers have considered the generalization to color images (for example see [1,5,7,8,13,16,21,23,25,26]). Chapter 2 of [9] contains a survey on visual cryptography for color images.

Obviously we could use any VCS for color images to share a black and white image. However, and not surprisingly, with color VCS we get a pixel expansion that is much bigger than the one we get with BW-VCS. Hence for the goal of this paper (decrease the pixel expansion of BW-VCS) color VCS are useless.

Although the generalization of visual cryptography to color images appears to be quite problematic, the use of colors can be of help in order to share black and white secret images.

In this paper we propose a new model that uses colors to share black and white secret images. That is, while the secret image is black and white, we allow the shares and thus the reconstructed image, to be color images. As before each secret pixel is expanded into m subpixels. Each subpixel can be colored with an arbitrary color. The reconstruction has to guarantee that among the m subpixels we will have at most ℓ black subpixels, if the secret pixel is white, and at least h black subpixels if the secret pixel is black, with $0 \leqslant \ell < h \leqslant m$. This requirement is the same as the one that we have for regular black and white cryptography. However reconstructed pixels are colored. We call this new model *colored-black-&-white* visual cryptography, or CBW-VC for short, and the scheme CBW-VC schemes, or CBW-VCS for short.

Using the CBW-VC model we can beat the pixel expansion of BW-VC schemes; obviously this is possible because the CBW-VC model is more powerful than the BW-VC model. In particular, we provide a construction of CBW-VC $(2, n)$-threshold schemes whose pixel expansion is $m = \lceil \log_3 n \rceil$ improving on the pixel expansion of BW-VCS (which is optimal in the BW-VC model). This means that for the cases of $n = 2, 3$ we get schemes with no pixel expansion. For these special cases the reconstructed image will have exactly the same size of the original one, white pixels will be reconstructed as colored pixels and black pixels will be reconstructed as black pixels. That is, the image will be as the original one, but the white background will be substituted with a 2-color (for $n = 2$) or a 3-color (for $n = 3$) mixture.

We also prove that the above two particular cases are the only ones for which we can construct schemes with no pixel expansion. More specifically, we prove that in the CBW-VC model it is not possible to construct $(2, n)$-threshold schemes, for $n \geqslant 4$, and (k, n)-threshold schemes, for $k \geqslant 3$, using $m = 1$.

As it happens for black and white images, among schemes with the same contrast, the reconstructed image is more clearly visible when black pixels are reconstructed with only black pixels. Schemes that have this property are called schemes with perfect reconstruction of black pixels.

We provide a general construction that allows us to take any BW-VC (k, n)-threshold scheme with perfect reconstruction of black pixels and transform it into a CBW-VC (k, n)-threshold scheme with perfect reconstruction of black pixels. The pixel expansion of the resulting CBW-VCS is $m = \lceil m'/3 \rceil$ where m' is the pixel expansion of the starting scheme. The construction works for any access structure and not just for threshold schemes.

The schemes that we present use only the eight full intensity colors white, black, red, green, blue, cyan, magenta and yellow. We prove that considering schemes that use only these colors is without loss of generality with respect to the optimal contrast. The above result is a direct consequence of the definition of the contrast property which distinguishes only between black and non-black pixels. We explore also the use of an alternative definition of contrast that makes a finer grained distinction among reconstructed pixels. We conjecture that also with this more involved definition one can restrict the attention to schemes using only full intensity colors.

This paper is organized as follows. Section 2 surveys previous relevant work while Section 3 describes the model that we use. In Section 4 we prove that restricting the attention to schemes that use only full intensity colors is without loss of generality. Section 5 provides the schemes for the case of $k = 2$, Section 6 describes the impossibility result and Section 7 presents the general construction for (k, n)-threshold schemes with perfect reconstruction of black pixels. Section 8 explores the use of an alternative definition of contrast. Finally Section 9 contains concluding remarks and directions for future work.

2. Previous work

Visual cryptography has been introduced by Naor and Shamir [20]. In a previous paper Kafri and Keren [15] provide a similar idea. The paper by Naor and Shamir [20] presents (k, n)-threshold schemes for black and white images. Quite a number of papers have followed. Many papers have studied the construction of schemes with optimal pixel expansion and both constructions and lower bounds are known. Other papers have studied the contrast of the schemes. Some papers have studied the generalization to color images. There are so many results about visual cryptography that a book with surveys has been published [9]. We refer the reader to such a book for references about papers on the subject. Recent papers that might not be cited in the book are [11,14,17–19,22,24].

Here, we will recall only the results that are necessary for this paper. Roughly speaking a black and white (k, n)-threshold visual cryptography scheme, BW-VCS for short, allows to share a secret black and white image by creating n shares in such a way that: (i) superposing k shares the secret is revealed and (ii) it is not possible to obtain any information about the secret when only $k - 1$ shares are available. To create the shares each pixel of the secret image is "expanded" into a given number m of subpixels. The scheme guarantees that when the secret pixel is white the reconstruction will have at most ℓ black subpixels and when the secret pixel is black, the reconstruction will have at least h black subpixels, with $0 \leqslant \ell < h \leqslant m$. The thresholds ℓ and h have been used to define the contrast of the scheme. The contrast is a measure of the goodness of the reconstruction. Several contrast measures have been used in the literature. In their seminal paper Naor and Shamir [20] define the contrast as $\alpha_{\text{NS}} = (h - \ell)/m$. Verheul and van Tilborg [23] used the following definition $\alpha_{\text{VV}} = (h - \ell)/(m(h + \ell))$. Eisen and Stinson [12] use $\alpha_{\text{ES}} = (h - \ell)/(m + \ell)$. We refer the reader to [12] for a discussion about these definitions of the contrast.

A particular class of schemes consists of those schemes for which the reconstruction of the black pixels is perfect, that is schemes for which $h = m$. Schemes with perfect reconstruction of black pixels, PB-BW-VCS for short, are important because, among schemes with equal contrast, they provide a reconstruction of the secret that is more clearly visible.

2.1. Lower bounds on the pixel expansion

Ateniese et al. [2] have proved the following lower bound on the pixel expansion of BW-VC (k, n)-threshold schemes:

Theorem 2.1. *(See [2].) In any (k, n)-threshold* BW-VCS *with pixel expansion m, it results that*

$$\binom{n}{k-1} \leqslant \binom{m}{\lfloor m/2 \rfloor} \tag{1}$$

and $m = \Omega(k \log_2 n)$.

We remark that the proof of the above bound uses the definition of contrast given by α_{NS} but the resulting lower bound on the pixel expansion is general, that is, it does not depend on the particular definition of the contrast and also it does not depend on the thresholds ℓ and h. For the case of $k = 2$ the above theorem can be restated as follows.

Theorem 2.2. *In any $(2, n)$-threshold* BW-VCS *with pixel expansion m, it results that*

$$n \leqslant \binom{m}{\lfloor m/2 \rfloor} \tag{2}$$

and $m = \Omega(\log_2 n)$.

Eisen and Stinson [12] have studied schemes with specified "whiteness" and "blackness" levels of reconstructed pixels. The whiteness and blackness levels are given by the thresholds ℓ and h. Recall that the definition of contrast used in [12] is α_{ES}. The following theorem (Theorem 9.1 of [12][1]) holds.

[1] We remark that Theorem 9.1 of paper [12] literally says: If $\hat{h} \geqslant (n-1)\hat{\ell}$ then $m = n\hat{h} - \frac{n(n-1)}{2}\hat{\ell}$. We have used $\hat{\ell}$ and $\hat{h}$ because paper [12] uses a different definition for the thresholds h and ℓ. It should not be hard to see that, with the definition used in this paper, they correspond to $\hat{\ell} = m - h$ and $\hat{h} = m - \ell$. Using this transformation we get Theorem 2.3.

Theorem 2.3. *(See [12].) In any* $(2, n)$*-threshold* BW-VCS *with pixel expansion* m *and thresholds* ℓ *and* h*, if* $m - \ell \geqslant (n-1)(m-h)$ *then*

$$m \geqslant n(m-\ell) - \frac{n(n-1)}{2}(m-h).$$

We can use the above theorem to obtain a lower bound on the pixel expansion of schemes with perfect reconstruction of black pixels, for which $h = m$.

When $h = m$, the condition $m - \ell \geqslant (n-1)(m-h)$ is always satisfied and thus for schemes with perfect reconstruction of black pixels the above bound can be restated as

Theorem 2.4. *In any* $(2, n)$*-threshold* PB-BW-VCS *with pixel expansion* m*, we have that* $m \geqslant n(m-\ell)$.

If we are not interested in the threshold ℓ or if we want a bound that does not depend on ℓ we can minimize the above bound over all possible values of ℓ. Since for schemes with perfect reconstruction of black pixels we have that $h = m$ and thus that $0 \leqslant \ell \leqslant m-1$ the above bound can be further restated as

Theorem 2.5. *In any* $(2, n)$*-threshold* PB-BW-VCS *with pixel expansion* m *we have that* $m \geqslant n$.

For $k = n$ we have the following lower bound.

Theorem 2.6. *(See [20].) In any* (n, n)*-threshold* BW-VCS *the pixel expansion* m *is* $m \geqslant 2^{n-1}$.

2.2. Schemes with optimal pixel expansion

Proof of existence of schemes with optimal pixel expansion are cited in [2]. The proofs are based on perfect hash families. However there is no explicit construction of optimal schemes. For the particular case of $k = 2$, Section 6.1 of [2] provides a simple construction of $(2, n)$-threshold schemes with pixel expansion $m = 2\lceil \log_2 n \rceil$. Such a pixel expansion is close to the optimal one given in Eq. (2). To illustrate the construction we provide an example and refer the reader to [2] for further details. Consider the case $n = 6$. Construct the following *starting matrix*:

$$SM = \begin{bmatrix} a_0 & a_0 & a_0 \\ a_0 & a_0 & a_1 \\ a_0 & a_1 & a_0 \\ a_0 & a_1 & a_1 \\ a_1 & a_0 & a_0 \\ a_1 & a_0 & a_1 \end{bmatrix},$$

where the subscripts of the elements in the rows of the matrix are the binary representation of the integers from 0 through $n-1$.

From the starting matrix SM we obtain the base matrices of the $(2, n)$-threshold scheme using the following substitutions. To obtain $B_\circ$ we substitute both a_0 and a_1 with $\bullet\circ$, while to obtain $B_\bullet$ we substitute a_0 with $\bullet\circ$ and a_1 with $\circ\bullet$. For the above example we have

$$B_\circ = \begin{bmatrix} \bullet\circ\bullet\circ\bullet\circ \\ \bullet\circ\bullet\circ\bullet\circ \\ \bullet\circ\bullet\circ\bullet\circ \\ \bullet\circ\bullet\circ\bullet\circ \\ \bullet\circ\bullet\circ\bullet\circ \\ \bullet\circ\bullet\circ\bullet\circ \end{bmatrix} \qquad B_\bullet = \begin{bmatrix} \bullet\circ\bullet\circ\bullet\circ \\ \bullet\circ\bullet\circ\circ\bullet \\ \bullet\circ\circ\bullet\bullet\circ \\ \bullet\circ\circ\bullet\circ\bullet \\ \circ\bullet\bullet\circ\bullet\circ \\ \circ\bullet\bullet\circ\circ\bullet \end{bmatrix}.$$

We will refer to such schemes as $\mathcal{S}^{\mathrm{A}}_{2,n}$.

2.3. Schemes with perfect reconstruction of black pixels

If we restrict the attention to schemes with perfect reconstruction of black pixels we have that the $(2, n)$-threshold scheme in the original paper by Naor and Shamir [20] is optimal. Indeed it has pixel expansion $m = n$ and perfect reconstruction of black pixels. Thus Theorem 2.5 implies that the scheme is optimal. The scheme is the following: the base matrix $B_\circ$ consists of one column of white pixels and $n-1$ columns with black pixels, while the base matrix $B_\bullet$ is the identity $n \times n$ matrix with the substitutions $1 \leftrightarrow \circ$ and $0 \leftrightarrow \bullet$. We will refer to such schemes as $\mathcal{S}^{\mathrm{NS}}_{2,n}$. For example, $\mathcal{S}^{\mathrm{NS}}_{2,5}$ is described by the following base matrices:

$$B_\circ = \begin{bmatrix} \circ\bullet\bullet\bullet\bullet \\ \circ\bullet\bullet\bullet\bullet \\ \circ\bullet\bullet\bullet\bullet \\ \circ\bullet\bullet\bullet\bullet \\ \circ\bullet\bullet\bullet\bullet \end{bmatrix} \qquad B_\bullet = \begin{bmatrix} \circ\bullet\bullet\bullet\bullet \\ \bullet\circ\bullet\bullet\bullet \\ \bullet\bullet\circ\bullet\bullet \\ \bullet\bullet\bullet\circ\bullet \\ \bullet\bullet\bullet\bullet\circ \end{bmatrix}.$$

Also the (n, n)-threshold scheme of [20] is with perfect reconstruction of black pixels. The scheme has pixel expansion $m = 2^{n-1}$ and thus, by Theorem 2.6, is optimal (also among the schemes that do not reconstruct black perfectly). The scheme is the following: the base matrix $B_\circ$ consists of all the columns with an even number of $\bullet$ pixels while the base matrix $B_\bullet$ consists of all the columns with an odd number of $\bullet$ pixels. We will refer to such schemes as $\mathcal{S}^{\mathrm{NS}}_{n,n}$. For example $\mathcal{S}^{\mathrm{NS}}_{4,4}$ is described by the following base matrices:

$$B_\circ = \begin{bmatrix} \circ\circ\circ\circ\bullet\bullet\bullet\bullet \\ \circ\circ\bullet\bullet\circ\circ\bullet\bullet \\ \circ\bullet\circ\bullet\circ\bullet\circ\bullet \\ \circ\bullet\bullet\circ\bullet\circ\circ\bullet \end{bmatrix} \qquad B_\bullet = \begin{bmatrix} \circ\circ\circ\bullet\bullet\bullet\bullet\circ \\ \circ\circ\bullet\circ\bullet\bullet\circ\bullet \\ \circ\bullet\circ\circ\bullet\circ\bullet\bullet \\ \bullet\circ\circ\circ\circ\bullet\bullet\bullet \end{bmatrix}.$$

Blundo et al. [3] have generalized the above two constructions to (k, n)-threshold schemes for any k, $2 \leqslant k \leqslant n$. The construction specifies the multiplicity $\mu_{b,j}$ of the columns with j black pixels in each base matrix B_x, where $x \in \{\circ, \bullet\}$.

If k is odd, then the multiplicities of columns in the base matrices are described by the following equations:

$$\begin{aligned} &\mu_{\circ,0} = 1 \\ &\quad \text{for } 0 \leqslant i \leqslant \frac{k-3}{2}, \quad \mu_{\circ,n-2i-1} = \binom{n-2i-2}{k-2i-2} \\ &\quad \text{for } 0 \leqslant i \leqslant \frac{k-1}{2}, \quad \mu_{\bullet,n-2i} = \binom{n-2i-1}{k-2i-1} \end{aligned} \tag{3}$$

whereas all the remaining $\mu_{x,j}$'s are equal to zero.

If k is even, then the multiplicities of columns in the base matrices are described by the following equations:

$$\begin{aligned} &\mu_{\circ,0} = 1 \\ &\quad \text{for } 0 \leqslant i \leqslant \frac{k-2}{2}, \quad \mu_{\circ,n-2i} = \binom{n-2i-1}{k-2i-1} \\ &\quad \text{for } 0 \leqslant i \leqslant \frac{k-2}{2}, \quad \mu_{\bullet,n-2i-1} = \binom{n-2i-2}{k-2i-2} \end{aligned} \tag{4}$$

whereas all the remaining $\mu_{x,j}$'s are equal to zero.

We will refer to the above schemes as $\mathcal{S}^{\mathrm{B}}_{k,n}$.

For example the $\mathcal{S}^{\mathrm{B}}_{3,4}$, can be constructed using Eqs. (3) which give $\mu_{\circ,0} = 1$, $\mu_{\circ,3} = 2$, $\mu_{\bullet,4} = 3$, $\mu_{\bullet,2} = 1$ while all other μs are 0. Hence the base matrices of the scheme are:

$$B_\circ = \begin{bmatrix} \circ\bullet\bullet\bullet\bullet\bullet\circ\circ \\ \circ\bullet\bullet\bullet\bullet\circ\circ\bullet\bullet \\ \circ\bullet\bullet\circ\circ\bullet\bullet\bullet\bullet \\ \circ\circ\circ\bullet\bullet\bullet\bullet\bullet\bullet \end{bmatrix} \qquad B_\bullet = \begin{bmatrix} \bullet\bullet\bullet\bullet\bullet\bullet\circ\circ\circ \\ \bullet\bullet\bullet\bullet\circ\circ\bullet\bullet\circ \\ \bullet\bullet\bullet\circ\bullet\circ\bullet\circ\bullet \\ \bullet\bullet\bullet\circ\circ\bullet\circ\bullet\bullet \end{bmatrix}.$$

The pixel expansion of the $(2, n)$-threshold scheme is $m = n$, the pixel expansion of the (n, n)-threshold scheme is $m = 2^{n-1}$. For the $(3, n)$-threshold is $m = (n-1)^2$ and for the $(n-1, n)$ is $m = (n-2)2^{n-2} + 1$.

Theorem 2.7. *(See [3].) The pixel expansion m of the schemes $\mathcal{S}^{\mathrm{B}}_{k,n}$ satisfies*

$$\binom{n-1}{k-1}2^{k-2} + 1 \leqslant m \leqslant \left(\binom{n-1}{k-1} - 1\right)2^{k-1} + 1.$$

All of the above PB-BW-VCS have $\ell = m - 1$, and, obviously, $h = m$.

Table 1 provides a summary of the relevant known results. The companion table to the right summarizes the pixel expansion improvements obtained in this paper.

Table 1
Summary of known relevant results (and to the right a summary of the results of this paper).

Known results	Lower bound	Construction	This paper
BW-VCS			CBW-VCS
$k=2$	$m=\Omega(\log_2 n)$ [2]	$m=2\lceil\log_2 n\rceil$ [2]	$m=\lceil\log_3 n\rceil$
PB-BW-VCS			PB-CBW-VCS
$k=2$	$m\geqslant n$ [12]	$m=n$ [20]	$m=\lceil m'/3\rceil$
$k=3$	Theorem 2.1	$m=(n-1)^2$ [4]	where m' is the
$4\leqslant k\leqslant n-2$	Theorem 2.1	Lemma 2.7	pixel expansion of
$k=n-1$	Theorem 2.1	$m=(n-2)2^{n-2}+1$ [4]	any (k,n)-threshold
$k=n$	$m\geqslant 2^{n-1}$ [20]	$m=2^{n-1}$ [20]	PB-BW-VCS

3. The model

3.1. Colors

In order to deal we colored pixels we need to use a color model. W use the RGB color model: a color is represented as a triple (x, y, z), with $0\leqslant x, j, z\leqslant L$, for a fixed threshold L, where x, y and z are, respectively the amount of red, green and blue light present in the color. For example if we restrict x, y and z to be integers and set $L=255$ (that is we use a byte for each component) we can represent 256^3 different colors. Since in this paper the threshold L is irrelevant, for simplicity we assume that $L=1$ and that x, y and z are real numbers. A white light contains all colors and is represented by $(1, 1, 1)$. The color black is obtained when there is no light at all, and thus it is represented by $(0, 0, 0)$. The colors red, green and blue are represented, respectively, by $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$. The colors cyan, magenta and yellow are the "complement" of, respectively, red, green and blue, and thus are represented by $(0, 1, 1)$, $(1, 0, 1)$ and $(1, 1, 0)$. The eight full intensity colors, black, red, green, blue, cyan, magenta, yellow and white, will be denoted with, respectively, $\bullet$, R, G, B, C, M, Y and $\circ$.

When we superpose two colored pixels $c_1=(x_1, y_1, z_1)$ and $c_2=(x_2, y_2, z_2)$, the resulting color is a function of the two colored pixels. A good approximation of the resulting color is given by the following operator add:

$$\mathtt{add}(c_1, c_2)=\left(\mathtt{int}\left(\frac{x_1x_2}{L}\right), \mathtt{int}\left(\frac{y_1y_2}{L}\right), \mathtt{int}\left(\frac{z_1z_2}{L}\right)\right),$$

that, for $L=1$, becomes

$$\mathtt{add}(c_1, c_2)=(x_1x_2, y_1y_2, z_1z_2).$$

The add operator can be extended to handle vectors of colors and to matrices (in which case we add the colors in each column and thus the result will be a vector whose length is equal to the number of columns).

3.2. Visual cryptography schemes

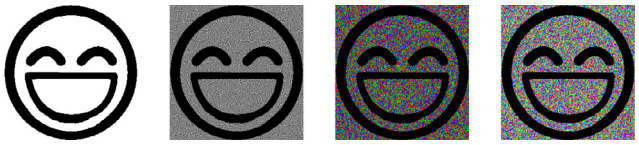
A secret image, consisting of black and white pixels, has to be shared among a set $\mathcal{P}=\{1,\ldots,n\}$ of *participants*. A trusted party, which is called the *dealer* and is not a participant, knows the secret image. The dealer has to distribute the *shares* to the n participants in the form of printed transparencies. Some subsets of $\mathcal{P}$, called *qualified sets* have to be able to "visually" recover the secret image, by superposing their shares (transparencies) and holding the stacked set of transparencies to the light. Other subsets of $\mathcal{P}$, called *forbidden sets*, must not be able to get any information on the secret image from their shares, neither by superposing the transparencies nor by any other computation. In this paper we consider (k, n)-threshold schemes for which the qualified sets are all the subsets of $\mathcal{P}$ with cardinality at least k. All the subsets with less than k participants are forbidden.

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. The secret image is made up of black and white pixels.

Each pixel appears in n versions called *shares*, one for each transparency. Each share is a collection of m pixels. We denote by $\mathcal{P}al$ the universe of all colors, that is $\mathcal{P}al=\{(x, y, z)\mid 0\leqslant x, y, z\leqslant 1\}$. Each pixel is an element of $\mathcal{P}al$. We denote by $\mathcal{P}al_{\mathrm{FI}}$ the set of the eight full intensity colors $\mathcal{P}al_{\mathrm{FI}}=\{\circ, \mathtt{R}, \mathtt{G}, \mathtt{B}, \mathtt{C}, \mathtt{M}, \mathtt{Y}, \bullet\}$ and by $\mathcal{P}al_{\mathrm{BW}}$ the set containing only black and white, $\mathcal{P}al_{\mathrm{BW}}=\{\circ, \bullet\}$. Clearly $\mathcal{P}al_{\mathrm{BW}}\subset\mathcal{P}al_{\mathrm{FI}}\subset\mathcal{P}al$.

A visual cryptography scheme (vcs) is described by two collections $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ of $n\times m$ matrices with elements in $\mathcal{P}al$. A matrix M in one of such collections is called a distribution matrix and is just a representation of the pixels in the shares: each row corresponds to a share (row i is the share of participant i) and the m elements of the row provide the colors of the m pixels into which the secret pixel has to be expanded. Often the m pixels in a row are called "subpixels" because, taken together, they represent the secret pixel in a share. The superposition operation is given by the add of the rows corresponding to the shares.

For example, below is a matrix M with full intensity colors and the resulting add(M):



b&w image (100x100px) | b&w background $\lambda = 50\%$ | RGB background $\lambda = 33\%$ | RGBCMY background $\lambda = 50\%$

Fig. 1. Average light transmission comparison for different backgrounds.

$$M = \begin{bmatrix} \circ\circ\mathtt{CM}\bullet\mathtt{RR} \\ \circ\mathtt{GM}\circ\mathtt{RRG} \\ \circ\mathtt{BBGRRB} \end{bmatrix}$$

$$\mathtt{add}(M) = \quad \circ\bullet\mathtt{B}\bullet\bullet\mathtt{R}\bullet$$

Below is another example:

$$M = \begin{bmatrix} (0.8, 0.2, 1) & (1, 0.5, 0.5) & (0, 0.4, 0.4) \\ (0.1, 1.0, 1) & (0.8, 0.5, 0.5) & (0, 1.0, 1) \\ (0.3, 0.5, 1) & (1, 0.5, 1) & (0.4, 0.4, 1) \end{bmatrix}$$

$$\mathtt{add}(M) = \ (0.24, 0.1, 1)\ (0.8, 0.125, 0.25)\ (0, 0.16, 0.4)$$

3.3. Contrast in the reconstructed images

The contrast property, which will be defined formally shortly, is an important property of a visual cryptography scheme because it measures the "goodness" of the reconstructed image. In the regular BW-VCS model the contrast property requires that in the reconstruction of a white pixel there not be too many black subpixels (namely, at most ℓ) while in the reconstruction of black subpixels there be many black subpixels (namely, at least h, with $0 \leqslant \ell < h < m$).

The use of colors allows for more involved definitions of the contrast property. For simplicity we will use a definition of contrast that is similar to the one used for the BW-VC model. More specifically "black" in the reconstructed image is interpreted as black (in the secret image) and "anything that is not black" in the reconstructed image is interpreted as white (in the secret image). With this interpretation of the colors, as we point out later, it is without loss of generality to consider only the eight full intensity colors to construct the schemes. So we will concentrate our attention on schemes that use only full intensity colors.

In Section 8 we discuss the use of a different and more involved definition of contrast and we explore the use of all the colors providing some evidence that, also with a more involved definition of contrast, one gets the best contrast when using full intensity colors.

3.4. Colored background

From the point of view of the user, the main difference between the CBW-VC model and the BW-VC model is that in the former white areas of the secret image are reconstructed as a mixture of colored pixels and in the latter they are reconstructed as a mixture of black and white pixels. Black areas can be reconstructed either as perfect black or as a mixture of black and white (in the BW-VC model) or colored pixels (in the CBW-VC model). The following applies to schemes with perfect reconstruction of black pixels, although the reasoning is valid, with some approximation, in general.

The fact that in the CBW-VC model the secret is reconstructed as black over a mixture of colored pixels is not a drawback with respect to the BW-VC model where the secret is reconstructed as black over a mixture of black and white pixel.

We can give a formal argument by considering the average light transmission that is defined as the amount of light that passes through a transparency having the image printed on it. For a random grid[2] of black and white pixels, for example, the average light transmission λ is 50%, because a black pixel blocks completely the light while a white pixel allows the light to pass through without alterations. A completely white (transparent) image has $\lambda = 100\%$, while a completely black image has $\lambda = 0\%$. For color images we can use an average of the three components. For example the average light transmission of a red pixel is $\lambda \simeq 33\%$ since the RGB components of a red pixel are $(100, 0, 0)$. A random grid of red, green and blue pixels has $\lambda \simeq 33\%$.

Fig. 1 shows a black and white image and the same image with the original white background represented as a random mixture of black and white pixels, which gives an average light transmission of $\lambda = 50\%$, a random mixture of R, G and B pixels, which gives $\lambda = 33\%$, and a random mixture of R, G, B, C, M and Y pixels, which gives $\lambda = 50\%$.

[2] A random grid is an image where each pixel is chosen uniformly at random.

The average light transmission is directly related to the thresholds ℓ and h and thus is directly related to the contrast. This means that if we estimate the contrast we get also an estimate of the average light transmission. In the analysis of the schemes that we present in this paper we explicitly give the values of ℓ and h (and thus implicitly estimate the average light transmission of both white and black areas of the secret image). The analysis shows that the average light transmission of the images reconstructed with the CBW-VC schemes that we propose in this paper are comparable to those of the BW-VC schemes, since the contrast of the former schemes are comparable to those of the latter ones.

3.5. Formal definition of a VCS

Given a vector v of elements in $\mathcal{P}al$ and a color $c \in \mathcal{P}al$ we denote with $w_c(v)$, the number of elements of v equal to c and with $w_{\bar{c}}(v)$ the number of elements of v different from c. For example, $w_\bullet(v)$ is the number of elements of v equal to $\bullet$, $w_{\bar{\bullet}}(v)$ is the number of elements of v different from $\bullet$ and $w_\circ(v)$ is the number of elements of v equal to $\circ$.

Next we provide a formal definition of a VCS. Notice that this definition works both for the regular BW-VC model in which the shares are restricted to be black and white and in the CBW-VC model in which the shares can have colored pixels. For the BW-VC model the shares palette is $\mathcal{P}al_{\mathrm{BW}}$, while for the CBW-VC model the shares palette is $\mathcal{P}al_{\mathrm{FI}}$.

Definition 3.1. A (k, n)-threshold scheme is given by two collections $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ of $n \times m$ distribution matrices that satisfy the following conditions. There must exist two integers ℓ and h, with $0 \leqslant \ell < h \leqslant m$, such that

1. (Contrast property) Given any qualified set X, $|X| \geqslant k$, of participants the following holds: for any $M \in \mathcal{C}_\circ$, we have that $w_\bullet(\mathtt{add}(M|X)) \leqslant \ell$ and for any $M \in \mathcal{C}_\bullet$, we have that $w_\bullet(\mathtt{add}(M|X)) \geqslant h$.
2. (Security property) Given any forbidden set X, $|X| < k$, the two collections of $|X| \times m$ matrices, $\mathcal{D}_\circ = \{M|X$, for each $M \in \mathcal{C}_\circ\}$, and $\mathcal{D}_\bullet = \{M|X$, for each $M \in \mathcal{C}_\bullet\}$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Let M be a distribution matrix. Given a subset X of participants we denote by $M|X$ the submatrix of M consisting of all the rows of M that represent shares of participants in X.

A scheme is used in the following way: if the secret pixel is of color $\circ$ (resp. $\bullet$), then the dealer randomly chooses one of the matrices in $\mathcal{C}_\circ$ (resp. $\mathcal{C}_\bullet$) and uses it as the distribution matrix.

The security property guarantees that forbidden sets of participants have no information about which collection has been used to encode the pixel because with the information provided by the shares, any of the collections is equally likely to have been used to encode the pixel. The contrast property guarantees that the reconstructed image is visible.

The contrast property requires that in the reconstruction of a white pixel the number of black subpixels is sufficiently small (at most ℓ), whereas in the reconstruction of a black pixel the number of black subpixels is sufficiently large (at least h).

Notice that this property is the same that we have for regular black and white schemes. In that case however we have that the shares can only have black and white subpixels and thus $w_\circ + w_\bullet = m$ while in the case of colored black and white schemes we can have $w_\circ + w_\bullet < m$ because some pixels of the reconstruction can be colored. Clearly it is always the case that $w_\bullet + w_{\bar{\bullet}} = m$.

The main parameter that we use for the evaluation of a scheme is the pixel expansion m. The pixel expansion measures the loss of resolution since pixels in the reconstructed image are m times bigger. We aim at constructing schemes with the smallest possible pixel expansion.

We also evaluate the contrast of the scheme. For regular BW-VCS the contrast has been defined in several ways for BW-VCS. We refer the reader to [12] for a discussion about the contrast property and about which definition is better. In this paper we will use the definition $\alpha_{\mathrm{NS}} = (h - \ell)/m$. In the following sections we will use α to denote α_{NS}. In Section 8 we will discuss an alternative measure of contrast α_{CBW}.

4. Using full intensity colors

The contrast property of Definition 3.1 makes the following characterization for the reconstructed pixels: a black subpixel contributes to the interpretation of the reconstructed pixel as black and any non-black subpixel contributes to the interpretation of the reconstructed pixel as white. That is, the only distinction made on reconstructed (sub)pixels is black and non-black. This fact, together with the observation that one can get black only by having color components equal to 0, suggests that one can use only full intensity colors without losing in generality. Indeed the next theorem allows us to restrict our attention to schemes using only full intensity colors, without losing the possibility of finding schemes with optimal contrast.

Before providing the theorem let us define the following *make-full* transformation operation. Let $c = (x, y, z)$ be a color. The *make-full* transformation produces $c' = (x', y', z') = \mathit{make\text{-}full}(c)$ as follows:

$$x' = \begin{cases} 0, & \text{if } x = 0 \\ 1, & \text{if } x > 0 \end{cases} \qquad y' = \begin{cases} 0, & \text{if } y = 0 \\ 1, & \text{if } y > 0 \end{cases} \qquad z' = \begin{cases} 0, & \text{if } z = 0 \\ 1, & \text{if } z > 0 \end{cases}$$

that is, any non-zero component is changed to 1. Given a vector of colors $(c_1, \ldots, c_z)$ and a matrix of colors M it should not be hard to see that

$$w_\bullet(c_1, \ldots, c_z) = w_\bullet\big(\textit{make-full}(c_1, \ldots, c_z)\big)$$

and thus

$$w_\bullet\big(\mathtt{add}(M)\big) = w_\bullet\big(\mathtt{add}\big(\textit{make-full}(M)\big)\big) = w_\bullet\big(\textit{make-full}\big(\mathtt{add}(M)\big)\big)$$

where the *make-full* transformation for a vector or a matrix is obtained by applying the *make-full* transformation to every element of the vector or the matrix. In other words, the *make-full* operation does not change the weight $w_\bullet$ of a vector of colors. Indeed a color component of the superposition goes to 0 only when superposing a pixel that has 0 for that component. So the actual value of a non-zero component does not matter. Here is an example:

$$M = \begin{bmatrix} (0.3, 0.8, 1) & (0.4, 0.8, 0) & (0, 0.7, 0.4) \\ (1, 0.5, 0) & (0.8, 0, 0.5) & (0.2, 1, 1) \\ (0.9, 1, 0.3) & (0, 0.5, 0.6) & (0.6, 0.5, 0.6) \end{bmatrix}$$

$$\mathtt{add}(M) = \quad (0.27, 0.4, 0) \quad (0, 0, 0) \quad (0, 0.25, 0.24)$$

Let $M' = \textit{make-full}(M)$. We have that

$$M' = \begin{bmatrix} (1, 1, 1) & (1, 1, 0) & (0, 1, 1) \\ (1, 1, 0) & (1, 0, 1) & (1, 1, 1) \\ (1, 1, 1) & (0, 1, 1) & (1, 1, 1) \end{bmatrix}$$

$$\mathtt{add}\big(M'\big) = \quad (1, 1, 0) \quad (0, 0, 0) \quad (0, 1, 1)$$

We have $w_\bullet(\mathtt{add}(M)) = 1$ and $w_\bullet(\mathtt{add}(\textit{make-full}(M))) = 1$ because in both cases there is only one pixel in the result of the superposition that is $(0, 0, 0)$ due to the three zeroes in the red, green and blue components. The fact that other numbers are 1 or something else greater than 0, does not matter for the weight $w_\bullet$.

We are now ready to provide the following theorem.

Theorem 4.1. *Given a scheme S with contrast $\alpha(S)$, there exist a scheme S' using only full intensity colors and having $\alpha(S') = \alpha(S)$.*

Proof. Let S be a scheme and let $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ be the two collections of distribution matrices of S. Construct a new scheme S' whose collections of distribution matrices $\mathcal{C}'_\circ$ and $\mathcal{C}'_\bullet$ are obtained by transforming every pixel in the matrices of $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ using the *make-full* transformation.

Since the *make-full* transformation produces only full intensity colors, scheme S' is a scheme that uses only full intensity colors. We have to prove that $\alpha(S') = \alpha(S)$.

Let ℓ and h the thresholds of scheme S. Let $M \in \mathcal{C}_\circ$. By definition we have that $w_\bullet(\mathtt{add}(M|X)) \leqslant \ell$ for any qualified set of participants X. By the definition of *make-full* we have that $w_\bullet(\mathtt{add}(M'|X)) \leqslant \ell$, where M' is the matrix of $\mathcal{C}'_\circ$ obtained applying the *make-full* transformation to M. Similarly for any $M' \in \mathcal{C}_\bullet$ we have that $w_\bullet(\mathtt{add}(M'|X)) \geqslant h$. Hence $\alpha(S') = \alpha(S)$. □

Because of the above theorem we restrict our attention to schemes that use only full intensity colors. In Section 8 we discuss further the contrast property and the use of all the colors to construct schemes.

5. $(2, n)$-threshold schemes

In this section we provide a construction of CBW-VC $(2, n)$-threshold schemes. The construction gives schemes with pixel expansion $m = \lceil \log_3 n \rceil$. We start by first describing two simple cases, for $n = 2, 3$, and then we provide the generalization to any n.

5.1. $(2, 2)$-threshold scheme

Let's start with the case $n = 2$. There are several ways to implement a $(2, 2)$-threshold CBW-VCS. In the first one we use the 3 colors R, G and B.

Construction 5.1 *(Scheme $(2, 2)$-RGB). The following collections of distribution matrices describe a $(2, 2)$-threshold* CBW-VCS *with a shares palette equal to* {R, G, B}*, pixel expansion $m = 1$, $h = 1$, $\ell = 0$ (and thus contrast $\alpha = 1$[3]):*

[3] Notice that a contrast of 1 is not possible in the BW-VC model. In the CBW-VC model it is possible because of the extra power that arises from interpreting any non-black pixel as a "white" pixel. Although distinguishing a black pixel from a non-black but very dark pixel is difficult if not impossible,

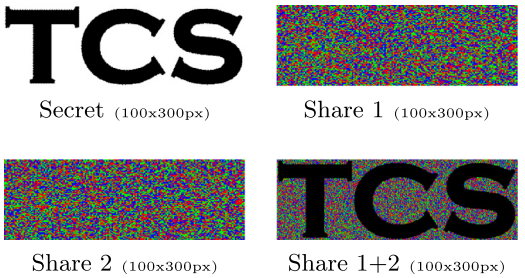


Fig. 2. Sharing and reconstruction for the $(2,2)$-RGB scheme.

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} \mathtt{R} \\ \mathtt{R} \end{bmatrix}, \begin{bmatrix} \mathtt{G} \\ \mathtt{G} \end{bmatrix}, \begin{bmatrix} \mathtt{B} \\ \mathtt{B} \end{bmatrix} \right\}$$

$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} \mathtt{R} \\ \mathtt{G} \end{bmatrix}, \begin{bmatrix} \mathtt{G} \\ \mathtt{R} \end{bmatrix}, \begin{bmatrix} \mathtt{R} \\ \mathtt{B} \end{bmatrix}, \begin{bmatrix} \mathtt{B} \\ \mathtt{R} \end{bmatrix}, \begin{bmatrix} \mathtt{G} \\ \mathtt{B} \end{bmatrix}, \begin{bmatrix} \mathtt{B} \\ \mathtt{G} \end{bmatrix} \right\}.$$

Proof. The security property is satisfied because if we restrict the attention to one single row in the two collections of distribution matrices, in both cases we see the same pixels with the same frequencies. The contrast property is satisfied because when we reconstruct a black pixel we obtain a black pixel, while when we reconstruct a white pixel we obtain either R, G or B. That is, we have $\ell = 0$ and $h = 1$. The pixel expansion for such a scheme is $m = 1$ and thus the contrast is $\alpha = 1$. □

The proof is straightforward and holds for the other $(2,2)$-threshold CBW-VCS that we will present in this section. So we will not repeat the proof. Fig. 2 shows an example of use of the $(2,2)$-RGB scheme: a secret black and white image, the two shares and the reconstructed secret image.

We remark that with a regular BW-VC schemes we must have some pixel expansion. Our $(2,2)$-threshold CBW-VC scheme is without pixel expansion; this means that the reconstructed image is the same size as the original one.

In a regular BW-VCS the reconstructed image is a black image over a mixture of black and white pixels. In our CBW-VCS the reconstructed image is a black image over a mixture of colored pixels (R, G and B in the example).

Another $(2,2)$-threshold CBW-VCS can be obtained using the set of colors R, G, B, C, M and Y.

Construction 5.2 *(Scheme $(2,2)$-RGBCMY). The following collections of distribution matrices describe a $(2,2)$-threshold* CBW-VCS *with a shares palette equal to* $\{\mathtt{R},\mathtt{G},\mathtt{B},\mathtt{C},\mathtt{M},\mathtt{Y}\}$*, pixel expansion $m = 1$, $h = 1$, $\ell = 0$ (and thus contrast $\alpha = 1$):*

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} \mathtt{R} \\ \mathtt{R} \end{bmatrix}, \begin{bmatrix} \mathtt{G} \\ \mathtt{G} \end{bmatrix}, \begin{bmatrix} \mathtt{B} \\ \mathtt{B} \end{bmatrix}, \begin{bmatrix} \mathtt{C} \\ \mathtt{C} \end{bmatrix}, \begin{bmatrix} \mathtt{M} \\ \mathtt{M} \end{bmatrix}, \begin{bmatrix} \mathtt{Y} \\ \mathtt{Y} \end{bmatrix} \right\}$$

$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} \mathtt{R} \\ \mathtt{C} \end{bmatrix}, \begin{bmatrix} \mathtt{C} \\ \mathtt{R} \end{bmatrix}, \begin{bmatrix} \mathtt{G} \\ \mathtt{M} \end{bmatrix}, \begin{bmatrix} \mathtt{M} \\ \mathtt{G} \end{bmatrix}, \begin{bmatrix} \mathtt{B} \\ \mathtt{Y} \end{bmatrix}, \begin{bmatrix} \mathtt{Y} \\ \mathtt{B} \end{bmatrix} \right\}.$$

The reconstructed image will be a black image over a random mixture of R, G, B, C, M and Y pixels. Notice that the particular choice of superposing R with C, G with M and B with Y is justified by the fact that superposition of these particular pairs gives black. So the scheme reconstructs black pixels perfectly.

It is possible also to construct schemes using only two colors:

Construction 5.3 *(Scheme $(2,2)$-RG). The following collections of distribution matrices describe a $(2,2)$-threshold* CBW-VCS *with a shares palette equal to* $\{\mathtt{R},\mathtt{G}\}$*, pixel expansion $m = 1$, $h = 1$, $\ell = 0$ (and thus contrast $\alpha = 1$):*

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} \mathtt{R} \\ \mathtt{R} \end{bmatrix}, \begin{bmatrix} \mathtt{G} \\ \mathtt{G} \end{bmatrix} \right\}$$

$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} \mathtt{R} \\ \mathtt{G} \end{bmatrix}, \begin{bmatrix} \mathtt{G} \\ \mathtt{R} \end{bmatrix} \right\}.$$

distinguishing a black pixel from another full intensity color (red, green, blue, cyan, magenta, yellow) is immediate. To take care of the problem of distinguishing very dark pixels from black pixels, or more in general, pixels with very similar colors, the definition of contrast should take into account the exact value of the color of the pixels. In Section 8 we discuss this issue.

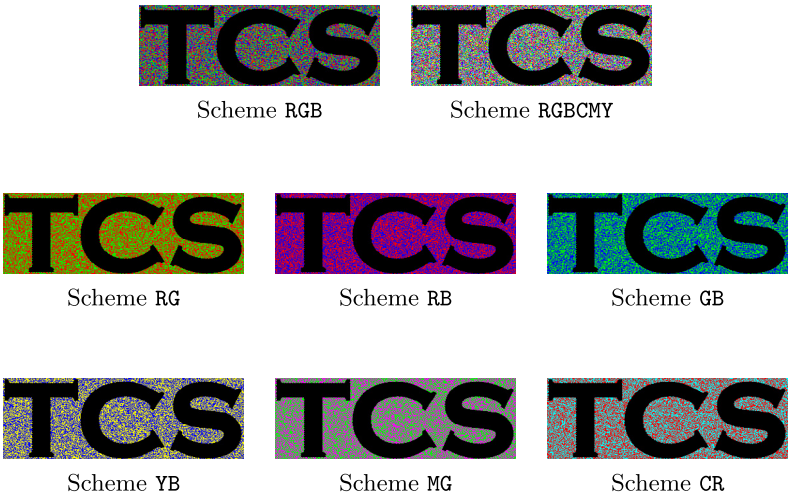


Fig. 3. Reconstructed images for the $(2,2)$-threshold CBW-VCS.

The choice of R and G is not the only one. We can obtain similar schemes using any pair of colors whose superposition gives •. Pairs of colors that satisfy such a property are: (R, G), (R, B), (G, B), (Y, B), (M, G), (C, R).

Fig. 3 shows the reconstructed image for each of the pairs (R, G), (R,B), (G, B), (Y,B), (M, G), (C, R) and also for the two schemes $(2,2)$-RGBCMY and $(2,2)$-RGB.

5.2. $(2,3)$-threshold scheme

In this section we provide a $(2,3)$-threshold scheme.

Construction 5.4 *(Scheme $(2,3)$-RGB). The following collections of distribution matrices describe a $(2,3)$-threshold* CBW-VCS *with a shares palette equal to* {R, G, B}*, pixel expansion $m=1$, $h=1$, $\ell=0$ (and thus contrast $\alpha=1$):*

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} \mathtt{R} \\ \mathtt{R} \\ \mathtt{R} \end{bmatrix}, \begin{bmatrix} \mathtt{G} \\ \mathtt{G} \\ \mathtt{G} \end{bmatrix}, \begin{bmatrix} \mathtt{B} \\ \mathtt{B} \\ \mathtt{B} \end{bmatrix} \right\}$$

$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} \mathtt{R} \\ \mathtt{B} \\ \mathtt{G} \end{bmatrix}, \begin{bmatrix} \mathtt{G} \\ \mathtt{R} \\ \mathtt{B} \end{bmatrix}, \begin{bmatrix} \mathtt{B} \\ \mathtt{G} \\ \mathtt{R} \end{bmatrix} \right\}.$$

Proof. The security property is satisfied because if we restrict the attention to one single row in the two collections of distribution matrices, in both cases we see three distribution matrices each with one pixel of color, respectively, R, G and B. The contrast property is satisfied because when we reconstruct a black pixel we obtain a black pixel, while when we reconstruct a white pixel we obtain one of R, G and B. That is, we have $\ell=0$ and $h=1$. The pixel expansion is $m=1$ and thus the contrast is $\alpha=1$. □

As for the $(2,2)$-threshold schemes also in this case we have that the reconstructed image is a black image over a mixture of colors. In this case the mixture of colors is made up of the three colors R, G and B. Fig. 4 shows the shares and the reconstructed images.

5.3. $(2,n)$-threshold schemes

In this section we present a generalization of the technique used for the particular cases $n=2,3$. For $n \geqslant 4$ we have to start expanding the secret pixels into $m>1$ subpixels and the contrast of the reconstructed images degrades as n increases.

Construction 5.5. *Let $m=\lceil \log_3 n \rceil$. Consider the set $\mathcal{S}$ of all the strings of length m over the alphabet $\Sigma=$ {R, G, B}. These are $3^m \geqslant n$. Choose any n such strings and denote them $s_1, s_2, \ldots, s_n$. The collections of distribution matrices of the scheme are shown in Table 2.*

Some examples will clarify the construction. Let $n=4$. We have that $m=2$ and $\mathcal{S}=$ {RR, RG, RB, GG, GR, GB, BB, BR, BG}. We choose the following 4 elements of $\mathcal{S}$: {RR, GG, BB, RG}. The collections of distribution matrices are:

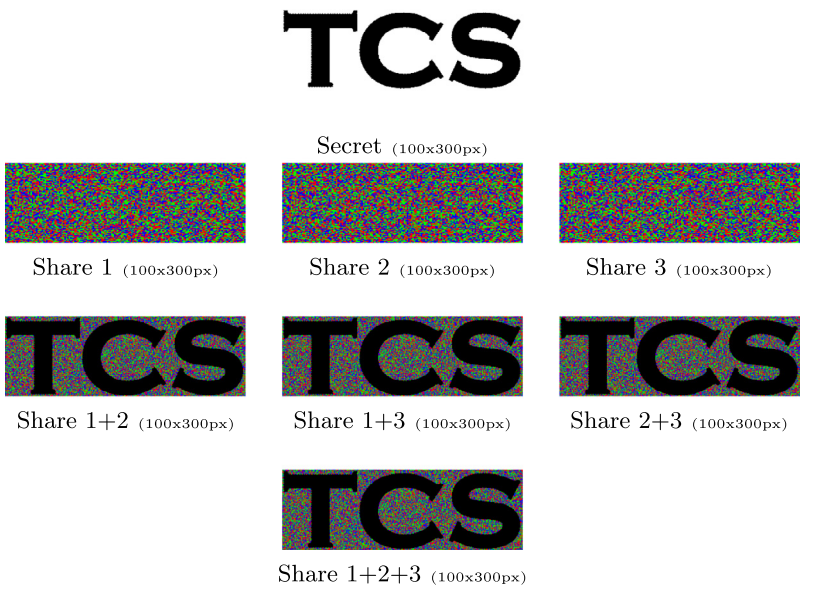


Fig. 4. Shares and reconstructed images for the $(2, 3)$-threshold CBW-VCS.

Table 2
Collections for Construction 5.5.

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} s_1 \\ s_1 \\ s_1 \\ \cdots \\ \cdots \\ s_1 \\ s_1 \\ s_1 \end{bmatrix}, \begin{bmatrix} s_2 \\ s_2 \\ s_2 \\ \cdots \\ \cdots \\ s_2 \\ s_2 \\ s_2 \end{bmatrix}, \begin{bmatrix} s_3 \\ s_3 \\ s_3 \\ \cdots \\ \cdots \\ s_3 \\ s_3 \\ s_3 \end{bmatrix}, \ldots\ldots\ldots\ldots, \begin{bmatrix} s_{n-1} \\ s_{n-1} \\ s_{n-1} \\ \cdots \\ \cdots \\ s_{n-1} \\ s_{n-1} \\ s_{n-1} \end{bmatrix}, \begin{bmatrix} s_n \\ s_n \\ s_n \\ \cdots \\ \cdots \\ s_n \\ s_n \\ s_n \end{bmatrix} \right\}$$

$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_{n-2} \\ s_{n-1} \\ s_n \end{bmatrix}, \begin{bmatrix} s_n \\ s_1 \\ s_2 \\ \cdots \\ \cdots \\ s_{n-3} \\ s_{n-2} \\ s_{n-1} \end{bmatrix}, \begin{bmatrix} s_{n-1} \\ s_n \\ s_1 \\ \cdots \\ \cdots \\ s_{n-4} \\ s_{n-3} \\ s_{n-2} \end{bmatrix}, \ldots\ldots\ldots\ldots, \begin{bmatrix} s_3 \\ s_4 \\ s_5 \\ \cdots \\ \cdots \\ s_n \\ s_1 \\ s_2 \end{bmatrix}, \begin{bmatrix} s_2 \\ s_3 \\ s_4 \\ \cdots \\ \cdots \\ s_{n-1} \\ s_n \\ s_1 \end{bmatrix} \right\}$$

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} \mathtt{RR} \\ \mathtt{RR} \\ \mathtt{RR} \\ \mathtt{RR} \end{bmatrix}, \begin{bmatrix} \mathtt{BB} \\ \mathtt{BB} \\ \mathtt{BB} \\ \mathtt{BB} \end{bmatrix}, \begin{bmatrix} \mathtt{GG} \\ \mathtt{GG} \\ \mathtt{GG} \\ \mathtt{GG} \end{bmatrix}, \begin{bmatrix} \mathtt{RG} \\ \mathtt{RG} \\ \mathtt{RG} \\ \mathtt{RG} \end{bmatrix} \right\}$$

$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} \mathtt{RR} \\ \mathtt{GG} \\ \mathtt{BB} \\ \mathtt{RG} \end{bmatrix}, \begin{bmatrix} \mathtt{RG} \\ \mathtt{RR} \\ \mathtt{GG} \\ \mathtt{BB} \end{bmatrix}, \begin{bmatrix} \mathtt{BB} \\ \mathtt{RG} \\ \mathtt{RR} \\ \mathtt{GG} \end{bmatrix}, \begin{bmatrix} \mathtt{GG} \\ \mathtt{BB} \\ \mathtt{RG} \\ \mathtt{RR} \end{bmatrix} \right\}.$$

Here is another example. Let $n = 10$. Then we have that $m = 3$ and $\mathcal{S} = \{\mathtt{RRR}, \mathtt{GGG}, \mathtt{BBB}, \mathtt{RGB}, \mathtt{RBG}, \mathtt{BGR}, \mathtt{BRG}, \mathtt{GRB}, \mathtt{GBR}, \mathtt{RRG}, \mathtt{RGR}, \mathtt{GRR}, \mathtt{RRB}, \mathtt{RBR}, \mathtt{BRR}, \mathtt{GGR}, \mathtt{GRG}, \mathtt{RGG}, \mathtt{GGB}, \mathtt{GBG}, \mathtt{BGG}, \mathtt{BBR}, \mathtt{BRB}, \mathtt{RBB}, \mathtt{BBG}, \mathtt{BGB}, \mathtt{GBB}\}$. We choose the following 10 elements of $\mathcal{S}$: $\{\mathtt{RGB}, \mathtt{RBG}, \mathtt{BGR}, \mathtt{BRG}, \mathtt{GRB}, \mathtt{GBR}, \mathtt{RRG}, \mathtt{RGR}, \mathtt{GRR}, \mathtt{RRB}\}$.

The collections of distribution matrices are shown in Table 3.

Theorem 5.6. *Construction 5.5 gives a $(2, n)$-threshold scheme with pixel expansion $m = \lceil \log_3 n \rceil$, $\ell = 0$ and $h = 1$ (and thus contrast $\alpha = 1/\lceil \log_3 n \rceil$).*

Proof. Let $s_1, s_2, \ldots, s_n$ be the strings used for the construction of the scheme. Security property: For any participant i, the set $\mathcal{D}_\circ = \{M|i$, for each $M \in \mathcal{C}_\circ\}$, and $\mathcal{D}_\bullet = \{M|i$, for each $M \in \mathcal{C}_\bullet\}$, are both equal to the set $\{s_1, s_2, \ldots, s_n\}$. Contrast

Table 3
Example for Construction 5.5.

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} \texttt{RGB} \\ \texttt{RGB} \\ \texttt{RGB} \\ \texttt{RGB} \\ \texttt{RGB} \\ \texttt{RGB} \\ \texttt{RGB} \\ \texttt{RGB} \\ \texttt{RGB} \end{bmatrix}, \begin{bmatrix} \texttt{RBG} \\ \texttt{RBG} \\ \texttt{RBG} \\ \texttt{RBG} \\ \texttt{RBG} \\ \texttt{RBG} \\ \texttt{RBG} \\ \texttt{RBG} \\ \texttt{RBG} \end{bmatrix}, \begin{bmatrix} \texttt{BGR} \\ \texttt{BGR} \\ \texttt{BGR} \\ \texttt{BGR} \\ \texttt{BGR} \\ \texttt{BGR} \\ \texttt{BGR} \\ \texttt{BGR} \\ \texttt{BGR} \end{bmatrix}, \begin{bmatrix} \texttt{BRG} \\ \texttt{BRG} \\ \texttt{BRG} \\ \texttt{BRG} \\ \texttt{BRG} \\ \texttt{BRG} \\ \texttt{BRG} \\ \texttt{BRG} \\ \texttt{BRG} \end{bmatrix}, \begin{bmatrix} \texttt{GRB} \\ \texttt{GRB} \\ \texttt{GRB} \\ \texttt{GRB} \\ \texttt{GRB} \\ \texttt{GRB} \\ \texttt{GRB} \\ \texttt{GRB} \\ \texttt{GRB} \end{bmatrix}, \begin{bmatrix} \texttt{GBR} \\ \texttt{GBR} \\ \texttt{GBR} \\ \texttt{GBR} \\ \texttt{GBR} \\ \texttt{GBR} \\ \texttt{GBR} \\ \texttt{GBR} \\ \texttt{GBR} \end{bmatrix}, \begin{bmatrix} \texttt{RRG} \\ \texttt{RRG} \\ \texttt{RRG} \\ \texttt{RRG} \\ \texttt{RRG} \\ \texttt{RRG} \\ \texttt{RRG} \\ \texttt{RRG} \\ \texttt{RRG} \end{bmatrix}, \begin{bmatrix} \texttt{RGR} \\ \texttt{RGR} \\ \texttt{RGR} \\ \texttt{RGR} \\ \texttt{RGR} \\ \texttt{RGR} \\ \texttt{RGR} \\ \texttt{RGR} \\ \texttt{RGR} \end{bmatrix}, \begin{bmatrix} \texttt{GRR} \\ \texttt{GRR} \\ \texttt{GRR} \\ \texttt{GRR} \\ \texttt{GRR} \\ \texttt{GRR} \\ \texttt{GRR} \\ \texttt{GRR} \\ \texttt{GRR} \end{bmatrix}, \begin{bmatrix} \texttt{RRB} \\ \texttt{RRB} \\ \texttt{RRB} \\ \texttt{RRB} \\ \texttt{RRB} \\ \texttt{RRB} \\ \texttt{RRB} \\ \texttt{RRB} \\ \texttt{RRB} \end{bmatrix} \right\}$$

$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} \texttt{RGB} \\ \texttt{RBG} \\ \texttt{BGR} \\ \texttt{BRG} \\ \texttt{GRB} \\ \texttt{GBR} \\ \texttt{RRG} \\ \texttt{RGR} \\ \texttt{GRR} \end{bmatrix}, \begin{bmatrix} \texttt{RRB} \\ \texttt{RGB} \\ \texttt{RBG} \\ \texttt{BGR} \\ \texttt{BRG} \\ \texttt{GBR} \\ \texttt{GRR} \\ \texttt{RGR} \\ \texttt{RRG} \end{bmatrix}, \begin{bmatrix} \texttt{GRR} \\ \texttt{RRB} \\ \texttt{RGB} \\ \texttt{RBG} \\ \texttt{BGR} \\ \texttt{BRG} \\ \texttt{RRG} \\ \texttt{GRR} \\ \texttt{RGR} \end{bmatrix}, \begin{bmatrix} \texttt{RGR} \\ \texttt{GRR} \\ \texttt{RRB} \\ \texttt{RGB} \\ \texttt{RBG} \\ \texttt{BGR} \\ \texttt{BRG} \\ \texttt{RRG} \\ \texttt{GRR} \end{bmatrix}, \begin{bmatrix} \texttt{RRG} \\ \texttt{RGR} \\ \texttt{GRR} \\ \texttt{RRB} \\ \texttt{RGB} \\ \texttt{RBG} \\ \texttt{BRG} \\ \texttt{BGR} \\ \texttt{GBR} \end{bmatrix}, \begin{bmatrix} \texttt{GBR} \\ \texttt{RRG} \\ \texttt{RGR} \\ \texttt{GRR} \\ \texttt{RRB} \\ \texttt{RGB} \\ \texttt{RBG} \\ \texttt{BRG} \\ \texttt{GRB} \end{bmatrix}, \begin{bmatrix} \texttt{GRB} \\ \texttt{GBR} \\ \texttt{RRG} \\ \texttt{RGR} \\ \texttt{GRR} \\ \texttt{RRB} \\ \texttt{RGB} \\ \texttt{RBG} \\ \texttt{BRG} \end{bmatrix}, \begin{bmatrix} \texttt{BRG} \\ \texttt{GRB} \\ \texttt{GBR} \\ \texttt{RRG} \\ \texttt{RGR} \\ \texttt{GRR} \\ \texttt{RRB} \\ \texttt{RGB} \\ \texttt{BGR} \end{bmatrix}, \begin{bmatrix} \texttt{BGR} \\ \texttt{BRG} \\ \texttt{GRB} \\ \texttt{GBR} \\ \texttt{RRG} \\ \texttt{RGR} \\ \texttt{GRR} \\ \texttt{RRB} \\ \texttt{RGB} \end{bmatrix}, \begin{bmatrix} \texttt{RBG} \\ \texttt{BGR} \\ \texttt{BRG} \\ \texttt{GRB} \\ \texttt{GBR} \\ \texttt{RRG} \\ \texttt{RGR} \\ \texttt{GRR} \\ \texttt{RRB} \end{bmatrix} \right\}$$

property: Take any two participants i and j. If the secret pixel is white then we have that the shares of i and j are both equal to one of the base strings, say s_k, with $k \in 1, 2, \ldots, n$. Hence we have that $w_\bullet(\texttt{add}(s_k, s_k)) = 0$, that is $\ell = 0$.

If the secret pixel is black then we have that the two shares of i and j are equal to two different base string s_{k_1} and s_{k_2}. Since the two strings are different we have that $w_\bullet(\texttt{add}(s_{k_1}, s_{k_2})) \geqslant 1$, because there will be at least one position in which they differ. Recall that the superposition of two different colors in the set Σ gives black. Hence $h = 1$.

Finally the pixel expansion is $m = \lceil \log_3 n \rceil$ because each matrix in the collections has $\lceil \log_3 n \rceil$ columns. □

5.4. *Comparison* BW-VCS *vs.* CBW-VCS

The CBW-VC model is more powerful than the BW-VC model. This allows us to get schemes with smaller pixel expansion. This is made possible by the presence of colored pixels in the reconstructed image.

As an example, Fig. 5 compares the reconstructed images obtained with the $\mathcal{S}^{\mathrm{B}}_{2,n}$ BW-VCS and the reconstructed image obtained with the CBW-VC scheme presented in this section, for $n = 4, 8, 81$.

Using the CBW-VC model we can construct schemes that have pixel expansion $\lceil \log_3 n \rceil$. Although there is no improvement from an asymptotical point of view, the actual CBW-VCS do have a much smaller pixel expansion. Table 4 shows the explicit value of the lower bound of Theorem 2 and the pixel expansion of CBW-VC schemes.

As we have already pointed out, the fact that white areas are reconstructed as a mixture of colored pixels (instead of just black and white pixels) is not a problem for recognizing the image. Notice that the average light transmission of the CBW-VC scheme is proportional to that of the BW-VC scheme. In both cases the average light transmission gradually degrades when n increases.

6. Impossibility results

In this section we prove that the extra power of the CBW-VC model allows to construct schemes without pixel expansion only for the cases of $(2, 2)$-threshold and $(2, 3)$-threshold schemes. Indeed we show in this section that it is not possible to construct $(2, n)$-threshold schemes, for $n \geqslant 4$, nor (k, n)-threshold schemes, for $k \geqslant 3$, without pixel expansion.

In the following we will use $\star$ to denote a number in the interval $[0, 1]$ and $+$ to denote a positive number in the interval $]0, 1]$.

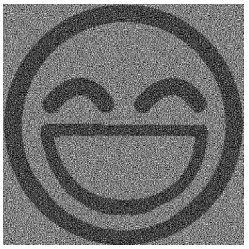
Theorem 6.1. *In the* CBW-VC *model it is not possible to construct a* $(2, n)$*-threshold scheme, for* $n \geqslant 4$*, with pixel expansion* $m = 1$.

Proof. By contradiction assume that such a scheme exists and let $\mathcal{C}_\circ, \mathcal{C}_\bullet$ be the collections of distribution matrices. Let B be a distribution matrix for a black secret pixel, that is $B \in \mathcal{C}_\bullet$. Since $m = 1$ matrix B has one column:

$$B = \begin{bmatrix} (\star, \star, \star) \\ (\star, \star, \star) \\ \cdots \\ (\star, \star, \star) \\ (\star, \star, \star) \end{bmatrix}.$$

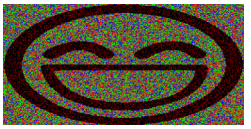
Secret image

(100x100px)



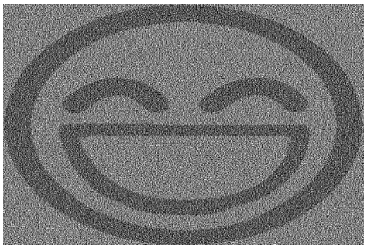
$(2,4)$ BW-VCS, $m=4$

(200x200px)



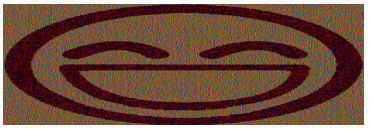
$(2,4)$ CBW-VCS, $m=2$

(200x100px)



$(2,8)$ BW-VCS, $m=6$

(300x200px)



$(2,8)$ CBW-VCS, $m=3$

(300x100px)

Fig. 5. Reconstruction comparison for $(2,n)$-threshold schemes.

Table 4
Pixel expansion comparison.

n	2	3	4	5	6	7	8	9	10	11	12
Theorem 2 (BW-VC lower bound), $m \geqslant$	2	3	4	4	4	5	5	5	5	6	6
$\mathcal{S}^{B}_{2,n}$ (BW-VCS), $m=$	2	4	4	6	6	6	6	6	8	8	8
Construction 5.5 (CBW-VCS), $m=$	1	1	2	2	2	2	2	2	3	3	3

Since $m=1$ we must have $\ell=0$ and $h=1$. This means that it must be $\mathtt{add}(B|X)=\bullet=(0,0,0)$ for any qualified set X. It also means that $\mathtt{add}(W|X)=\circ=(1,1,1)$ for any $W\in\mathcal{C}_{\circ}$.

Claim 1: B cannot have two pixels that are equal, with the exception of black pixels. Indeed if there are two pixels that are equal and are different from the black pixels the qualified set of 2 participants corresponding to those two pixels would reconstructed a black pixel as a colored pixel violating the contrast property.

Claim 2: Any pixel in B cannot be $\bullet$, that is cannot have the form $(0,0,0)$. Indeed such a triple, for the security property has to appear also in a distribution matrix for the white color. But this violates the contrast property because all the qualified sets that contain a participant that get $\bullet$ as a share for the white pixel would not be able to reconstruct white pixels.

Claim 3: Any pixel in B cannot have the form $(+,+,+)$, and thus, in particular, cannot be $\circ$. Indeed if $(+,+,+)$ appears in a row of B then all other $k-1\geqslant 3$ row of B should be $(0,0,0)$ because any qualified set must reconstruct black pixels as black. But by Claim 2, we know that this is not possible.

Claim 4: Any pixel in B cannot have one component equal to 0 and two components equal to $+$. Indeed if $(0,+,+)$ appears in a row of B then all other $k-1\geqslant 3$ rows of B should be $(+,0,0)$ because any qualified set must reconstruct black pixels as black. We know, by Claim 1, that this is not possible. We get the same contradiction for the other two cases $(+,0,+)$ and $(+,+,0)$.

By Claims 1–4, we have that all the pixels of B must be different and each must have the one of the forms $(0,0,+)$, $(0,+,0)$, $(+,0,0)$. However since we have at least $k\geqslant 4$ rows in B this is impossible. □

Theorem 6.2. *In the* CBW-VC *model it is not possible to construct a* (k, n)*-threshold scheme, for* $k \geqslant 3$*, with pixel expansion* $m = 1$.

Proof. By contradiction assume that such a scheme exists and let $\mathcal{C}_\circ, \mathcal{C}_\bullet$ be the collections of distribution matrices. Let B be a distribution matrix for a black secret pixel, that is $B \in \mathcal{C}_\bullet$. Since $m = 1$ matrix M has one column:

$$B = \begin{bmatrix} (\star, \star, \star) \\ (\star, \star, \star) \\ \cdots \\ (\star, \star, \star) \\ (\star, \star, \star) \end{bmatrix}.$$

Since $m = 1$ we must have $\ell = 0$ and $h = 1$. This means that it must be $\mathtt{add}(B|X) = \bullet = (0, 0, 0)$ for any qualified set X. It also means that $\mathtt{add}(W|X) = \circ = (1, 1, 1)$ for any $W \in \mathcal{C}_\circ$.
Claim 1: Any pixel in B cannot be $\bullet$. Indeed for the security property such a pixel should appear also in a distribution matrix $W \in \mathcal{C}_\circ$. Then we would have $\mathtt{add}(W|X) = \bullet = (0, 0, 0)$ for any qualified set X and this violates the contrast property.
Claim 2: Any pixel in B cannot have 2 components equal to 0, that is cannot have the form $(0, 0, +)$, $(0, +, 0)$ or $(+, 0, 0)$. For the sake of contradiction, assume that B has such a pixel. Assume that the pixel is $(0, 0, +)$; the following reasoning is valid, with the obvious modifications, also for the other cases, so the assumption is without loss of generality. In order to have $\mathtt{add}(B) = (0, 0, 0)$ matrix B must have another pixel equal to $(\star, \star, 0)$. That is, matrix B must have the form

$$B = \begin{bmatrix} \cdots \\ (0, 0, +) \\ \cdots \\ (\star, \star, 0) \\ \cdots \end{bmatrix}.$$

Notice that all the reasoning is up to a permutation of the rows. Since $k \geqslant 3$, for the security property the same pair must appear in a distribution matrix $W \in \mathcal{C}_\circ$ for the white color. But this implies that $\mathtt{add}(W) = (0, 0, 0)$. This violates the contrast property. Hence the claim is true.

Claims 1 and 2 imply that the pixels in matrix B must have either the form $(+, +, +)$ or one of the form $(0, +, +), (+, 0, +), (+, +, 0)$. We now distinguish two cases: $k = 3$ and $k \geqslant 4$.

Case $k = 3$: Matrix B cannot have pixels of the form $(+, +, +)$. Indeed if this was the case it would be impossible to have $\mathtt{add}(B) = \bullet$. Indeed since $k = 3$ and pixels can only be $(+, +, +)$ or have at most one component equal to 0, superposing 3 pixels will always yield at least one component greater than 0. This means that pixels must have one component equal to 0 and the other two components equal to $+$. Since $k = 3$ the only possible form (up to a permutation of the rows) for matrix B is

$$B = \begin{bmatrix} (0, +, +) \\ (+, 0, +) \\ (+, +, 0) \end{bmatrix}.$$

Consider now any two rows of B, for example the first and the second. By the security property we have that the same two rows must appear in a matrix $W \in \mathcal{C}_\circ$. That is, there is $W \in \mathcal{C}_\circ$ such that

$$W = \begin{bmatrix} (0, +, +) \\ (+, 0, +) \\ (\star, \star, \star) \end{bmatrix}.$$

The $(\star, \star, \star)$ row of W cannot be $(+, +, 0)$ otherwise we would have $\mathtt{add}(W) = \bullet$ and this would violate the contrast property. Hence it must be either

$$W = \begin{bmatrix} (0, +, +) \\ (+, 0, +) \\ (0, +, +) \end{bmatrix} \quad \text{or} \quad W = \begin{bmatrix} (0, +, +) \\ (+, 0, +) \\ (+, 0, +) \end{bmatrix}.$$

In both cases we have two pixels that are equal. For the security property such a pair of pixels should appear also in B. But this contradicts the fact that B must have 3 different pixels. Hence we have that matrix B cannot exist. This concludes the proof for the case $k = 3$.

Case $k \geqslant 4$: In this case matrix B can have pixels of the form $(+, +, +)$. However it can have at most one such a pixel. Indeed if B had 2 or more of such pixels, then it would be possible to select a qualified set X for which it would be impossible to have $\mathtt{add}(B|X) = \bullet$. Indeed since pixels can only be $(+, +, +)$ or have at most one component equal to 0, superposing 4 pixels, among which at least 2 are $(+, +, +)$, will always yield at least one component greater than 0.

Thus, denoting by X a qualified set, in order to have $\mathtt{add}(B|X) = \bullet$, it must be the case that matrix B has the following form

$$B = \begin{bmatrix} \cdots \\ (\star,\star,\star) \\ \cdots \\ (0,+,+) \\ \cdots \\ (+,0,+) \\ \cdots \\ (+,+,0) \\ \cdots \end{bmatrix},$$

where the pixels made explicit are those of $B|X$ and the $(\star,\star,\star)$ pixel is either $(+,+,+)$ or one of $(0,+,+)$, $(+,+,0)$, $(+,+,0)$.

By the security property, since $k \geqslant 4$ the triple of pixels $(0,+,+)$, $(+,+,0)$, $(+,+,0)$ must appear also in a matrix $W \in \mathcal{C}_\circ$. That is, for a matrix $W \in \mathcal{C}_\circ$ we have

$$W = \begin{bmatrix} \cdots \\ (0,+,+) \\ \cdots \\ (+,0,+) \\ \cdots \\ (+,+,0) \\ \cdots \end{bmatrix}.$$

This implies that $\mathtt{add}(W) = \bullet$ which violates the contrast property. Hence we have that B cannot exist, and this concludes the proof for $k \geqslant 4$. □

7. PB-CBW-VC (k, n)-threshold schemes

In this section we provide a general technique that allows us to transform any BW-VC (k, n)-threshold scheme with perfect black reconstruction (PB-BW-VCS for short) into a CBW-VC (k, n)-threshold scheme with perfect black reconstruction (PB-BW-VCS for short). However we first present a simple construction of $(2, n)$-threshold schemes with pixel expansion $\lceil n/3 \rceil$. The general construction that we will see later will also produce schemes with the same pixel expansion for the case $k = 2$. We provide also the next construction because it is very simple and directly constructs a scheme, while the general construction starts from a BW-VCS.

7.1. PB-CBW-VCS $(2, n)$-threshold scheme

The construction is very similar to Construction 5.5, with the basic difference that the alphabet used contains also the symbol for black.

Construction 7.1. *Let $m = \lceil n/3 \rceil$. Consider the set $\mathcal{S}$ of all the strings of length m with $m - 1$ characters equal to $\bullet$ and 1 character chosen in the alphabet $\Sigma = \{\mathtt{R}, \mathtt{G}, \mathtt{B}\}$. These are $3m \geqslant n$. Choose any n such strings and denote them $s_1, s_2, \ldots, s_n$. The collection of distribution matrices of the scheme are as the ones used in Construction 5.5 and shown in Table 2.*

An example will clarify the construction. Let $n = 5$. We have that $m = 2$ and $\mathcal{S} = \{\bullet\mathtt{R}, \bullet\mathtt{G}, \bullet\mathtt{B}, \mathtt{R}\bullet, \mathtt{G}\bullet, \mathtt{B}\bullet\}$. We choose the following 5 elements of $\mathcal{S}$: $\{\bullet\mathtt{R}, \bullet\mathtt{G}, \bullet\mathtt{B}, \mathtt{R}\bullet, \mathtt{G}\bullet\}$. The collections of distribution matrices are:

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} \bullet\mathtt{R} \\ \bullet\mathtt{R} \\ \bullet\mathtt{R} \\ \bullet\mathtt{R} \\ \bullet\mathtt{R} \end{bmatrix}, \begin{bmatrix} \bullet\mathtt{G} \\ \bullet\mathtt{G} \\ \bullet\mathtt{G} \\ \bullet\mathtt{G} \\ \bullet\mathtt{G} \end{bmatrix}, \begin{bmatrix} \bullet\mathtt{B} \\ \bullet\mathtt{B} \\ \bullet\mathtt{B} \\ \bullet\mathtt{B} \\ \bullet\mathtt{B} \end{bmatrix}, \begin{bmatrix} \mathtt{R}\bullet \\ \mathtt{R}\bullet \\ \mathtt{R}\bullet \\ \mathtt{R}\bullet \\ \mathtt{R}\bullet \end{bmatrix}, \begin{bmatrix} \mathtt{G}\bullet \\ \mathtt{G}\bullet \\ \mathtt{G}\bullet \\ \mathtt{G}\bullet \\ \mathtt{G}\bullet \end{bmatrix} \right\}$$

$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} \bullet\mathtt{R} \\ \bullet\mathtt{G} \\ \bullet\mathtt{B} \\ \mathtt{R}\bullet \\ \mathtt{G}\bullet \end{bmatrix}, \begin{bmatrix} \mathtt{G}\bullet \\ \bullet\mathtt{R} \\ \bullet\mathtt{G} \\ \bullet\mathtt{B} \\ \mathtt{R}\bullet \end{bmatrix}, \begin{bmatrix} \mathtt{R}\bullet \\ \mathtt{G}\bullet \\ \bullet\mathtt{R} \\ \bullet\mathtt{G} \\ \bullet\mathtt{B} \end{bmatrix}, \begin{bmatrix} \bullet\mathtt{B} \\ \mathtt{R}\bullet \\ \mathtt{G}\bullet \\ \bullet\mathtt{R} \\ \bullet\mathtt{G} \end{bmatrix}, \begin{bmatrix} \bullet\mathtt{G} \\ \bullet\mathtt{B} \\ \mathtt{R}\bullet \\ \mathtt{G}\bullet \\ \bullet\mathtt{R} \end{bmatrix} \right\}.$$

Theorem 7.2. *Construction 7.1 gives a $(2, n)$-threshold scheme with pixel expansion $m = \lceil n/3 \rceil$, $\ell = m - 1$ and $h = m$ (and thus contrast $\alpha = 1/\lceil n/3 \rceil$).*

Proof. Let $s_1, s_2, \ldots, s_n$ be the base strings used for the construction of the scheme. Security property: For any participant i, the set $\mathcal{D}_\circ = \{M|i, \text{ for each } M \in \mathcal{C}_\circ\}$, and $\mathcal{D}_\bullet = \{M|i, \text{ for each } M \in \mathcal{C}_\bullet\}$, are both equal to the set $\{s_1, s_2, \ldots, s_n\}$.

Contrast property: Take any two participants i and j. If the secret pixel is white then we have that the shares of i and j are both equal to one of the base strings, say s_k, with $k \in 1, 2, \ldots, n$. Hence we have that $w_\bullet(\mathtt{add}(s_k, s_k)) = m - 1$ (recall that the base strings are made up of $n - 1$ characters $\bullet$ and a character equal to one of {R, G, B}). Hence $\ell = m - 1$.

If the secret pixel is black then we have that the two shares of i and j are equal to two different base string s_{k_1} and s_{k_2}. Since the two strings are different we have that $w_\bullet(\mathtt{add}(s_{k_1}, s_{k_2})) = m$, because either we superpose a $\bullet$ pixel or we superpose two pixels with different colors (in either case we get a black pixel). Hence $h = m$.

Finally the pixel expansion is $m = \lceil n/3 \rceil$ because each matrix in the collections has $\lceil n/3 \rceil$ columns. □

7.2. PB-CBW-VCS (k, n)-threshold schemes

In this section we present a general technique that allows us to take any BW-VCS with perfect reconstruction of black pixels and to transform it into a CBW-VCS with perfect reconstruction of black pixels.[4] The technique works only for schemes with perfect reconstruction of black pixels and not for schemes that do not have this property. This is because if we do not have this property we cannot guarantee that black pixels are reconstructed with a sufficient number of black subpixels and there are cases where we can end up with a black secret pixel being reconstructed with less black subpixels than a white secret pixel. The idea is to group the black and white pixels in triples and transform each triple into a color. Since each triple of pixels is transformed into 1 colored pixel, the pixel expansion of the constructed scheme is $m = \lceil m'/3 \rceil$, where m' is the pixel expansion of the starting scheme.

Let us start by describing the transformation from a black and white distribution matrix M' to a color distribution matrix M.

Transformation 7.3. *Let M' be an $n \times m$ black and white distribution matrix. If m is not a multiple of 3 then add either 1 or 2 columns with all black pixels to M'. It is not important where these columns are added but to make things easier let's assume that these added columns are appended as last columns of M. Then group the $m = 3z$ columns of M into z groups of 3 columns. For each row (triple) in each group substitute the 3 black and white pixels with the colored pixels specified by the following table*:

Triplet in matrix M'			Color in matrix M
Column 1	Column 2	Column 3	
○	○	○	○
●	○	○	Y
○	●	○	M
○	○	●	C
●	●	○	B
●	○	●	G
○	●	●	R
●	●	●	●

Let us see an example of the above transformation. Consider the black and white distribution matrix M':

$$M' = \begin{bmatrix} ○ & ● & ○ & ● & ● & ○ & ● \\ ● & ○ & ● & ○ & ○ & ● & ○ \\ ● & ● & ● & ● & ● & ● & ○ \\ ○ & ● & ● & ○ & ○ & ○ & ● \\ ○ & ○ & ● & ○ & ● & ○ & ○ \end{bmatrix}.$$

Since $m = 7$ we add two extra columns with black pixels and group the columns into 3 groups:

$$M' = \left[\begin{array}{ccc|ccc|ccc} ○ & ● & ○ & ● & ● & ○ & ● & ● & ● \\ ● & ○ & ● & ○ & ○ & ● & ○ & ● & ● \\ ○ & ○ & ● & ● & ● & ● & ○ & ● & ● \\ ○ & ● & ● & ○ & ○ & ○ & ● & ● & ● \\ ● & ○ & ○ & ○ & ● & ○ & ○ & ● & ● \end{array}\right].$$

[4] The technique works also for general access structure schemes.

Table 5
Example for Construction 7.4: The collection $\mathcal{C}'_\circ$ for a $(3,3)$-threshold scheme.

$\mathcal{C}'_\circ =$ { $(\sigma\colon 1234)$ $(\sigma\colon 1243)$ $(\sigma\colon 1324)$ $(\sigma\colon 1423)$ $(\sigma\colon 1342)$ $(\sigma\colon 1432)$ $(\sigma\colon 2134)$ $(\sigma\colon 2143)$ $(\sigma\colon 3124)$ $(\sigma\colon 4123)$ $(\sigma\colon 3142)$ $(\sigma\colon 4132)$ $(\sigma\colon 2314)$ $(\sigma\colon 2413)$ $(\sigma\colon 3214)$ $(\sigma\colon 4213)$ $(\sigma\colon 3412)$ $(\sigma\colon 4312)$ $(\sigma\colon 2341)$ $(\sigma\colon 2431)$ $(\sigma\colon 3241)$ $(\sigma\colon 4231)$ $(\sigma\colon 3421)$ $(\sigma\colon 4321)$ }

Finally for each triple we substitute a color as specified in the substitution table:

$$M = \begin{bmatrix} \mathtt{M} & \mathtt{B} & \bullet \\ \mathtt{G} & \mathtt{C} & \mathtt{R} \\ \mathtt{C} & \bullet & \mathtt{R} \\ \mathtt{R} & \circ & \bullet \\ \mathtt{Y} & \mathtt{M} & \mathtt{R} \end{bmatrix}.$$

Since matrices M' and M are closely related the following holds. Let $z' = \mathtt{add}(M')$ and let z be the vector obtained by transforming vector z' with Transformation 7.3. Then we have that $z = \mathtt{add}(M)$. For the above example we would have that $z' = [\bullet\bullet\bullet|\bullet\bullet\bullet|\bullet\bullet\bullet]$ and $z = [\bullet\bullet\bullet]$ and $\mathtt{add}(M) = [\bullet\bullet\bullet]$. As another example let $X = \{2, 3, 5\}$ and consider the matrix $M'|X$. Let $z' = \mathtt{add}(M'|X)$. We have that $z' = [\bullet\circ\bullet|\circ\bullet\bullet|\circ\bullet\bullet]$ and thus $z = [\mathtt{GRR}]$. We also have $\mathtt{add}(M) = [\mathtt{GRR}]$. With an abuse of notation we will write that $\mathtt{add}(M') = \mathtt{add}(M)$.

We are now ready to present the construction for PB-CBW-VC (k, n)-threshold schemes.

Construction 7.4. *Let S' be a* BW-VCS *with perfect reconstruction of black pixel whose collections of distribution matrices are $\mathcal{C}'_\circ$ and $\mathcal{C}'_\bullet$ and let m' be the pixel expansion of S'. The* CBW-VCS *scheme S is defined by the two collections $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ obtained from $\mathcal{C}'_\circ$ and $\mathcal{C}'_\bullet$ by applying Transformation 7.3 to every matrix in the collections.*

Applying Construction 7.4 to the BW-VCS $S' = \mathcal{S}^{\mathrm{NS}}_{2,2}$ we obtain one of the schemes presented in Section 5.1.

As a more significant example of use of Construction 7.4 let us apply it to the BW-VC $(3, 3)$-threshold scheme $S' = \mathcal{S}^{\mathrm{NS}}_{3,3}$ defined by the base matrices:

$$B_\circ = \begin{bmatrix} \circ & \bullet & \bullet & \circ \\ \bullet & \circ & \bullet & \circ \\ \bullet & \bullet & \circ & \circ \end{bmatrix} \qquad B_\bullet = \begin{bmatrix} \bullet & \bullet & \circ & \circ \\ \bullet & \circ & \bullet & \circ \\ \bullet & \circ & \circ & \bullet \end{bmatrix}.$$

Tables 5 and 6 show the collections $\mathcal{C}'_\circ$ and $\mathcal{C}'_\bullet$ for scheme $\mathcal{S}^{\mathrm{NS}}_{3,3}$ with matrices already padded with two columns of black pixels in order to have a number of columns that is multiple of 3, and Tables 7 and 8 show the collections $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ that describe the PB-CBW-VCS obtained with Construction 7.4. For each distribution matrix in the collections we have also specified the corresponding permutation of the columns of the base matrix.

Theorem 7.5. *Construction 7.4 provides a (k, n)-*CBW-VCS*-threshold scheme with pixel expansion $m = \lceil m'/3 \rceil$, where m' is the pixel expansion of the starting (k, n)-*VCS*-threshold scheme.*

Proof. Let S' be the starting PB-BW-VCS with collections $\mathcal{C}'_\circ$ and $\mathcal{C}'_\bullet$ and let m' be the pixel expansion of S. Let S be the scheme obtained from S' using Construction 7.4.

Security property. Let X be a non-qualified set of participants. Consider the sets of matrices $\{M|X\colon\ M \in \mathcal{C}'_\circ\}$ and $\{M|X\colon\ M \in \mathcal{C}'_\bullet\}$. By the safety property for S' we have that A and B contain the same matrices each with the same frequency. Since each matrix of $\in \mathcal{C}'_\circ$ is transformed into a matrix of $\in \mathcal{C}_\bullet$ and each matrix of $\in \mathcal{C}'_\bullet$ is transformed into a matrix

Table 6
Example for Construction 7.4: The collection $\mathcal{C}'_\bullet$ for a $(3,3)$-threshold scheme.

$\mathcal{C}'_\bullet = \Big\{$

$\begin{bmatrix}\bullet\bullet\circ\circ\bullet\bullet\bullet\\ \bullet\circ\bullet\circ\bullet\bullet\bullet\\ \bullet\circ\circ\bullet\bullet\bullet\end{bmatrix}$ (σ: 1234)	$\begin{bmatrix}\bullet\bullet\circ\circ\bullet\bullet\bullet\\ \bullet\circ\circ\bullet\bullet\bullet\\ \bullet\circ\bullet\circ\bullet\bullet\end{bmatrix}$ (σ: 1243)	$\begin{bmatrix}\bullet\circ\bullet\circ\bullet\bullet\\ \bullet\bullet\circ\circ\bullet\bullet\\ \bullet\circ\circ\bullet\bullet\bullet\end{bmatrix}$ (σ: 1324)	$\begin{bmatrix}\bullet\circ\circ\bullet\bullet\bullet\\ \bullet\bullet\circ\circ\bullet\bullet\\ \bullet\circ\bullet\circ\bullet\bullet\end{bmatrix}$ (σ: 1423)	$\begin{bmatrix}\bullet\circ\bullet\circ\bullet\bullet\\ \bullet\circ\circ\bullet\bullet\bullet\\ \bullet\bullet\circ\circ\bullet\bullet\end{bmatrix}$ (σ: 1342)	$\begin{bmatrix}\bullet\circ\circ\bullet\bullet\bullet\\ \bullet\circ\bullet\circ\bullet\bullet\\ \bullet\bullet\circ\circ\bullet\bullet\end{bmatrix}$ (σ: 1432)
$\begin{bmatrix}\bullet\bullet\circ\circ\bullet\bullet\\ \circ\bullet\bullet\circ\bullet\bullet\\ \circ\bullet\circ\bullet\bullet\bullet\end{bmatrix}$ (σ: 2134)	$\begin{bmatrix}\bullet\bullet\circ\circ\bullet\bullet\\ \circ\bullet\circ\bullet\bullet\bullet\\ \circ\bullet\bullet\circ\bullet\bullet\end{bmatrix}$ (σ: 2143)	$\begin{bmatrix}\bullet\circ\bullet\circ\bullet\bullet\\ \circ\bullet\bullet\circ\bullet\bullet\\ \circ\circ\bullet\bullet\bullet\bullet\end{bmatrix}$ (σ: 3124)	$\begin{bmatrix}\bullet\circ\circ\bullet\bullet\bullet\\ \circ\bullet\circ\bullet\bullet\bullet\\ \circ\circ\bullet\bullet\bullet\bullet\end{bmatrix}$ (σ: 4123)	$\begin{bmatrix}\bullet\circ\bullet\circ\bullet\bullet\\ \circ\circ\bullet\bullet\bullet\bullet\\ \circ\bullet\circ\bullet\bullet\bullet\end{bmatrix}$ (σ: 3142)	$\begin{bmatrix}\bullet\circ\circ\bullet\bullet\bullet\\ \circ\circ\bullet\bullet\bullet\bullet\\ \circ\bullet\bullet\circ\bullet\bullet\end{bmatrix}$ (σ: 4132)
$\begin{bmatrix}\circ\bullet\bullet\circ\bullet\bullet\\ \bullet\bullet\circ\circ\bullet\bullet\\ \circ\bullet\circ\bullet\bullet\bullet\end{bmatrix}$ (σ: 2314)	$\begin{bmatrix}\circ\bullet\circ\bullet\bullet\bullet\\ \bullet\bullet\circ\circ\bullet\bullet\\ \circ\bullet\bullet\circ\bullet\bullet\end{bmatrix}$ (σ: 2413)	$\begin{bmatrix}\circ\bullet\bullet\circ\bullet\bullet\\ \bullet\circ\bullet\circ\bullet\bullet\\ \circ\circ\bullet\bullet\bullet\bullet\end{bmatrix}$ (σ: 3214)	$\begin{bmatrix}\circ\bullet\circ\bullet\bullet\bullet\\ \bullet\circ\circ\bullet\bullet\bullet\\ \circ\circ\bullet\bullet\bullet\bullet\end{bmatrix}$ (σ: 4213)	$\begin{bmatrix}\circ\circ\bullet\bullet\bullet\bullet\\ \bullet\circ\bullet\circ\bullet\bullet\\ \circ\bullet\bullet\circ\bullet\bullet\end{bmatrix}$ (σ: 3412)	$\begin{bmatrix}\circ\circ\bullet\bullet\bullet\bullet\\ \bullet\circ\circ\bullet\bullet\bullet\\ \circ\bullet\circ\bullet\bullet\bullet\end{bmatrix}$ (σ: 4312)
$\begin{bmatrix}\circ\bullet\bullet\circ\bullet\bullet\\ \circ\bullet\circ\bullet\bullet\bullet\\ \bullet\bullet\circ\circ\bullet\bullet\end{bmatrix}$ (σ: 2341)	$\begin{bmatrix}\circ\bullet\circ\bullet\bullet\bullet\\ \circ\bullet\bullet\circ\bullet\bullet\\ \bullet\bullet\circ\circ\bullet\bullet\end{bmatrix}$ (σ: 2431)	$\begin{bmatrix}\circ\bullet\bullet\circ\bullet\bullet\\ \circ\circ\bullet\bullet\bullet\bullet\\ \bullet\circ\bullet\circ\bullet\bullet\end{bmatrix}$ (σ: 3241)	$\begin{bmatrix}\circ\bullet\circ\bullet\bullet\bullet\\ \circ\circ\bullet\bullet\bullet\bullet\\ \bullet\circ\circ\bullet\bullet\bullet\end{bmatrix}$ (σ: 4231)	$\begin{bmatrix}\circ\circ\bullet\bullet\bullet\bullet\\ \circ\bullet\bullet\circ\bullet\bullet\\ \bullet\circ\bullet\circ\bullet\bullet\end{bmatrix}$ (σ: 3421)	$\begin{bmatrix}\circ\circ\bullet\bullet\bullet\bullet\\ \circ\bullet\circ\bullet\bullet\bullet\\ \bullet\circ\circ\bullet\bullet\bullet\end{bmatrix}$ (σ: 4321)

$\Big\}$

Table 7
Example for Construction 7.4: The collection $\mathcal{C}_\circ$ for a $(3,3)$-threshold scheme.

$\mathcal{C}_\circ = \Big\{$

$\begin{bmatrix}\mathrm{RR}\\ \mathrm{GR}\\ \mathrm{BR}\end{bmatrix}$ (σ: 1234)	$\begin{bmatrix}\mathrm{M}\bullet\\ \mathrm{Y}\bullet\\ \mathrm{BR}\end{bmatrix}$ (σ: 1243)	$\begin{bmatrix}\mathrm{RR}\\ \mathrm{BR}\\ \mathrm{GR}\end{bmatrix}$ (σ: 1324)	$\begin{bmatrix}\mathrm{M}\bullet\\ \mathrm{BR}\\ \mathrm{Y}\bullet\end{bmatrix}$ (σ: 1423)	$\begin{bmatrix}\mathrm{C}\bullet\\ \mathrm{Y}\bullet\\ \mathrm{GR}\end{bmatrix}$ (σ: 1342)	$\begin{bmatrix}\mathrm{C}\bullet\\ \mathrm{GR}\\ \mathrm{Y}\bullet\end{bmatrix}$ (σ: 1432)
$\begin{bmatrix}\mathrm{GR}\\ \mathrm{RR}\\ \mathrm{BR}\end{bmatrix}$ (σ: 2134)	$\begin{bmatrix}\mathrm{Y}\bullet\\ \mathrm{M}\bullet\\ \mathrm{BR}\end{bmatrix}$ (σ: 2143)	$\begin{bmatrix}\mathrm{BR}\\ \mathrm{RR}\\ \mathrm{GR}\end{bmatrix}$ (σ: 3124)	$\begin{bmatrix}\mathrm{BR}\\ \mathrm{M}\bullet\\ \mathrm{Y}\bullet\end{bmatrix}$ (σ: 4123)	$\begin{bmatrix}\mathrm{Y}\bullet\\ \mathrm{C}\bullet\\ \mathrm{GR}\end{bmatrix}$ (σ: 3142)	$\begin{bmatrix}\mathrm{GR}\\ \mathrm{C}\bullet\\ \mathrm{Y}\bullet\end{bmatrix}$ (σ: 4132)
$\begin{bmatrix}\mathrm{GR}\\ \mathrm{BR}\\ \mathrm{RR}\end{bmatrix}$ (σ: 2314)	$\begin{bmatrix}\mathrm{Y}\bullet\\ \mathrm{BR}\\ \mathrm{M}\bullet\end{bmatrix}$ (σ: 2413)	$\begin{bmatrix}\mathrm{BR}\\ \mathrm{GR}\\ \mathrm{RR}\end{bmatrix}$ (σ: 3214)	$\begin{bmatrix}\mathrm{BR}\\ \mathrm{Y}\bullet\\ \mathrm{M}\bullet\end{bmatrix}$ (σ: 4213)	$\begin{bmatrix}\mathrm{Y}\bullet\\ \mathrm{GR}\\ \mathrm{C}\bullet\end{bmatrix}$ (σ: 3412)	$\begin{bmatrix}\mathrm{GR}\\ \mathrm{Y}\bullet\\ \mathrm{C}\bullet\end{bmatrix}$ (σ: 4312)
$\begin{bmatrix}\mathrm{C}\bullet\\ \mathrm{M}\bullet\\ \mathrm{RR}\end{bmatrix}$ (σ: 2341)	$\begin{bmatrix}\mathrm{C}\bullet\\ \mathrm{RR}\\ \mathrm{M}\bullet\end{bmatrix}$ (σ: 2431)	$\begin{bmatrix}\mathrm{M}\bullet\\ \mathrm{C}\bullet\\ \mathrm{RR}\end{bmatrix}$ (σ: 3241)	$\begin{bmatrix}\mathrm{RR}\\ \mathrm{C}\bullet\\ \mathrm{M}\bullet\end{bmatrix}$ (σ: 4231)	$\begin{bmatrix}\mathrm{M}\bullet\\ \mathrm{RR}\\ \mathrm{C}\bullet\end{bmatrix}$ (σ: 3421)	$\begin{bmatrix}\mathrm{RR}\\ \mathrm{M}\bullet\\ \mathrm{C}\bullet\end{bmatrix}$ (σ: 4321)

$\Big\}$

Table 8
Example for Construction 7.4: The collection $\mathcal{C}_\bullet$ for a $(3,3)$-threshold scheme.

$\mathcal{C}_\bullet = \Big\{$

$\begin{bmatrix}\mathrm{BR}\\ \mathrm{GR}\\ \mathrm{Y}\bullet\end{bmatrix}$ (σ: 1234)	$\begin{bmatrix}\mathrm{BR}\\ \mathrm{Y}\bullet\\ \mathrm{GR}\end{bmatrix}$ (σ: 1243)	$\begin{bmatrix}\mathrm{GR}\\ \mathrm{BR}\\ \mathrm{Y}\bullet\end{bmatrix}$ (σ: 1324)	$\begin{bmatrix}\mathrm{Y}\bullet\\ \mathrm{BR}\\ \mathrm{GR}\end{bmatrix}$ (σ: 1423)	$\begin{bmatrix}\mathrm{GR}\\ \mathrm{Y}\bullet\\ \mathrm{BR}\end{bmatrix}$ (σ: 1342)	$\begin{bmatrix}\mathrm{Y}\bullet\\ \mathrm{GR}\\ \mathrm{BR}\end{bmatrix}$ (σ: 1432)
$\begin{bmatrix}\mathrm{BR}\\ \mathrm{RR}\\ \mathrm{M}\bullet\end{bmatrix}$ (σ: 2134)	$\begin{bmatrix}\mathrm{BR}\\ \mathrm{M}\bullet\\ \mathrm{RR}\end{bmatrix}$ (σ: 2143)	$\begin{bmatrix}\mathrm{GR}\\ \mathrm{RR}\\ \mathrm{C}\bullet\end{bmatrix}$ (σ: 3124)	$\begin{bmatrix}\mathrm{Y}\bullet\\ \mathrm{M}\bullet\\ \mathrm{C}\bullet\end{bmatrix}$ (σ: 4123)	$\begin{bmatrix}\mathrm{GR}\\ \mathrm{C}\bullet\\ \mathrm{RR}\end{bmatrix}$ (σ: 3142)	$\begin{bmatrix}\mathrm{Y}\bullet\\ \mathrm{C}\bullet\\ \mathrm{M}\bullet\end{bmatrix}$ (σ: 4132)
$\begin{bmatrix}\mathrm{RR}\\ \mathrm{BR}\\ \mathrm{M}\bullet\end{bmatrix}$ (σ: 2314)	$\begin{bmatrix}\mathrm{M}\bullet\\ \mathrm{BR}\\ \mathrm{RR}\end{bmatrix}$ (σ: 2413)	$\begin{bmatrix}\mathrm{RR}\\ \mathrm{GR}\\ \mathrm{C}\bullet\end{bmatrix}$ (σ: 3214)	$\begin{bmatrix}\mathrm{M}\bullet\\ \mathrm{Y}\bullet\\ \mathrm{C}\bullet\end{bmatrix}$ (σ: 4213)	$\begin{bmatrix}\mathrm{C}\bullet\\ \mathrm{GR}\\ \mathrm{RR}\end{bmatrix}$ (σ: 3412)	$\begin{bmatrix}\mathrm{C}\bullet\\ \mathrm{Y}\bullet\\ \mathrm{M}\bullet\end{bmatrix}$ (σ: 4312)
$\begin{bmatrix}\mathrm{RR}\\ \mathrm{M}\bullet\\ \mathrm{BR}\end{bmatrix}$ (σ: 2341)	$\begin{bmatrix}\mathrm{M}\bullet\\ \mathrm{RR}\\ \mathrm{BR}\end{bmatrix}$ (σ: 2431)	$\begin{bmatrix}\mathrm{RR}\\ \mathrm{C}\bullet\\ \mathrm{GR}\end{bmatrix}$ (σ: 3241)	$\begin{bmatrix}\mathrm{M}\bullet\\ \mathrm{C}\bullet\\ \mathrm{Y}\bullet\end{bmatrix}$ (σ: 4231)	$\begin{bmatrix}\mathrm{C}\bullet\\ \mathrm{RR}\\ \mathrm{GR}\end{bmatrix}$ (σ: 3421)	$\begin{bmatrix}\mathrm{C}\bullet\\ \mathrm{M}\bullet\\ \mathrm{Y}\bullet\end{bmatrix}$ (σ: 4321)

$\Big\}$

of $\in \mathcal{C}_\circ$ we have that also the sets $\{M|X\colon\ M \in \mathcal{C}_\circ\}$ and $\{M|X\colon\ M \in \mathcal{C}_\bullet\}$ have the same matrices with the same frequencies. Hence the safety property for S' is also satisfied.

Contrast property. Let X be a qualified set of participants. Consider any matrix $M \in \mathcal{C}_\bullet$ and let M' be the corresponding matrix in $\mathcal{C}'_\bullet$. By the construction we have that $\mathtt{add}(M|X) = \mathtt{add}(M'|X)$. Since S' is with perfect reconstruction of the black

Table 9
Pixel expansion comparison for small values of k and n.

$(2,n)$			$(3,n)$			$(n-1,n)$			(n,n)		
n	m BW VCS	m in CBW VCS	n	m BW VCS	m in CBW VCS	n	m BW VCS	m in CBW VCS	n	m BW VCS	m in CBW VCS
2	2	1	2	–	–	2	–	–	2	2	1
3	3	1	3	4	2	3	3	1	3	4	2
4	4	2	4	9	3	4	9	3	4	8	3
5	5	2	5	16	6	5	25	9	5	16	6
6	6	2	6	25	9	6	65	22	6	32	12

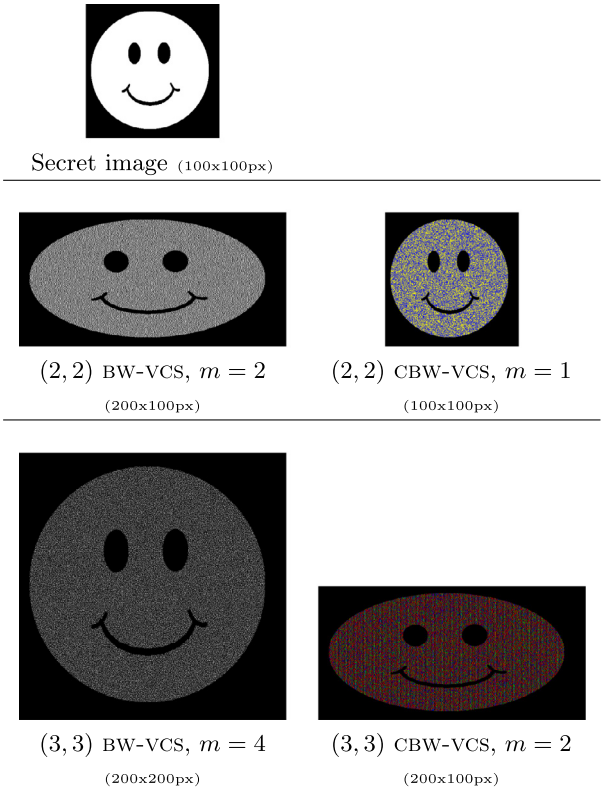


Fig. 6. Reconstruction comparison for (n,n)-threshold schemes.

pixels we have that $\mathtt{add}(M'|X)$ is made up of m' black pixels. Hence $\mathtt{add}(M|X)$ is made up of $m = m'/3$ black pixels. This implies that $h = m$.

Similarly, consider any matrix $M \in \mathcal{C}_\circ$ and let M' be the corresponding matrix in $\mathcal{C}'_\circ$. By the construction we have that $\mathtt{add}(M|X) = \mathtt{add}(M'|X)$. By the contrast property of S' we have that $\mathtt{add}(M'|X)$ contains at least one white pixels. Since $\mathtt{add}(M'|X) = \mathtt{add}(M|X)$, we have that $\mathtt{add}(M|X)$ must contain at least one pixel that is not black. This implies that $\ell = m - 1$. □

7.3. *Comparison of* PB-BW-VCS *vs.* PB-CBW-VCS

For the case of schemes with perfect reconstruction of black pixels we have that the CBW-VC model allows us to decrease the pixel expansion of a factor of $1/3$ with respect to the BW-VC model. This constant factor improvement does not make any difference for very large values of n, however it makes quite a difference for small, practicable, values of k and n. Table 9 shows explicitly the comparison for schemes with small values of k and n.

Fig. 6 compares the reconstructed images obtained with the best (n,n)-threshold black and white scheme and the reconstructed image obtained with the CBW-VC scheme presented in this section, for $n = 2, 3, 4$.

8. On the definition of contrast

In Section 4 we have proved that one can restrict the attention to schemes that use only full intensity colors. This is due the definition of the contrast property (Definition 3.1) that, in the reconstructed image, distinguishes only between black and non-black pixels. In this section we explore the use of an alternative definition of the contrast property that makes a finer grained classification of the reconstructed color pixels. However it seems, as we point out in the sequel, that the use of full intensity colors is anyway the best choice.

Each color (x, y, z) can be seen as a point in the 3-dimensional space within the cube with corners $(0, 0, 0)$ and $(1, 1, 1)$. Hence it is natural to measure how different are two colors by using the Cartesian distance of the corresponding points in the 3-dimensional space:

$$d\big((x_1, y_1, z_1), (x_2, y_2, z_2)\big) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}.$$

Notice that the maximum distance between any two colors is the distance between black $(0, 0, 0)$ and white $(1, 1, 1)$ and such a distance is $\sqrt{3} \simeq 1.7320$.

Using the above distance metric between colors we can give the following alternative definition of vcs:

Definition 8.1. A (k, n)-threshold scheme is given by two collections $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ of $n \times m$ distribution matrices that must satisfy the following conditions. There must exist two non-negative thresholds r_1 and r_2, with $r_1 + r_2 < \sqrt{3}$, such that

1. (Contrast property) Given any qualified set X, $|X \geqslant k$, of participants the following holds: for any $M \in \mathcal{C}_\circ$, we have that $\max_{c \in \mathtt{add}(M|X)} dist(\bullet, c) \leqslant r_1$ and for any $M \in \mathcal{C}_\bullet$, we have that $\max_{c \in \mathtt{add}(M|X)} dist(\circ, c) \leqslant r_2$.
2. (Security property) Same as that of Definition 3.1.

With such a definition a reconstructed pixel is considered black if the distance between black and any of its subpixels is less than r_1 and it is considered white if the distance between white and any of its subpixels is less than r_2. In other words all the colors of the reconstructed image in the sphere centered in $(0, 0, 0)$ and with radius r_1 represent black in the original image while all the colors of the reconstructed image in the sphere with center $(1, 1, 1)$ and radius r_2 represent white. The condition $r_1 + r_2 < \sqrt{3}$ guarantees that the two spheres do not intersect. The contrast can be defined as $\alpha_{\text{CBW}} = \sqrt{3} - r_1 - r_2$.

To understand why this definition is more appropriate than α_{NS} in the CBW-VC model, consider $(2, 2)$-threshold schemes defined using two colors c_1 and c_2 as follows:

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} c_1 \\ c_1 \end{bmatrix}, \begin{bmatrix} c_2 \\ c_2 \end{bmatrix} \right\}$$

$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}, \begin{bmatrix} c_2 \\ c_1 \end{bmatrix} \right\}.$$

Using $c_1 = \mathtt{R}$ and $c_2 = \mathtt{G}$ we get the scheme of Construction 5.3. Call this scheme S1. According to the definition of contrast $\alpha_{\text{NS}} = (h - \ell)/m$ the contrast of scheme S1 is $\alpha(\text{S1}) = 1$.

Using $c_1 = (0.9, 0.8, 0.1)$ and $c_2 = (0.1, 0.1, 0.9)$ we get a scheme, call it S2, with $\ell = 0$ and $h = 0$ which has contrast $\alpha(\text{S2}) = 0$. Technically S2 is not even a scheme because with a contrast of 0 the reconstructed image should not be recognizable since the contrast property is not satisfied. However in practice the image reconstructed with scheme S2 is quite recognizable being not very much different from the one reconstructed using scheme S1.

Using $c_1 = (0.9, 0.5, 0.2)$ and $c_2 = (0.3, 0.6, 0.8)$ we get a scheme, call it S3, again with $\ell = 0$ and $h = 0$ which has contrast $\alpha(\text{S3}) = 0$. Also S3 technically is not a scheme but the reconstructed image is still recognizable even though not as well as the one of S2.

Finally with $c_1 = (0.5, 0.5, 0.5)$ and $c_2 = (0.5, 0.5, 0.5)$ we get a scheme, call it S4, with $\ell = 0$ and $h = 0$ which has contrast $\alpha(\text{S4}) = 0$. In this case however, really there is no distinction between white and black pixels in the reconstructed image.

With the new definition of contrast we have that $\alpha_{\text{CBW}}(\text{S1}) = 0.3178$, $\alpha_{\text{CBW}}(\text{S2}) = 0.1688$, $\alpha_{\text{CBW}}(\text{S2}) = 0.0649$, $\alpha_{\text{CBW}}(\text{S4}) = 0$, which gives a more realistic assessment of the goodness of the schemes.

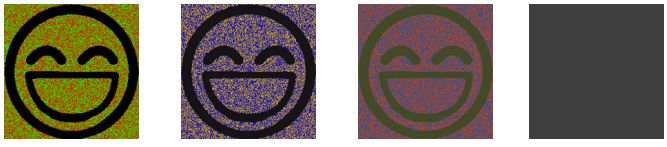
Fig. 7 shows the images reconstructed with schemes S1, S2, S3 and S4.

The use of α_{CBW} prompts for the exploitation of all colors and not just those with full intensity components. However we conjecture that considering only fully intensity colors is enough to obtain maximum contrast schemes and in this section we provide some evidence supporting such a statement. For the rest of the section α will mean α_{CBW}.

Let us start by considering again the $(2, 2)$-threshold scheme S2:

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} (0.9, 0.8, 0.1) \\ (0.9, 0.8, 0.1) \end{bmatrix}, \begin{bmatrix} (0.1, 0.1, 0.9) \\ (0.1, 0.1, 0.9) \end{bmatrix} \right\}$$

$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} (0.9, 0.8, 0.1) \\ (0.1, 0.1, 0.9) \end{bmatrix}, \begin{bmatrix} (0.1, 0.1, 0.9) \\ (0.9, 0.8, 0.1) \end{bmatrix} \right\}.$$



S1	S2	S3	S4
$\alpha_{\text{NS}} = 1$	$\alpha_{\text{NS}} = 0$	$\alpha_{\text{NS}} = 0$	$\alpha_{\text{NS}} = 0$
$\alpha_{\text{CBW}} = 0.3178$	$\alpha_{\text{CBW}} = 0.1688$	$\alpha_{\text{CBW}} = 0.0649$	$\alpha_{\text{CBW}} = 0$

Fig. 7. Empirical evidence supporting the use of α_{CBW}.

In this scheme a black secret pixel is always reconstructed as $(0.09, 0.08, 0.09)$ and thus we have $r_1 \simeq 0.1503$, while a white secret pixel is reconstructed as either $(0.81, 0.64, 0.01)$ which is at distance 1.0704 from white or as $(0.01, 0.01, 0.81)$ which is at distance 1.4129 from white, hence we have $r_2 \simeq 1.4129$. The contrast of the scheme is $\alpha = \sqrt{3} - 0.1503 - 1.4129 = 0.1688$.

We can improve the contrast by increasing to 1 the components that are close to 1 and decreasing to 0 the components that are close to 0, obtaining the scheme S1, with contrast $\alpha = 0.3178$:

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} (1,1,0) \\ (1,1,0) \end{bmatrix}, \begin{bmatrix} (0,0,1) \\ (0,0,1) \end{bmatrix} \right\}$$
$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} (1,1,0) \\ (0,0,1) \end{bmatrix}, \begin{bmatrix} (0,0,1) \\ (1,1,0) \end{bmatrix} \right\}.$$

The intuition is that a color component that contributes to the reconstruction of white pixels (think of a component close to 1) can be increased, up the maximum of 1, to improve the contrast. Indeed taking a bigger value for the component results in a color closer to white and this improves the reconstruction of white pixels; although this might cause also a worse reconstruction of black pixels the overall contrast increases. Similarly a color component that contributes to the reconstruction of black pixels (think of a component close to 0) can be decreased, up to the minimum value of 0, to improve the contrast.

Providing an analytical proof of this intuition seems to be complicated. Thus in the following we consider a simple case by focusing the attention on a CBW-VC $(2, 2)$-threshold scheme without pixel expansion and whose collections of base matrices contain 2 matrices each. We will also restrict the scheme to use only 2 colors, call them c_1 and c_2. Clearly this is quite restrictive since we can have several other ways to define schemes, but this is the simplest possible case.

By the security and contrast properties it follows that the scheme must be as follows:

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} c_1 \\ c_1 \end{bmatrix}, \begin{bmatrix} c_2 \\ c_2 \end{bmatrix} \right\} \qquad \mathcal{C}_\bullet = \left\{ \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}, \begin{bmatrix} c_2 \\ c_1 \end{bmatrix} \right\}.$$

Notice that color black is always reconstructed as the superposition of c_1 and c_2. Let $c_1 = (x_1, y_1, z_1)$ and $c_2 = (x_2, y_2, z_2)$, we have that the black pixel is always reconstructed with color (x_1x_2, y_1y_2, z_1z_2), and thus we have that

$$r_1 = \sqrt{(x_1x_2)^2 + (y_1y_2)^2 + (z_1z_2)^2}.$$

A white secret pixel instead is sometime reconstructed as $\texttt{add}(c_1, c_1)$ and sometime reconstructed as $\texttt{add}(c_2, c_2)$. Hence we have that

$$r_2 = \max\left\{ \sqrt{(1-x_1^2)^2 + (1-y_1^2)^2 + (1-z_1^2)^2}, \sqrt{(1-x_2^2)^2 + (1-y_2^2)^2 + (1-z_2^2)^2} \right\}.$$

We are interested in finding the maximum contrast, that is we want to maximize

$$\alpha = \sqrt{3} - r_1 - r_2$$

over all possible choices of $x_1, y_1, z_1, x_2, y_2, z_2$ with the constraint $r_1 + r_2 < \sqrt{3}$. Hence we want to maximize a nonlinear function of 6 variables. The intuition that we have started with, tells us that the maximum of α should be reached by choosing either 0 or 1 for each of the 6 variables.

In the following we provide a proof for the case of colors with 2 components and empirical evidence for the more general case.

8.1. A proof for the case of colors with 2 components

Assume that we have a bi-dimensional color space, that is instead of being triples of values the colors are pairs of values. In other words we have only 2 color components, say red and green. Then the colors are $c_1 = (x_1, x_2)$ and $c_2 = (y_1, y_2)$ and

we have that

$$r_1 = \sqrt{(x_1x_2)^2 + (y_1y_2)^2},$$

and

$$r_2 = \max\left\{\sqrt{\left(1-x_1^2\right)^2 + \left(1-y_1^2\right)^2}, \sqrt{\left(1-x_2^2\right)^2 + \left(1-y_2^2\right)^2}\right\},$$

while the contrast is

$$\alpha = \sqrt{2} - r_2 - r_1.$$

We are interested in finding the maximum contrast over all possible choices of x_1, x_2, y_1, y_2, with the constraint $r_1 + r_2 < \sqrt{2}$. Finding the maximum of α is equivalent to finding the minimum of $r_1 + r_2$.

Notice that if we choose $c_1 = (1, 0)$ and $c_2 = (0, 1)$ we have that $r_1 = 0$ and $r_2 = 1$ thus we know that the minimum of $r_1 + r_2$ must be less or equal to 1. Moreover if we prove that is equal to 1 we have that the scheme with full intensity colors $c_1 = (1, 0)$ and $c_2 = (0, 1)$ is optimal. In the following we prove that indeed the minimum is 1.

Since all variables appear squared we make the following variable substitutions: $\alpha_1 = x_1^2$, $\alpha_2 = x_2^2$, $\beta_1 = y_1^2$, $\beta_2 = y_1^2$. Hence we have that

$$r_1 = \sqrt{\alpha_1\beta_1 + \alpha_2\beta_2},$$
$$r_2 = \max\left\{\sqrt{(1-\alpha_1)^2 + (1-\alpha_2)^2}, \sqrt{(1-\beta_1)^2 + (1-\beta_2)^2}\right\},$$

and the constraints $0 \leqslant x_i, y_i \leqslant 1$ remain the same on the new variables $0 \leqslant \alpha_i, \beta_i \leqslant 1$.

Notice by the definition of r_2 we have that $2r_2^2 \geqslant (1-\alpha_1)^2 + (1-\alpha_2)^2 + (1-\beta_1)^2 + (1-\beta_2)^2$. Using this fact we have that

$$\begin{aligned} 2\left(r_1^2 + r_2^2\right)^2 &\geqslant 2(\alpha_1\beta_1 + \alpha_2\beta_2) + (1-\alpha_1)^2 + (1-\alpha_2)^2 + (1-\beta_1)^2 + (1-\beta_2)^2 \\ &= 2\alpha_1\beta_1 + 2\alpha_2\beta_2 + 1 + \alpha_1^2 - 2\alpha_1 + 1 + \alpha_2^2 - 2\alpha_2 + 1 + \beta_1^2 - 2\beta_1 + 1 + \beta_2^2 - 2\beta_2 \\ &= \left((\alpha_1+\beta_1)^2 + 2 - 2(\alpha_1+\beta_1)\right) + \left((\alpha_2+\beta_2)^2 + 2 - 2(\alpha_2+\beta_2)\right). \end{aligned}$$

The function $z^2 + 2 - 2z$ is a convex $\cup$ function of z reaching its minimum at $z = 1$ where the value of the function is 1. Hence we have that

$$\begin{aligned} 2\left(r_1^2 + r_2^2\right)^2 &\geqslant 1 + 1 \\ &= 2 \end{aligned}$$

and thus we have that

$$r_1^2 + r_2^2 \geqslant 1.$$

Finally we have that

$$\begin{aligned} r_1 + r_2 &= \sqrt{(r_1+r_2)^2} \\ &= \sqrt{r_1^2 + r_2^2 + 2r_1r_2} \\ &\geqslant \sqrt{r_1^2 + r_2^2} \\ &\geqslant 1. \end{aligned}$$

This implies that the minimum of $r_1 + r_2$ is at least 1. But we already know that it must be less or equal to 1 and thus we have that the minimum of $r_1 + r_2$ is exactly 1. Thus there exists a scheme with full intensity colors (the one obtained with $c_1 = (1, 0)$ and $c_2 = (0, 1)$) that has maximum contrast.

8.2. Empirical evidence for the more general case

A proof similar to the one that we have provided for the case of colors with 2 components seems to be much more complicated for the case of colors with 3 components. Indeed following a similar approach one ends up with an upper bound of $\sqrt{2} \simeq 1.41$ and a lower bound of about 1.22 leaving a gap for the exact value of the minimum. We believe that the minimum is $\sqrt{2}$. Using full intensity colors, for example by choosing $c_1 = (1, 1, 0)$ and $c_2 = (0, 0, 1)$, one can achieve $r_1 + r_2 = \sqrt{2}$.

The empirical evidence is the following. We consider a "discrete" version of the problem where the 6 variables can assume only a finite number of values which depend on a parameter K. The values that we allow for the x_is and the y_is are $0, 1/K, 2/K, \ldots, (K-1)/K, 1$. That is, instead of considering all real values in the interval $[0, 1]$ we consider only $K+1$ values of the same interval equally spaced over the interval. For example when using $K=2$ we allow only the values $0, 0.5, 1$ for the variables; when we consider $K=3$ we allow only $0, 1/3, 2/3, 1$. Computing the minimum of the discrete version of the problem can be done by an exhaustive search for small values of K because the search space has K^6 elements. We have written a program that performs the exhaustive search and we were able to make a test for K up to about 60. In all cases the minimum of $r_1 + r_2$ was $\sqrt{2}$.

The program took about one day to make the search for $K = 63$. Due to the exponential growth of the search space, it is not possible to push the test much further. The following observation, however, allows us to perform a branch and bound improvement to the exhaustive search.

(Ordering condition) There is always a choice for c_1 and c_2 that achieves maximum contrast and has the following property: the components of c_1 are ordered in decreasing order and the components of c_2 are ordered in increasing order (the claim is true also by swapping the orders, but we only need one of the two alternatives).

The above "ordering condition" can be proved by taking any point that does not satisfy the condition and providing a point satisfying the condition and resulting in an equal (if not better) contrast. Take any choice of c_1 and c_2 whose color components do not satisfy the above claim. For example consider $c_1 = (x_1, x_2, x_3)$ with $x_1 \geqslant x_2$ but $x_2 < x_3$ and $c_2 = (y_1, y_2, y_3)$ with $y_1 \leqslant y_2 \leqslant y_3$. Then we can swap x_2 and x_3, that is we can choose $c_1 = (x_1, x_3, x_2)$. With a simple algebra it is possible to see that when swapping two components that do not satisfy the ordering condition, r_2 does not change and r_1 can only decrease. This is true for all pairs of components that do not satisfy the ordering condition. By repeatedly swapping unordered components we will end up with a choice for c_1 and c_2 satisfying the ordering condition and resulting in a scheme with a contrast greater or equal to the contrast of the starting scheme. Hence there always exist a point of maximum contrast satisfying the ordering condition.

The ordering condition is very useful to branch and bound the search space. Indeed we can search only among the points whose color components satisfy the ordering condition. This allowed us to push the testing up to $K = 255$. The results has been that the minimum of $r_1 + r_2$ is always $\sqrt{2}$ and thus the maximum contrast is $\alpha = \sqrt{3} - \sqrt{2} \simeq 0.3178$. Such a contrast is achieved, for example, using $c_1 = (1, 1, 0) = \mathtt{Y}$ and $c_2 = (0, 0, 1) = \mathtt{B}$. Notice that choosing $K = 255$ is equivalent to consider all possible colors that can be represented in a real RGB color representation which uses one byte for each color component.

9. Conclusions and future work

In this paper we have proposed the use of colors to decrease the pixel expansion of visual cryptography schemes for black and white images. The extra power that comes from allowing the shares to be colored images enabled us to provide schemes with a smaller pixel expansion (compared to the schemes that one can obtain using only black and white shares). We have provided a direct construction of $(2, n)$-threshold schemes and a construction by transformation of existing (k, n)-threshold scheme for the case of scheme with perfect reconstruction of black pixels. We have also discussed the contrast property and the role of colors for such a property. There are several directions of research that one could follow. It would be interesting to study the minimum pixel expansion in this new model. Another possibility is that of studying the optimal contrast. The last section of the paper has left an open problem with an unproven conjecture: the use of full intensity colors is always preferable. It would be interesting to prove such a conjecture (or to disprove it).

References

[1] A. Adhikari, S. Sikdar, A new $(2, n)$-visual threshold scheme for color images, in: Proceedings of the Indocrypt 2003, in: LNCS, vol. 2904, Springer, 2005, pp. 148–161.
[2] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inf. Comput. 129 (2) (1996) 86–106.
[3] C. Blundo, A. De Bonis, A. De Santis, Improved schemes for visual cryptography, Des. Codes Cryptogr. 24 (2001) 255–278.
[4] C. Blundo, De Bonis, New constructions for visual cryptography, in: Italian Conference on Theoretical Computer Science, Word Scientific, 1998.
[5] S. Cimato, R. De Prisco, A. De Santis, Optimal colored threshold visual cryptography schemes, Des. Codes Cryptogr. 35 (3) (2005) 311–335.
[6] S. Cimato, R. De Prisco, A. De Santis, Probabilistic visual cryptography schemes, Comput. J. 49 (1) (2006) 97–107.
[7] S. Cimato, R. De Prisco, A. De Santis, Visual cryptography for color images, Chap. 2, in: Visual Cryptography and Secret Image Sharing, CRC Press, ISBN 978-1-4398-3721-4, 2012, pp. 31–56.
[8] S. Cimato, R. De Prisco, A. De Santis, Colored visual cryptography without color darkening, Theor. Comput. Sci. 374 (1–3) (2007) 261–276.
[9] S. Cimato, C.-N. Yang (Eds.), Visual Cryptography and Secret Image Sharing, CRC Press, Boca Raton, FL, USA, ISBN 978-1-4398-3721-4, 2012.
[10] R. De Prisco, A. De Santis, Using colors to improve visual cryptography for black and white images, in: Proceedings of ICITS 2011, in: Lect. Notes Comput. Sci., vol. 6673, 2011, pp. 182–201.
[11] R. De Prisco, A. De Santis, Cheating immune threshold visual secret sharing, Comput. J. 53 (9) (2010) 1485–1496.
[12] P.A. Eisen, D.R. Stinson, Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels, Des. Codes Cryptogr. 25 (2002) 15–61.
[13] Y.-C. Hou, Visual cryptography for color images, Pattern Recognit. 36 (2003) 1619–1629.
[14] M. Iwamoto, A weak security notion for visual secret sharing schemes, IEEE Trans. Inform. Forensics Secur. 7 (2) (2012) 372–382.
[15] O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, Opt. Lett. 12 (6) (1987) 377–379.
[16] H. Koga, H. Yamamoto, Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 81-A (6) (June 1998) 1262–1269.

[17] K.-H. Lee, P.-L. Chiu, An extended visual cryptography algorithm for general access structures, IEEE Trans. Inform. Forensics Secur. 7 (1) (2012) 219–229.
[18] S.-J. Lin, W.-H. Chung, A probabilistic model of visual cryptography scheme with dynamic group, IEEE Trans. Inform. Forensics Secur. 7 (1) (2012) 197–207.
[19] F. Liu, C. Wu, Embedded extended visual cryptography schemes, IEEE Trans. Inf. Forensics Secur. 6 (2) (2012) 307–322.
[20] M. Naor, A. Shamir, Visual Cryptography, in: Advances in Cryptology—EUROCRYPT '94, in: Lect. Notes Comput. Sci., vol. 950, 1995, pp. 1–12.
[21] S.J. Shyu, Efficient visual secret sharing scheme for color images, Pattern Recognit. 35 (2006) 866–880.
[22] S.J. Shyu, M.C. Chen, Optimum pixel expansions for threshold visual secret sharing schemes, IEEE Trans. Inf. Forensics Secur. 6 (3) (2012) 960–969.
[23] E.R. Verheul, H.C.A. van Tilborg, Constructions and properties of k out of n visual secret sharing schemes, Des. Codes Cryptogr. 11 (2) (1997) 179–196.
[24] D. Wang, L. Dong, X. Li, Towards shift tolerant visual secret sharing schemes, IEEE Trans. Inf. Forensics Secur. 6 (2) (2011) 323–337.
[25] C.-N. Yang, New visual secret sharing schemes using probabilistic method, Pattern Recognit. Lett. 25 (4) (2004) 481–494.
[26] C.-N. Yang, C.-A. Laih, New colored visual secret sharing schemes, Des. Codes Cryptogr. 20 (2000) 325–335.