ELSEVIER

Theoretical Computer Science 250 (2001) 143–161

Theoretical Computer Science

www.elsevier.com/locate/tcs

Extended capabilities for visual cryptography

Giuseppe Ateniese[a,1], Carlo Blundo[b,*], Alfredo De Santis[b], Douglas R. Stinson[c]

[a] *Dipartimento di Informatica e Scienze dell'Informazione, Università di Genova, via Dodecaneso 35, 16146 Genova, Italy*

[b] *Dipartimento di Informatica ed Applicazioni, Università di Salerno, 84081 Baronissi (SA), Italy*

[c] *Department of Combinatorics and Optimization, University of Waterloo, Waterloo Ont., Canada N2L 3G1*

Received May 1998; revised January 1999
Communicated by A. Salomaa

Abstract

An extended visual cryptography scheme (EVCS), for an access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ on a set of n participants, is a technique to encode n images in such a way that when we stack together the transparencies associated to participants in any set $X \in \Gamma_{\mathsf{Qual}}$ we get the secret message with no trace of the original images, but any $X \in \Gamma_{\mathsf{Forb}}$ has no information on the shared image. Moreover, after the original images are encoded they are still meaningful, that is, any user will recognize the image on his transparency.

The main contributions of this paper are the following:

- A trade-off between the contrast of the reconstructed image and the contrast of the image on each transparency for (k,k)-threshold EVCS (in a (k,k)-threshold EVCS the image is visible if and only if k transparencies are stacked together). This yields a necessary and sufficient condition for the existence of (k,k)-threshold EVCS for the values of such contrasts. In case a scheme exists we explicitly construct it.
- A general technique to implement EVCS, which uses hypergraph colourings. This technique yields (k,k)-threshold EVCS which are optimal with respect to the pixel expansion. Finally, we discuss some applications of this technique to various interesting classes of access structures by using relevant results from the theory of hypergraph colourings.

Keywords: Visual cryptography; Secret sharing schemes

* Corresponding author. URL: http://www.unisa.it/{∼carblu,∼ads}.

E-mail addresses: ateniese@disi.unige.it (G. Ateniese), carblu@dia.unisa.it (C. Blundo).

[1] URL: http://www.disi.unige.it/phd/ateniese/ateniese.html

0304-3975/01/$ - see front matter
PII: S0304-3975(99)00127-9

1. Introduction

A visual cryptography scheme for a set $\mathscr{P}$ of n participants is a method to encode a secret image SI into n shadow images called shares, where each participant in $\mathscr{P}$ receives one share. Certain qualified subsets of participants can "visually" recover the secret image, but other, forbidden, sets of participants have no information (in an information-theoretic sense) on SI. A "visual" recovery for a set $X \subseteq \mathscr{P}$ consists of xeroxing the shares given to the participants in X onto transparencies, and then stacking them. 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. The schemes we consider are unconditionally secure in that any forbidden set of participants does not gain information about the shared image, even though it has access to an infinite computational power. Visual cryptography schemes are characterized by two parameters: The *pixel expansion*, which is the number of sub-pixels each pixel of the original image is encoded into on each transparency, and the *contrast* which measures the "difference" between a black and a white pixel in the reconstructed image.

This cryptographic paradigm was introduced by Naor and Shamir [13]. They analysed the case of a (k,n)-threshold visual cryptography schemes, in which the secret image is visible if and only if any k transparencies are stacked together. Further results on (k,n)-threshold visual cryptography schemes can be found in [1–6, 9, 11, 16].

The model by Naor and Shamir has been extended in [1, 2] to general access structures (an access structure is a specification of all qualified and forbidden subsets of participants) and general techniques to construct visual cryptography schemes for any access structure have been proposed. In [6] the authors propose k out of n visual cryptography schemes achieving a greater relative difference than previously known schemes. In the case of 2 out of n visual cryptography schemes the scheme given in [6] achieves the best possible value for the relative difference. In [9] a new technique is presented to construct k out of n visual cryptography schemes. Finally, in [11], using a linear programming technique, the authors gave constructions for (k,n)-threshold visual cryptography schemes having large relative difference, for $k \in \{3,4,n\}$. Also, for $k=2$, they have independently derived some results similar to the ones in [6] for certain values of n.

In implementing visual cryptography schemes it would be useful to conceal the existence of the secret message, namely, the shares given to participants in the scheme should not look as a random bunch of pixels, but they should be images (an house, a dog, a tree, etc.). As an example, let $\mathscr{P}=\{1,2,3\}$ and consider the access structure $\Gamma_{\mathsf{Qual}}=\{\{1,2\},\{2,3\},\{1,2,3\}\}$ (we stipulate that all remaining subsets of $\mathscr{P}$ are forbidden). We would like to share the picture $\boxed{\text{S}}$ in such a way that the share of participant 1 is the picture $\boxed{\text{A}}$ the share of participant 2 is the picture $\boxed{\text{B}}$, and the share of participant 3 is the picture $\boxed{\text{C}}$. This shares distribution should have the property that when participants 1 and 2, or participants 2 and 3, or participants 1, 2, and 3 stack together their transparencies they get the secret image $\boxed{\text{S}}$ (the shares generated by an extended visual cryptography scheme for Γ_{Qual} are given in Appendix A).

An extended visual cryptography scheme for an access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ on a set of n participants, is a technique to encode n images in such a way that when we stack together the transparencies associated to participants in any set $X \in \Gamma_{\mathsf{Qual}}$ we get the secret message with no trace of the original images, but any $X \in \Gamma_{\mathsf{Forb}}$ has no information on the shared image. Moreover, after the original images are encoded they are still meaningful, that is, any user will recognize the image on his transparency.

Naor and Shamir [13] first considered the problem of concealing the existence of the secret message for the case of 2 out of 2 threshold VCS. Droste [9] considered the problem of sharing more than one secret image among a set of participants. For example, in the appendix of [9], a 2 out of 3 threshold visual cryptography scheme is presented in which each pair of transparencies reveals a different secret image. A construction is given to obtain visual cryptography schemes in which different subsets of transparencies reveal different secret images. This construction also provides a method of obtaining EVCS; however, it is not as efficient as the method presented in this paper.

Visual cryptography schemes have been also considered in [12, 14–16]. In [14] an alternative reconstruction method for visual cryptography schemes is studied. This method yields a higher contrast in the reconstructed image for 2 out of n threshold schemes, but the technique is not applicable to k out of n threshold schemes with $k \geqslant 3$. Visual cryptography schemes to encrypt coloured images are given in [12, 15, 16].

In this paper we study extended visual cryptography schemes, EVCS for short, for any access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$. The parameter m denotes the pixel expansion of the scheme, and the quantities α_F and α_S measure the contrast of the reconstructed image and the contrast of the shares, respectively. We provide a trade-off between the contrast of the reconstructed image (i.e., $\alpha_F(m) \cdot m$) and the contrast of the image on each transparency (i.e, $\alpha_F(m) \cdot m$) for (k,k)-threshold EVCS. In a (k,k)-threshold EVCS the original image is visible if and only if k transparencies are stacked together. (The contrasts are measured by the *relative differences* of the scheme, defined in Section 3.) This yields a necessary and sufficient condition for the existence of (k,k)-threshold EVCS for the values of such contrasts. We characterize the *admissible region* for the relative differences $\alpha_F(m)$ and $\alpha_S(m)$ and for any pair of values in this region we show how to construct a (k,k)-threshold EVCS achieving both relative differences. We give a general technique to implement extended visual cryptography schemes, which uses hypergraph colourings. This technique yields (k,k)-threshold EVCS which are optimal with respect to the pixel expansion. Finally, we discuss some applications of this technique to various interesting classes of access structures by using relevant results from the theory of hypergraph colourings.

2. Visual cryptography schemes

Let $\mathscr{P} = \{1, \ldots, n\}$ be a set of elements called *participants*, and let $2^{\mathscr{P}}$ denote the set of all subsets of $\mathscr{P}$. Let $\Gamma_{\mathsf{Qual}} \subseteq 2^{\mathscr{P}}$ and $\Gamma_{\mathsf{Forb}} \subseteq 2^{\mathscr{P}}$, where $\Gamma_{\mathsf{Qual}} \cap \Gamma_{\mathsf{Forb}} = \emptyset$. We

refer to members of Γ_{Qual} as *qualified sets* and we call members of Γ_{Forb} *forbidden sets*. The pair $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is called the *access structure* of the scheme.

Define Γ_0 to consist of all the minimal qualified sets:

$$\Gamma_0 = \{A \in \Gamma_{\mathsf{Qual}}\colon\ A' \notin \Gamma_{\mathsf{Qual}} \text{ for all } A' \subseteq A,\ A' \neq A\}.$$

A participant $P \in \mathscr{P}$ is an *essential* participant if there exists a set $X \subseteq \mathscr{P}$ such that $X \cup \{P\} \in \Gamma_{\mathsf{Qual}}$ but $X \notin \Gamma_{\mathsf{Qual}}$. If a participant P is not essential then we can construct a visual cryptography scheme giving him nothing as his/her share. In fact, a non-essential participant does not need to participate "actively" in the reconstruction of the image, since the information he/she has is not needed by any set in $\mathscr{P}$ in order to recover the shared image. In any VCS having non-essential participants, these participants do not require any information in their shares. Therefore, we assume throughout this paper that all participants are essential.

In the case where Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing, and $\Gamma_{\mathsf{Qual}} \cup \Gamma_{\mathsf{Forb}} = 2^{\mathscr{P}}$, the access structure is said to be *strong*, and Γ_0 is termed a *basis*. (This situation is the usual setting for traditional secret sharing.) In a strong access structure,

$$\Gamma_{\mathsf{Qual}} = \{C \subseteq \mathscr{P}\colon\ B \subseteq C \text{ for some } B \in \Gamma_0\}$$

and we say that Γ_{Qual} is the *closure* of Γ_0 (denoted by $cl(\Gamma_0)$).

For sets X and Y and for elements x and y, to avoid overburdening the notation, we often will write x for $\{x\}$, xy for $\{x, y\}$, xY for $\{x\} \cup Y$, and XY for $X \cup Y$.

We assume that the message consists of a collection of black and white pixels. Each pixel appears in n versions called *shares*, one for each transparency. Each share is a collection of m black and white sub-pixels. The resulting structure can be described by an $n \times m$ Boolean matrix $S = [s_{ij}]$ where $s_{ij} = 1$ iff the jth sub-pixel in the ith transparency is black. Therefore, the grey level of the combined share, obtained by stacking the transparencies $i_1, \ldots, i_s$, is proportional to the Hamming weight $w_H(V)$ of the m-vector $V = OR(r_{i_1}, \ldots, r_{i_s})$ where $r_{i_1}, \ldots, r_{i_s}$ are the rows of S associated with the transparencies we stack. This grey level is interpreted by the visual system of the users as black or as white in according with some rule of contrast. We recall the formal definition of VCS proposed in [1], which is an extension of [13].

Definition 2.1. Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set of n participants. Two collections (multisets) of $n \times m$ boolean matrices $\mathscr{C}_0$ and $\mathscr{C}_1$ constitute a *visual cryptography scheme* ($(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS) if there exist the value $\alpha(m)$ and the set $\{(X, t_X)\}_{X \in \Gamma_{\mathsf{Qual}}}$ satisfying:

1. *Any* (*qualified*) *set* $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Qual}}$ *can recover the shared image by stacking their transparencies.*
   Formally, for any $M \in \mathscr{C}_0$, the "or" V of rows $i_1, i_2, \ldots, i_p$ satisfies $w_H(V) \leqslant t_X - \alpha(m) \cdot m$; whereas, for any $M \in \mathscr{C}_1$ it results that $w_H(V) \geqslant t_X$.
2. *Any* (*forbidden*) *set* $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Forb}}$ *has no information on the shared image.*

Formally, the two collections of $p \times m$ matrices $\mathscr{D}_t$, with $t \in \{0,1\}$, obtained by restricting each $n \times m$ matrix in $\mathscr{C}_t$ to rows $i_1, i_2, \ldots, i_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Each pixel of the original image will be encoded into n pixels, each of which consists of m sub-pixels. To share a white (black, resp.) pixel, the dealer randomly chooses one of the matrices in $\mathscr{C}_0$ ($\mathscr{C}_1$, resp.), and distributes row i to participant i. The chosen matrix defines the m sub-pixels in each of the n transparencies. Observe that the size of the collections $\mathscr{C}_0$ and $\mathscr{C}_1$ does not need to be the same.

The first property is related to the contrast of the image. It states that when a qualified set of users stack their transparencies they can correctly recover the image shared by the dealer. The value $\alpha(m)$ is called *relative difference*, the number $\alpha(m) \cdot m$ is referred to as the *contrast* of the image, the set $\{(X, t_X)\}_{X \in \Gamma_{\mathsf{Qual}}}$ is called the *set of thresholds*, and t_X is the threshold associated to $X \in \Gamma_{\mathsf{Qual}}$. We want the contrast to be as large as possible and at least one, that is, $\alpha(m) \geqslant 1/m$. The second property is called *security*, since it implies that, even by inspecting all their shares, a forbidden set of participants cannot gain any information in deciding whether the shared pixel was white or black.

Notice that if a set of participants X is a superset of a qualified set X', then they can recover the shared image by considering only the shares of the set X'. This does not in itself rule out the possibility that stacking all the transparencies of the participants in X does not reveal any information about the shared image.

Let M be a matrix in the collection $\mathscr{C}_0 \cup \mathscr{C}_1$ of a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS on a set of participants $\mathscr{P}$. For $X \subseteq \mathscr{P}$, let M_X denote the m-vector obtained by considering the *or* of the vectors corresponding to participants in X; whereas $M[X]$ denotes the $|X| \times m$ matrix obtained from M by considering only the rows corresponding to participants in X.

We make a couple of observations about the structure of Γ_{Qual} and Γ_{Forb} in light of the above definition. First, it is clear that any subset of a forbidden subset is forbidden, so Γ_{Forb} is necessarily monotone decreasing. Second, it is also easy to see that no superset of a qualified subset is forbidden. Hence, a strong access structure is simply one in which Γ_{Qual} is monotone increasing and $\Gamma_{\mathsf{Qual}} \cup \Gamma_{\mathsf{Forb}} = 2^{\mathscr{P}}$.

Notice also that, given an (admissible) access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$, we can "embed" it in a strong access structure $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$ in which $\Gamma_{\mathsf{Qual}} \subseteq \Gamma'_{\mathsf{Qual}}$ and $\Gamma_{\mathsf{Forb}} \subseteq \Gamma'_{\mathsf{Forb}}$. One way to do this is to take $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$ to be the strong access structure having as basis Γ_0, where Γ_0 consists of the minimal sets in Γ_{Qual}, as usual. In view of the above observations, it suffices to construct VCS for strong access structures.

2.1. Basis matrices

The constructions in this paper are realized using two $n \times m$ matrices, S^0 and S^1 called *basis matrices* satisfying the following definition.

Definition 2.2. Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set of n participants. A visual cryptography scheme $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS with relative difference $\alpha(m)$ and set of thresholds $\{(X, t_X)\}_{X \in \Gamma_{\mathsf{Qual}}}$ is realized using the $n \times m$ basis matrices S^0 and S^1 if the following two conditions hold:

1. If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Qual}}$ (*i.e.,* if X it is a qualified set), then the "or" V of rows $i_1, i_2, \ldots, i_p$ of S^0 *satisfies* $w_H(V) \leqslant t_X - \alpha(m) \cdot m$; whereas, for S^1 it results that $w_H(V) \geqslant t_X$.
2. If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Forb}}$ (i.e., if X is a forbidden set), then the two $p \times m$ matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots, i_p$ are equal up to a column permutation.

The collections $\mathscr{C}_0$ and $\mathscr{C}_1$ are obtained by permuting the columns of the corresponding basis matrix (S^0 for $\mathscr{C}_0$ and S^1 for $\mathscr{C}_1$) in all possible ways. Note that, in this case, the size of the collections $\mathscr{C}_0$ and $\mathscr{C}_1$ is the same and it is denoted by r. This technique has been introduced in [13]. The algorithm for the VCS based on the previous construction of the collections $\mathscr{C}_0$ and $\mathscr{C}_1$ has small memory requirements (it keeps only the basis matrices S^0 and S^1) and it is efficient (to choose a matrix in $\mathscr{C}_0$ ($\mathscr{C}_1$, resp.) it only generates a permutation of the columns of S^0 (S^1, resp.)).

3. Extended visual cryptography schemes

To realize a VCS for an access structure Γ on a set of n participants we want to encode a secret image into n shares in such a way that the properties of Definition 2.1 are satisfied. In the case of EVCSs the n shares have to be images. Therefore, we start with $n+1$ images (the first n are associated with the n participants whereas the last one is the secret image) to obtain n shares that have to be still meaningful, that is, any user is able to see the image in his transparency we started with. Hence, any technique to implement EVCSs has to take into consideration the colour of the pixel in the secret image we want to obtain. In the following, we will refer to the colour of a white (black) pixel as a w pixel (b pixel). In general, we denote with $\mathscr{C}_c^{c_1 \cdots c_n}$, where $c, c_1, \ldots, c_n \in \{b, w\}$, the collection of matrices from which the dealer chooses a matrix to encode, for $i = 1, \ldots, n$, a c_i pixel in the image associated to participants i in order to obtain a c pixel when the transparencies associated to a set $X \in \Gamma_{\mathsf{Qual}}$ are stacked together. Hence, to realize an EVCS we have to construct 2^n pairs of such collections $(\mathscr{C}_w^{c_1 \cdots c_n}, \mathscr{C}_b^{c_1 \cdots c_n})$, one for each possible combination of white and black pixels in the n original images.

A participant P is *isolated* if $\{P\} \in \Gamma_{\mathsf{Qual}}$, that is, if he can reconstruct the secret by himself, without the concurrence of other participants. In this paper we assume that there is no isolated participant in the access structure. This assumption is not so strong as it could seem, since it does not make sense to consider isolated participants in EVCS. If we allow access structure to contain isolated participants in EVCS, then this would mean that from a meaningful picture (the one held by the isolated

participant) we are able to get the secret image just looking at it, without performing any cryptographic computation. Clearly, this is impossible, unless the picture held by the isolated participant is the secret itself. Hence, through this paper we assume that the access structures do not contain isolated participant.

An EVCS for an access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is defined as follows.

Definition 3.1. Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set of n participants. A family of 2^n pairs of collections (multisets) of $n \times m$ boolean matrices $\{(\mathscr{C}_w^{c_1 \cdots c_n}, \mathscr{C}_b^{c_1 \cdots c_n})\}_{c_1,\ldots,c_n \in \{b,w\}}$ constitutes a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-EVCS if there exist values $\alpha_F(m)$, $\alpha_S(m)$, and $\{(X, t_X)\}_{X \in \Gamma_{\mathsf{Qual}}}$ satisfying:

1. *Any (qualified) set* $X \in \Gamma_{\mathsf{Qual}}$ *can recover the shared image.*
   Formally, for any $X \in \Gamma_{\mathsf{Qual}}$ and for any $c_1, \ldots, c_n \in \{b, w\}$ the threshold t_X and the relative difference $\alpha_F(m)$ are such that for any $M \in \mathscr{C}_w^{c_1 \cdots c_n}$ we have that $w_H(M_X) \leqslant t_X - \alpha_F(m) \cdot m$; whereas, for any $M \in \mathscr{C}_b^{c_1 \cdots c_n}$ it results that $w_H(M_X) \geqslant t_X$.
2. *Any (forbidden) set* $X = \{i_1, \ldots, i_p\} \in \Gamma_{\mathsf{Forb}}$ *has no information on the shared image.*
   Formally, for any $X \in \Gamma_{\mathsf{Forb}}$ and for any $c_1, \ldots, c_n \in \{b, w\}$, the two collections of $p \times m$ matrices $\mathscr{D}_t^{c_1,\ldots,c_n}$ with $t = \{b, w\}$, obtained by restricting each $n \times m$ matrix in $\mathscr{C}_t^{c_1,\ldots,c_n}$ to rows $i_1, \ldots i_p$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.
3. *After the original images are encoded they are still meaningful, that is, any user will recognize the image on his transparency.*
   Formally, for any $i \in \{1, \ldots, n\}$ and any $c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n \in \{b, w\}$ it results that

$$\min_{M \in \mathscr{M}_b} w_H(M_i) - \max_{M \in \mathscr{M}_w} w_H(M_i) \geqslant \alpha_S(m) \cdot m,$$

   where $\mathscr{M}_b = \bigcup_{c_1,\ldots,c_{i-1},c_{i+1},\ldots,c_n \in \{b,w\}} \mathscr{C}_w^{c_1 \cdots c_{i-1} b c_{i+1} \cdots c_n}$

   and $\mathscr{M}_w = \bigcup_{c_1,\ldots,c_{i-1},c_{i+1},\ldots,c_n \in \{b,w\}} \mathscr{C}_w^{c_1 \cdots c_{i-1} w c_{i+1} \cdots c_n}$.

The values $\alpha_F(m)$ and $\alpha_S(m)$ are referred to as *relative difference of the final image* and *relative difference of the shares*, respectively. We assume $\alpha_F(m)$ and $\alpha_S(m)$ take values on the rational numbers. As we want the contrast to be as large as possible, we have that $\alpha_F(m) \cdot m \geqslant 1$ and $\alpha_S(m) \cdot m \geqslant 1$.

The first condition states that a qualified set of users, belonging to Γ_{Qual}, stacking their transparencies can correctly recover the secret image. The second condition is related to the security of the scheme, it implies that by inspecting the shares associated to a non-qualified subset of participants one cannot gain any information on the shared image even though he knows the original images of all n participants we started with. Clearly, conditions 1 and 2 are equivalent to state that for any $c_1, \ldots, c_n \in \{b, w\}$, the pair of collections $(\mathscr{C}_w^{c_1 \cdots c_n}, \mathscr{C}_b^{c_1 \cdots c_n})$ constitutes a visual cryptography scheme. Finally, the third condition implies that the original images are not "modified", that is, after we

encode the n original images by using the 2^n pairs of collections $(\mathscr{C}_w^{c_1\cdots c_n}, \mathscr{C}_b^{c_1\cdots c_n})$, where $c_1,\ldots,c_n \in \{b,w\}$, any user will recognize the image on his transparency. Notice that defining the quantities $\mathscr{M}_w$ and $\mathscr{M}_b$ we do not include the collections $\mathscr{C}_b^{c_1\cdots c_{i-1}bc_{i+1}\cdots c_n}$ and $\mathscr{C}_b^{c_1\cdots c_{i-1}wc_{i+1}\cdots c_n}$ as, by the second condition, for any $c_1,\ldots,c_n \in \{b,w\}$ and any $i \in \{1,\ldots,n\}$, we have that $\{M[i] : M \in \mathscr{C}_w^{c_1\cdots c_n}\} = \{M[i] : M \in \mathscr{C}_b^{c_1\cdots c_n}\}$.

It is worthwhile to note that for any $X \in \Gamma_{\mathsf{Qual}}$ and for any $c_1,\ldots,c_n \in \{b,w\}$ the threshold t_X and the relative difference $\alpha(m)$ satisfy $t_X \leqslant t_X^{c_1\cdots c_n}$ and $t_X^{c_1\cdots c_n} - \alpha^{c_1\cdots c_n}(m)\cdot m \leqslant t_X - \alpha(m)\cdot m$, where $t_X^{c_1\cdots c_n}$ is the threshold associated to set X and $\alpha^{c_1\cdots c_n}(m)$ is the relative difference of the $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS represented by the pair of collections $(\mathscr{C}_w^{c_1\cdots c_n}, \mathscr{C}_b^{c_1\cdots c_n})$.

The dealer on input $n+1$ images, that is, the images for the n participants and the secret image, generates n shares to be distributed to the participants.

We considered EVCS in which the 2^n pairs of collections $\{(\mathscr{C}_w^{c_1\cdots c_n}, \mathscr{C}_b^{c_1\cdots c_n})\}$, where $c_1,\ldots,c_n \in \{b,w\}$, have the same parameter m. This is not a restriction at all, but we considered EVCS having the same parameter m only to avoid overburdening the notation. From an arbitrary EVCS we can easily obtain an EVCS having the same parameter m for all the collections $\{(\mathscr{C}_w^{c_1\cdots c_n}, \mathscr{C}_b^{c_1\cdots c_n})\}$.

The next example shows how to realize a 2 out of 2 threshold EVCS. This scheme is realized using the general construction presented in Section 5. The resulting family of pairs of collections of matrices are the same as that proposed in [13].

Example 3.2. The collections $\mathscr{C}_c^{c_1c_2}$, where $c, c_1, c_2 \in \{b,w\}$, of a 2 out of 2 threshold EVCS are obtained by permuting the columns of the following matrices:

$$S_w^{ww} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad S_b^{ww} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix},$$

$$S_w^{wb} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \quad \text{and} \quad S_b^{wb} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

$$S_w^{bw} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad S_b^{bw} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix},$$

$$S_w^{bb} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \quad \text{and} \quad S_b^{bb} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

In such a scheme we have that $\alpha_F = \alpha_S = \frac{1}{4}$.

4. Optimal contrast (k,k)-threshold EVCS

In this section we prove an upper bound on the relative differences $\alpha_F(m)$ and $\alpha_S(m)$ of any (k,k)-threshold EVCS. We characterize the *admissible region* for the relative

differences $\alpha_F(m)$ and $\alpha_S(m)$ and for any pair of values in this region we show how to construct a (k,k)-threshold EVCS with those relative differences.

The following lemma has been proved in [1]; we repeat its proof here for the reader's convenience. We will use it in our constructions for extended visual cryptography schemes. With $\circ$ we denote the operator "concatenation" of two matrices.

Lemma 4.1. *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set $\mathscr{P}$ of n participants. Let $\mathscr{C}_0$ and $\mathscr{C}_1$ be the matrices in a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS and let D be any $n \times h$ boolean matrix. The collections of matrices $\mathscr{C}'_0 = \{M \circ D: M \in \mathscr{C}_0\}$ and $\mathscr{C}'_1 = \{M \circ D: M \in \mathscr{C}_1\}$ comprise a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m+h)$-VCS.*

Proof. Since we concatenate the same matrix D to any $M \in \mathscr{C}_0 \cup \mathscr{C}_1$, then Properties 1. and 2. of Definition 2.1 are satisfied. Moreover, the frequencies of matrices associated with forbidden sets and the set of thresholds $\{(X, t_X)\}_{X \in \Gamma_{\mathsf{Qual}}}$ do not change in going from $\mathscr{C}_0$ and $\mathscr{C}_1$ to $\mathscr{C}'_0$ and $\mathscr{C}'_1$. Only the relative difference $\alpha'(m')$ changes, becoming $\alpha'(m') = (\alpha(m) \cdot m)/(m+h)$. □

The next theorem holds.

Theorem 4.2. *In any (k,k)-threshold EVCS with pixel expansion m the relative differences $\alpha_F(m)$ and $\alpha_S(m)$ satisfy*

$$2^{k-1}\alpha_F(m) + \frac{k}{k-1}\alpha_S(m) \leqslant 1.$$

Proof. Let $\{(\mathscr{C}_w^{c_1 \cdots c_k}, \mathscr{C}_b^{c_1 \cdots c_k})\}_{c_1,\ldots,c_k \in \{b,w\}}$ be a family of 2^n pairs of collections constituting a (k,k)-threshold EVCS. Since we are interested in limiting the relative differences $\alpha_F(m)$ and $\alpha_S(m)$, without loss of generality, we assume that, for any choices of $c_1,\ldots,c_n \in \{b,w\}$, the pair of collections $(\mathscr{C}_w^{c_1 \cdots c_n}, \mathscr{C}_b^{c_1 \cdots c_n})$ are obtained by permuting, in all possible ways, the columns of the pair of basis matrices $(S_w^{c_1 \cdots c_n}, S_b^{c_1 \cdots c_n})$ (see Section 6 of [6]). Let (S^0, S^1) be a pair of basis matrices of a (k,k)-threshold VCS with pixel expansion m and relative difference $\alpha(m)$. According to Theorem 7.2 in [6] there exist a boolean matrix D and an integer $h \geqslant \alpha(m) \cdot m$ such that D is a submatrix of both S^0 and S^1, all the even columns appear in $S^0 \backslash D$ with multiplicity h, and all the odd columns appear in $S^1 \backslash D$ with multiplicity h. Setting $B = S^0 \backslash D$ and $N = S^1 \backslash D$, we have that $w_H(B_i) = w_H(N_i)$, for $i = 1,\ldots,k$. Moreover, one can easily see that $w_H(B_j) = w_H(B_i)$ and $w_H(N_j) = w_H(N_i)$ for $j \neq i$. Indeed, if k is even, then, up to a column permutation, the matrix B (resp., N) does not change when we complement its entries; whereas, if k is odd, then, up to a column permutation, complementing the entries of the matrix B (resp., N) we get as result the matrix N (resp., B). Therefore, $w_H(N_i) = w_H(B_i) = m/2$, for $i = 1,\ldots,k$. Setting $X = \{1,\ldots,k\}$ we have that

$$\sum_{i=1}^{k} w_H(N_i) - w_H(N_X) = \sum_{i=1}^{k} 2^{k-2}h - 2^{k-1}h = k2^{k-2}h - 2^{k-1}h = (k-2)2^{k-2}h$$

and

$$w_H(B_X) - w_H(B_j) = (2^{k-1} - 1)h - 2^{k-2}h = (2^{k-2} - 1)h.$$

Let $M = S_b^{w\cdots w}$ and let $M' = S_w^{b\cdots b}$. Consequently, for any $j \in X$, we have that

$$\sum_{i=1}^{k} w_H(M_i) - w_H(M_X) \geqslant (k-2)2^{k-2}\alpha_F(m) \cdot m$$

and

$$w_H(M'_X) - w_H(M'_j) \geqslant (2^{k-2} - 1)\alpha_F(m) \cdot m.$$

Hence,

$$\begin{aligned}
\sum_{i=1}^{k} w_H(M_i) &\geqslant w_H(M_X) + (k-2)2^{k-2}\alpha_F(m) \cdot m \\
&\geqslant w_H(M'_X) + [(k-2)2^{k-2} + 1]\alpha_F(m) \cdot m \\
&\qquad \text{(from Property 1 of Definition 3.1)} \\
&\geqslant w_H(M'_j) + (k-1)2^{k-2}\alpha_F(m) \cdot m \\
&\geqslant w_H(M_j) + (k-1)2^{k-2}\alpha_F(m) \cdot m + \alpha_S(m) \cdot m. \\
&\qquad \text{(from Property 3 of Definition 3.1)}
\end{aligned}$$

Thus, for any $j \in X$, we get

$$\sum_{\substack{i=1 \\ i \neq j}}^{k} w_H(M_i) \geqslant \alpha_S(m) \cdot m + (k-1)2^{k-2}\alpha_F(m) \cdot m \tag{1}$$

and

$$w_H(M_X) \geqslant w_H(M_j) + \alpha_S(m) \cdot m + 2^{k-2}\alpha_F(m) \cdot m. \tag{2}$$

Since $m \geqslant w_H(M_X)$, we have that

$$\begin{aligned}
(k-1)m &\geqslant (k-1)w_H(M_X) \\
&= \sum_{\substack{i=1 \\ i \neq j}}^{k} w_H(M_X) \\
&\geqslant \sum_{\substack{i=1 \\ i \neq j}}^{k} [w_H(M_i) + \alpha_S(m) \cdot m + 2^{k-2}\alpha_F(m) \cdot m] \text{ (from (2))} \\
&= \sum_{\substack{i=1 \\ i \neq j}}^{k} w_H(M_i) + (k-1)\alpha_S(m) \cdot m + (k-1)2^{k-2}\alpha_F(m) \cdot m \\
&\geqslant k\alpha_S(m) \cdot m + (k-1)2^{k-1}\alpha_F(m) \cdot m \text{ (from (1))}.
\end{aligned}$$

Dividing by $(k-1)m$, we get

$$2^{k-1}\alpha_F(m) + \frac{k}{k-1}\alpha_S(m) \leqslant 1,$$

which proves the theorem. □

The next corollary is an immediate consequence of previous theorem.

Corollary 4.3. *In any (k,k)-threshold EVCS the pixel expansion satisfies $m \geqslant 2^{k-1}+2$.*

Since $\alpha_F(m) \cdot m \geqslant 1$ and $\alpha_S(m) \cdot m \geqslant 1$, from Theorem 4.2, we have that

$$m \geqslant 2^{k-1}\alpha_F(m) \cdot m + \frac{k}{k-1}\alpha_S(m) \cdot m \geqslant 2^{k-1} + \frac{k}{k-1}.$$

Therefore, as m must be an integer, we get that $m \geqslant 2^{k-1}+2$. □

In Section 5 we present a general technique to implement extended visual cryptography schemes, which uses hypergraph colourings. This technique yields to (k,k)-threshold EVCSs which, according to the previous corollary, are optimal with respect to the pixel expansion.

If $\alpha \triangleq = \alpha_S = \alpha_F$, then

$$\alpha \leqslant \left(2^{k-1} + \frac{k}{k-1}\right)^{-1}.$$

In any (k,k)-threshold EVCS the set

$$\mathscr{AR} = \left\{(\alpha_F, \alpha_S) \mid \alpha_F > 0, \alpha_S > 0, \text{ and } 2^{k-1}\alpha_F + \frac{k}{k-1}\alpha_S \leqslant 1\right\}$$

is referred to as the *admissible region* for $\alpha_F(m)$ and $\alpha_S(m)$. In the following, we will show that for any pair of rational numbers $(\alpha_F, \alpha_S) \in \mathscr{AR}$ there exists a (k,k)-threshold EVCS with relative differences α_F and α_S. Let $(\alpha_F, \alpha_S) \in \mathscr{AR}$ and suppose that $(\alpha_F, \alpha_S) = (d/e, f/g)$. Let $h = eg(k-1) - 2^{k-1}dg(k-1) - kef$. Since $(\alpha_F, \alpha_S) \in \mathscr{AR}$, then $h \geqslant 0$. Let T be a $k \times h$ matrix whose entries are all equal to 0 and let S^0 and S^1 be the basis matrices of a (k,k)-threshold VCS defined as follows: S^0 is the matrix whose columns are all the boolean k-vectors having an even number of '1's, and S^1 is the matrix whose columns are all the boolean k-vectors having an odd number of '1's. The following protocol realizes a (k,k)-threshold EVCS. In this construction, we describe how to encode k pixels, one for each of the input images, to obtain a pixel of the secret image. Clearly, to encode the whole images we repeat the next protocol on all the pixels in the images.

It is immediate to see that $S_w^{c_1 \cdots c_k}$ and $S_b^{c_1 \cdots c_k}$ constructed using the Protocol in Fig. 1 are basis matrices of a (k,k)-threshold EVCS having relative differences $\alpha_F = d/e$ and $\alpha_S = f/g$. Indeed, let $X = \{1, \ldots, k\}$, for any $c_1, \ldots, c_k \in \{w, b\}$, for any $M \in \mathscr{C}_b^{c_1 \cdots c_k}$,

Input:

1. The basis matrices S^0 and S^1.
2. The $k \times h$ matrix T.
3. The colours $c_1, \ldots, c_k \in \{b, w\}$ of the pixels in the original k images.
4. The colour $c \in \{b, w\}$ of the pixel of the secret image the dealer wants to share.

Generation of the k shares:

1. Construct a $k \times k$ matrix D as follows:

For $i = 1$ **to** k **do**

if $c_i = b$ **then** set all entries of row i of D to 1.

else set entry (i, i) of D to 1 and set all remaining entries of row i to 0.

2. The collection $\mathscr{C}_c^{c_1 \cdots c_k}$ is constructed by considering the matrices obtained by permuting, in all possible ways, the columns of the matrix

$$S_c^{c_1 \cdots c_k} = \begin{cases} \underbrace{S^0 \circ \cdots \circ S^0}_{(k-1)dg} \circ \underbrace{D \circ \cdots \circ D}_{ef} \circ T & \text{if } c = w \\ \underbrace{S^1 \circ \cdots \circ S^1}_{(k-1)dg} \circ \underbrace{D \circ \cdots \circ D}_{ef} \circ T & \text{if } c = b. \end{cases}$$

3. Let M be a matrix randomly chosen in $\mathscr{C}_c^{c_1 \cdots c_k}$.

Output: The matrix M.

Fig. 1. The protocol for a (k, k)-threshold EVCS.

and for any $M' \in \mathscr{C}_w^{c_1 \cdots c_k}$ it holds that

$$w_H(M_X) = 2^{k-1}(k-1)dg + kef$$

and

$$w_H(M'_X) = (2^{k-1} - 1)(k-1)dg + kef = w_H(M_X) - (k-1)dg = w_H(M_X) - \alpha_F \cdot m.$$

Hence, setting $t_X = w_H(M_X)$, we have that Property 1 of Definition 3.1 is satisfied. Clearly, Property 2 of Definition 3.1 holds. Property 3 is satisfied, too. Indeed, it is easy to see that for any $c_1, \ldots, c_k \in \{w, b\}$, for any $i \in X$, for any $M \in \mathscr{C}_{c_i}^{c_1 \cdots c_{i-1} b c_{i+1} \cdots c_k}$, and for any $M' \in \mathscr{C}_{c_i}^{c_1 \cdots c_{i-1} w c_{i+1} \cdots c_k}$, it holds that

$$w_H(M_i) - w_H(M'_i) = ef(k-1) = \alpha_S \cdot m.$$

5. A general construction for extended VCS

Our general construction uses hypergraph colourings. We begin with some relevant definitions. A *hypergraph* is a pair of the form $(X, \mathscr{B})$, where $\mathscr{B} \subseteq 2^X$. (In other words,

Input:

1. An access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ on a set $\mathscr{P}$ of n participants.
2. The basis matrices S^0 and S^1 of a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS.
3. The colours $c_1, \ldots, c_n \in \{b, w\}$ of the pixels in the original n images.
4. The colour $c \in \{b, w\}$ of the pixel of the secret image the dealer wants to share.
5. A q-colouring ϕ of the hypergraph $(\mathscr{P}, \Gamma_0)$.

Generation of the n shares:

1. Construct an $n \times q$ matrix D as follows:

For $i = 1$ **to** n **do**

if $c_i = b$ **then** set all entries of row i of D to 1.

else set entry $(i, \phi(i))$ of D to 0 and set all remaining entries of row i to 1.

2. The collection $\mathscr{C}_c^{c_1 \cdots c_n}$ is constructed by considering the matrices obtained by permuting, in all possible ways, the columns of the matrix

$$S_c^{c_1 \cdots c_n} = \begin{cases} S^0 \circ D \text{ if } c = w \\ S^1 \circ D \text{ if } c = b. \end{cases}$$

3. Let M be a matrix randomly chosen in $\mathscr{C}_c^{c_1 \cdots c_n}$.

Output: The matrix M.

Fig. 2. The protocol to generate the shares for EVCSs.

a hypergraph is a set of subsets of a given set.) Members of X are called *vertices* and members of $\mathscr{B}$ are called *edges*. (In the case where every edge has cardinality two, a hypergraph is in fact a graph.)

A *q-colouring* of a hypergraph $H = (X, \mathscr{B})$ is a function $\phi : X \to \{1, \ldots, q\}$ such that

$$|\{\phi(x) : x \in B\}| \geqslant 2$$

for all $B \in \mathscr{B}$ such that $|B| \geqslant 2$. (In other words, every edge having at least two vertices contains at least two vertices receiving different colours.) The *chromatic number* of H, denoted $\chi(H)$, is the minimum integer q such that a q-colouring of H exists.

We will have more to say about chromatic numbers of hypergraphs later on, but for now we observe that $\chi(H) \leqslant |X|$ for any hypergraph $H = (X, \mathscr{B})$. This is easily seen by assigning a different colour to every vertex. (This colouring will be called the *trivial* colouring.)

Our general construction for extended VCS, which we present in Fig. 2, uses an arbitrary q-colouring ϕ of the hypergraph $(\mathscr{P}, \Gamma_0)$. In this construction, we describe how to encode n pixels, one for each of the input images, to obtain a pixel of the secret image. Clearly, to encode the whole images we repeat the protocol of Fig. 2 on all the pixels in the images.

In the previous protocol the collections $\mathscr{C}_c^{c_1\cdots c_n}$ are obtained by permuting, in all possible ways, the columns of the matrix $S_c^{c_1\cdots c_n}$. Because of Lemma 4.1 we do not need to permute the columns of the matrix D in step 2. Even though we use more random bits, we prefer to permute all the columns to achieve more uniform distribution of the sub-pixels.

The construction presented in Example 3.2 used the trivial 2-colouring of the hypergraph $(\{1,2\},\{\{1,2\}\})$ and it is based on a 2 out of 2 threshold VCS described by the following basis matrices:

$$S^0=\begin{bmatrix}1&0\\1&0\end{bmatrix} \quad \text{and} \quad S^1=\begin{bmatrix}1&0\\0&1\end{bmatrix}.$$

The matrix D we concatenated to S^0 and S^1 to obtain the collections $\mathscr{C}_c^{c_1c_2}$, where $c,c_1,c_2\in\{b,w\}$, is constructed as follows:

$$D=\begin{cases}\begin{bmatrix}0&1\\1&0\end{bmatrix} & \text{if } c_1=c_2=w,\\ \begin{bmatrix}0&1\\1&1\end{bmatrix} & \text{if } c_1=w \text{ and } c_2=b,\\ \begin{bmatrix}1&1\\1&0\end{bmatrix} & \text{if } c_1=b \text{ and } c_2=w,\\ \begin{bmatrix}1&1\\1&1\end{bmatrix} & \text{if } c_1=c_2=b.\end{cases}$$

Here is another small example to illustrate the construction.

Example 5.1. Let $\mathscr{P}=\{1,2,3,4,5\}$ and let $\Gamma_{\mathsf{Qual}}=cl(\Gamma_0)$, where $\Gamma_0=\{\{1,2,3,4\},\{1,5\}\}$. Assume that $\Gamma_{\mathsf{Forb}}=2^{\mathscr{P}}\backslash\Gamma_{\mathsf{Qual}}$. A visual cryptography scheme for $(\Gamma_{\mathsf{Qual}},\Gamma_{\mathsf{Forb}})$ can be obtained using the following basis matrices:

$$S_0=\begin{bmatrix}0&0&0&0&1&1&1&1\\0&0&1&1&0&0&1&1\\0&1&0&1&0&1&0&1\\0&1&1&0&1&0&0&1\\0&0&0&0&1&1&1&1\end{bmatrix}, \qquad S_1=\begin{bmatrix}0&0&0&0&1&1&1&1\\0&0&1&1&0&0&1&1\\0&1&0&1&0&1&0&1\\1&0&0&1&0&1&1&0\\1&1&1&1&0&0&0&0\end{bmatrix}.$$

Let $H=(\mathscr{P},\Gamma_0)$. Now it is not hard to see that $\chi(H)=2$. For example, if we define $\phi(1)=1$ and $\phi(2)=\phi(3)=\phi(4)=\phi(5)=2$, then ϕ is a 2-colouring.

Therefore, the collections $\mathscr{C}_w^{wbwww}$ and $\mathscr{C}_b^{wbwww}$ are obtained by permuting the columns of the following basis matrices S_w^{wbwww} and S_b^{wbwww}, respectively:

$$S_w^{wbwww}=\begin{bmatrix}0&0&0&0&1&1&1&1&0&1\\0&0&1&1&0&0&1&1&1&1\\0&1&0&1&0&1&0&1&1&0\\0&1&1&0&1&0&0&1&1&0\\0&0&0&0&1&1&1&1&1&0\end{bmatrix},$$

$$S_b^{wbwww} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Let us now show that the construction given in Fig. 1 actually produces an extended VCS. First we observe that, by Lemma 4.1, it results that any pair of collections $(\mathscr{C}_w^{c_1\cdots c_n}, \mathscr{C}_b^{c_1\cdots c_n})$ constitutes a VCS for $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$. This implies that the extended visual cryptography scheme so obtained is secure as, for any $c_1,\ldots,c_n \in \{b,w\}$ and for any $X=\{i_1,\ldots,i_{|X|}\} \in \Gamma_{\mathsf{Forb}}$, it results that $S_w^{c_1\cdots c_n}[X] = S_b^{c_1\cdots c_n}[X]$ (i.e., for any $c_1,\ldots,c_n \in \{b,w\}$ the two collections of the $|X|\times(m+q)$ matrices obtained by restricting each $n\times(m+q)$ matrix in $\mathscr{C}_w^{c_1\cdots c_n}$ and $\mathscr{C}_b^{c_1\cdots c_n}$ to rows $i_1,i_2,\ldots,i_{|X|}$ are indistinguishable in the sense that they contain the same matrices with the same frequencies).

Next, we claim that for any $c_1,\ldots,c_n \in \{b,w\}$ and for any $X \in \Gamma_{\mathsf{Qual}}$ the *or* of the rows of the matrix D corresponding to participants in X has weight $w_H(D_X)=q$. Suppose that this is not the case. Then some component of D_X is zero, say the jth component. It follows that $\phi(i_1)=\cdots=\phi(i_{|X|})=j$, which contradicts the fact that ϕ is a q-colouring of the hypergraph $(\mathscr{P},\Gamma_0)$.

This implies that for any $c_1,\ldots,c_n \in \{b,w\}$, for any $M \in \mathscr{C}_w^{c_1\cdots c_n}$, and any $\hat{M} \in \mathscr{C}_b^{c_1\cdots c_n}$ it results that $w_H(\hat{M}_X) \geqslant t_X + q$ and

$$w_H(M_X) \leqslant t_X + q - \alpha'(m+q)\cdot(m+q),$$

where

$$\alpha'(m+q) = \alpha(m)\cdot m/(m+q),$$

t_X is the threshold of the scheme for $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ we start with, and $\alpha(m)$ is the relative difference satisfying Definition 2.2 for the access structures $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ when we use the VCS based on the basis matrices S^0 and S^1. Therefore, when transparencies associated to participants in a set $X \in \Gamma_{\mathsf{Qual}}$ are stacked together the secret image will be visible.

Finally, notice that even though the n original images are modified they are still meaningful as, for $i=1,\ldots,n$, a white pixel in the image of the ith participant is encoded into $m+q$ sub-pixels of which $w_H(S_i^0)+q-1$ are black; whereas, a black pixel in the image of the ith participants is encoded into $m+q$ sub-pixels of which $w_H(S_i^1)+q = w_H(S_i^0)+q$ are black. This implies that $\alpha_S(m)=1/m$. Therefore, participant i is still able to distinguish the image on his transparency.

The next theorem holds.

Theorem 5.2. *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set $\mathscr{P}$ of n participants. If there exists a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS constructed using basis matrices and a q-colouring of the hypergraph $(\mathscr{P},\Gamma_0)$, then there exists a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m+q)$-EVCS.*

6. Applications

In the construction of Fig. 1, we would like to minimize q, i.e., by taking $q=\chi(H)$ where $H=(\mathscr{P},\Gamma_0)$. In general, however, it is an NP-hard problem to compute the chromatic number of a hypergraph. In particular, determining if a hypergraph has chromatic number equal to two is already an NP-complete problem. Even if we restrict our attention to graphs, the situation is not much better, as it is NP-complete to determine if a graph has chromatic number equal to three. It is NP-hard even to compute an approximation of the chromatic number of a graph. In fact, recently in [10] it has been proved that for some $\varepsilon>0$ it is NP-hard to approximate the chromatic number of graphs with n vertices by a factor of n^{ε}. Moreover, is has been shown that for every $\varepsilon>0$ the chromatic number cannot be approximated by a factor of $n^{1/5-\varepsilon}$ unless $NP=ZPP$. Other results on the hardness of approximating the chromatic number can be found in [7].

However, we can make use of some known results to get upper bounds and/or exact values of χ for some interesting classes of access structures. As well, for "small" access structures it is not too difficult to compute the chromatic number.

As far as general bounds are concerned, there is an upper bound on χ which depends on a suitable definition of "maximum degree" of a hypergraph. Suppose $H=(X,\mathscr{B})$ is a hypergraph. For a vertex $x\in X$, define the *degree* of x to be

$$d(x)=\max\{|\mathscr{A}|:\ \mathscr{A}\subseteq\mathscr{B},E\cap F=\{x\}\ \text{for all}\ E,F\in\mathscr{A},E\neq F\}.$$

(Note that if H is a graph then the definition of $d(x)$ reduces to the usual graph-theoretic definition of the degree of x.) Then define $d_{\max}(H)=\max\{d(x):\ x\in X\}$. Notice that for any hypergraph $H=(\mathscr{P},\Gamma_0)$ we have that $d_{\max}(H)\leqslant|\Gamma_0|$.

The following result can be found in [8, p. 431], for example.

Theorem 6.1. *Suppose H is a hypergraph. Then $\chi(H)\leqslant d_{\max}(H)+1$.*

Note that this result reduces to the well-known Vizing's Theorem when H is a graph.

6.1. Threshold schemes

One case of interest is a threshold access structure. Let $(\Gamma_{\mathsf{Qual}},\Gamma_{\mathsf{Forb}})$ be the access structure of a k out of n threshold scheme. The basis consists of all k-subsets of an n-set. This hypergraph is called the *complete uniform* hypergraph K_n^k. It is not hard to see that the chromatic number is $\chi(K_n^k)=\lceil n/(k-1)\rceil$. In fact, a function $\phi:\{1,\ldots,n\}\to\{1,\ldots,q\}$ will be a q-colouring of K_n^k if and only if $|\phi^{-1}(j)|\leqslant k-1$ for $1\leqslant j\leqslant q$.

Hence, the next theorem holds.

Theorem 6.2. *Let $(\Gamma_{\mathsf{Qual}},\Gamma_{\mathsf{Forb}})$ be a (k,n)-threshold access structure. If there exists a $(\Gamma_{\mathsf{Qual}},\Gamma_{\mathsf{Forb}},m)$-VCS constructed using basis matrices then there exists a $(\Gamma_{\mathsf{Qual}},\Gamma_{\mathsf{Forb}},m+\lceil n/(k-1)\rceil)$-EVCS.*

Results on VCS for threshold access structures can be found in [1, 13]. The next corollary is an immediate consequence of Theorem 6.2 and [13, Lemma 3].

Corollary 6.3. *Let* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ *be an* (n,n)*-threshold access structure. Then there exists a* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, 2^{n-1}+2)$*-EVCS.*

According to Corollary 4.3 it results that the scheme provided by the previous corollary is optimal with respect to the pixel expansion.

6.2. Complete bipartite graphs

Suppose that the basis Γ_0 is a complete bipartite graph $K_{a,b}$. It is obvious that the chromatic number of any bipartite graph is equal to two. Also, it was shown in [1, Theorem 7.5] that there is a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, 2)$-VCS if $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is the strong access structure with basis $K_{a,b}$. Applying Theorem 5.2, the following result is obtained.

Theorem 6.4. *Suppose that* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ *is the strong access structure with basis* $K_{a,b}$*. Then there exists a* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, 4)$*-EVCS.*

Acknowledgements

We would like to thank Carmine Di Marino who implemented the techniques presented in this paper and provided us with the images depicted in Appendix A.

Appendix A. An example of extended visual cryptography schemes

In the following an example of the secret image, the shares corresponding to single participants, and few groups of participants are depicted. The family of qualified sets is

$$\Gamma_{\mathsf{Qual}} = \{\{1,2\},\{2,3\},\{1,2,3\}\}.$$

All remaining subsets of participants are forbidden. In this scheme we have that $\alpha_S(m) = \alpha_F(m) = \frac{1}{4}$ (Figs. 3–7).

Secret Image

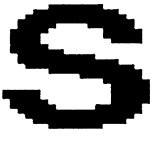
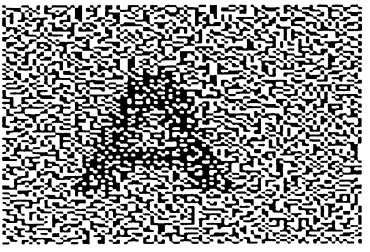
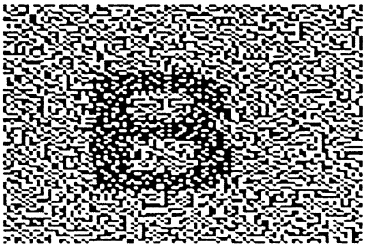


Fig. 3.

Share of participant 1



Share of participant 2



Share of participant 3

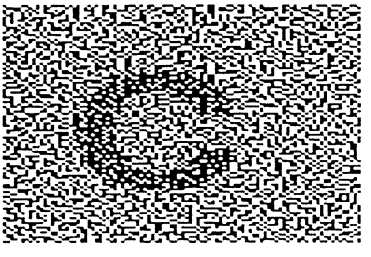


Fig. 4.

Image of participants 1 and 2

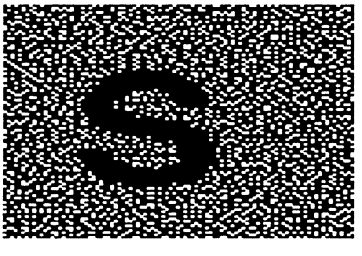


Image of participants 2 and 3

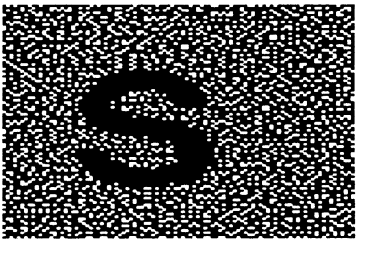


Fig. 5.

Image of participants 1, 2, and 3

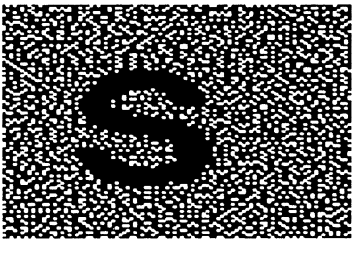


Fig. 6.

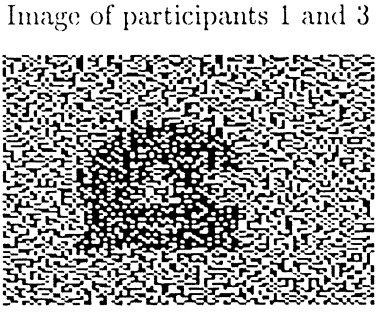


Fig. 7.

References

[1] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inform. Comput. 129 (1996) 86–106.
[2] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Constructions and bounds for visual cryptography, in 23rd Int. Colloq. on Automata, Languages and Programming (ICALP '96), Lecture Notes in Computer Science, vol. 1099, Springer, Berlin, 1996, pp. 416–428.
[3] C. Blundo, P. D'Arco, A. De Santis, D.R. Stinson, Contrast optimal threshold visual cryptography schemes, 1998, submitted for publication.
[4] C. Blundo, A. De Bonis, A. De Santis, Improved schemes for visual cryptography, 1998, submitted for publication.
[5] C. Blundo, A. De Santis, Visual cryptography schemes with perfect reconstruction of black pixels, J. Comput. Graphics (special issue) data security in image communications and networking 22-4 (1998) 449–455.
[6] C. Blundo, A. De Santis, D.R. Stinson, On the contrast in visual cryptography schemes, J. Cryptol, to appear.
[7] M. Bellare, O. Goldreich, M. Sudan, Free bits, PCPs and non-approximability — towards tight results, Proc. 36th IEEE Symp. on Foundations of Computer Science, 1995, pp. 422–431.
[8] C. Berge, Graphs and Hypergraphs, 2nd Edition, North-Holland, Amsterdam, 1976.
[9] S. Droste, New results on visual cryptography, in: Advances in Cryptology — CRYPTO '96, Lecture Notes in Computer Science, vol. 1109, Springer, Berlin, 1996, pp. 401–415.
[10] M. Fürer, Improving hardness results for approximating the chromatic number, Proc. 36th IEEE Symp. on Foundations of Computer Science, 1995, pp. 414–421.
[11] T. Hofmeister, M. Krause, H.U. Simon, Contrast-optimal k out of n secret sharing schemes in visual cryptography, COCOON '97, Lecture Notes in Computer Science, vol. 1276, Springer, Berlin, 1997, pp. 176–185.
[12] D. Naccache, Colorful Cryptography — a purely physical secret-sharing scheme based on chromatic filters, Coding and Information Integrity, French-Israeli Workshop, December 1994.
[13] M. Naor, A. Shamir, Visual cryptography, in: Advances in Cryptology — Eurocrypt '94, Lecture Notes in Computer Science, vol. 950, Springer, Berlin, 1995, pp. 1–12.
[14] M. Naor, A. Shamir, Visual cryptography II: improving the contrast via the cover base, Theory of Cryptography Library, n. 96-07, 1996, Available at `http://theory.lcs.mit.edu/~tcryptol/1996.html`.
[15] V. Rijmen, B. Preneel, Efficient colour visual encryption or shared colors of benetton, presented at EUROCRYPT '96 Rump Session, available as `http://www.iacr.org/conferences/ec96/rump/preneel.ps`.
[16] 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.