Extended Schemes for Visual Cryptography*

Giuseppe Ateniese[1], Carlo Blundo[2], Alfredo De Santis[2], and Douglas R. Stinson[3]

[1] Dipartimento di Informatica e Scienze dell'Informazione,
Università di Genova, via Dodecaneso 35, 16146 Genova, Italy
E-mail: ateniese@disi.unige.it
URL: http://www.disi.unige.it/person/AtenieseG/

[2] Dipartimento di Informatica ed Applicazioni,
Università di Salerno, 84081 Baronissi (SA), Italy
E-mail: {carblu,ads}@dia.unisa.it
URL: http://www.unisa.it/{carblu.dir/, ads.dir/}

[3] Department of Computer Science and Engineering
and Center for Communication and Information Science
University of Nebraska-Lincoln, Lincoln NE 68588, USA
E-mail: stinson@bibd.unl.edu
URL: http://bibd.unl.edu/~stinson

June 14, 1996

Abstract

An extended visual cryptography scheme, $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-EVCS for short, with pixel "expansion" m, for an access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ on a set of n participants, is a technique to encode n innocent looking 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 innocent looking images are encoded they are still meaningful, that is, any user will recognize the image on his transparency.

In this paper we first present a general technique to implement extended visual cryptography schemes, which uses hypergraph colourings. Then 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.

*Research of C. Blundo and A. De Santis is partially supported by Italian Ministry of University and Research (M.U.R.S.T.) and by National Council for Research (C.N.R.). Research of D. R. Stinson is supported by NSF grant CCR-9402141.

1 Introduction

A visual cryptography scheme for a set $\mathcal{P}$ of n participants is a method to encode a secret image SI into n shadow images called shares, where each participant in $\mathcal{P}$ 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 $X \subseteq \mathcal{P}$ 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.

This new cryptographic paradigm has been recently introduced by Naor and Shamir [8]. They analyzed the case of a k out of n threshold visual cryptography scheme, in which the secret image is visible if and only if any k transparencies are stacked together.

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 [3] 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 [3] achieves the best possible value for the relative difference. Finally, in [6] it is presented a new technique to construct k out of n visual cryptography schemes.

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 innocent looking images (an house, a dog, a tree, ...). As an example, let $\mathcal{P} = \{1, 2, 3\}$ and consider the access structure $\Gamma_{\mathsf{Qual}} = \{\{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}$ (we stipulate that all remaining subsets of $\mathcal{P}$ are forbidden). We would like to share the picture $\boxed{\mathbf{S}}$ in such a way that the share of participant 1 is the picture $\boxed{\mathbf{A}}$ the share of participant 2 is the picture $\boxed{\mathbf{B}}$, and the share of participant 3 is the picture $\boxed{\mathbf{C}}$. 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 $\boxed{\mathbf{S}}$ (the shares generated by an extended visual cryptography scheme for Γ_{Qual} are given in Appendix).

An extended visual cryptography scheme, $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-EVCS for short, with pixel "expansion" m, for an access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ on a set of n participants, is a technique to encode n innocent looking 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 innocent looking images are encoded they are still meaningful, that is, any user will recognize the image on his transparency.

Naor and Shamir [8] first considered the problem of concealing the existence of the secret message for the case of 2 out of 2 threshold VCS. Recently, Droste [6] considered the problem of sharing more than one secret image among a set of participants.

In this paper we first present a general techniques to implement extended visual cryptography schemes. Then, we give two constructions for general access structures. For k out of n extended visual cryptography schemes, we then provide an implementation achieving smaller pixel expansion than the general constructions.

2 Visual Cryptography Schemes

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

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

A participant $P \in \mathcal{P}$ is an *essential* participant if there exists a set $X \subseteq \mathcal{P}$ 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 or her share. In fact, a non-essential participant does not need to participate "actively" in the reconstruction of the image, since the information he has is not needed by any set in $\mathcal{P}$ 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 $\Gamma_{\mathsf{Qual}} \cup \Gamma_{\mathsf{Forb}} = 2^{\mathcal{P}}$, 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,

$$\Gamma_{\mathsf{Qual}} = \{C \subseteq \mathcal{P} : B \subseteq C \text{ for some } B \in \Gamma_0\},$$

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 j-th sub-pixel in the i-th 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 $w(V)$ 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 [8].

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 $\mathcal{C}_0$ and $\mathcal{C}_1$ constitute a* visual cryptography scheme *($(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS) if there exist values $\alpha(m)$ and $\{t_X\}_{X \in \Gamma_{\mathsf{Qual}}}$ 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 $M \in \mathcal{C}_0$, the "or" V of rows $i_1, i_2, \ldots, i_p$ satisfies $w(V) \leq t_X - \alpha(m) \cdot m$; whereas, for any $M \in \mathcal{C}_1$ it results that $w(V) \geq t_X$.

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 $\mathcal{D}_t$, with $t \in \{0, 1\}$, obtained by

restricting each $n \times m$ matrix in $\mathcal{C}_t$ 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 $\mathcal{C}_0$ ($\mathcal{C}_1$, 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 $\mathcal{C}_0$ and $\mathcal{C}_1$ 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, and the set $\{t_X\}_{X \in \Gamma_{\mathsf{Qual}}}$ is called the *set of thresholds*. We want the contrast to be as large as possible and at least one, that is, $\alpha(m) \geq 1/m$. 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 $\mathcal{C}_0 \cup \mathcal{C}_1$ of a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS on a set of participants $\mathcal{P}$. For $X \subseteq \mathcal{P}$, 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 $\Gamma_{\mathsf{Qual}} \cup \Gamma_{\mathsf{Forb}} = 2^{\mathcal{P}}$.

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 so 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 $\{t_X\}_{X \in \Gamma_{\mathsf{Qual}}}$ 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 is a qualified set), then the "or" V of rows $i_1, i_2, \ldots, i_p$ of S^0 satisfies $w(V) \leq t_X - \alpha(m) \cdot m$; whereas, for S^1 it results that $w(V) \geq t_X$.*

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 $\mathcal{C}_0$ and $\mathcal{C}_1$ are obtained by permuting the columns of the corresponding basis matrix (S^0 for $\mathcal{C}_0$, and S^1 for $\mathcal{C}_1$) in all possible ways. Note that, in this case, the size of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ is the same and it is denoted by r. This technique has been introduced in [8]. The algorithm for the VCS based on the previous construction of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ has small memory requirements (it keeps only the basis matrices S^0 and S^1) and it is efficient (to choose a matrix in $\mathcal{C}_0$ ($\mathcal{C}_1$, resp.) it only generates a permutation of the columns of S^0 (S^1, resp.)).

The following lemma has been proved in [1]. We will use it in our constructions for extended visual cryptography schemes.

Lemma 2.3 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set $\mathcal{P}$ of n participants. Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the matrices in a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS and let D be any $n \times t$ boolean matrix. The collections of matrices $\mathcal{C}'_0 = \{M \circ D : M \in \mathcal{C}_0\}$ and $\mathcal{C}'_1 = \{M \circ D : M \in \mathcal{C}_1\}$ comprise a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m+t)$-VCS.*

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 innocent looking images. Therefore, we start with $n+1$ images (the first n are associated with the n participants whereas the last 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 $\mathcal{C}_c^{c_1 \cdots c_n}$, 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 $(\mathcal{C}_w^{c_1 \cdots c_n}, \mathcal{C}_b^{c_1 \cdots c_n})$, 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. Moreover, we assume that no information is known on the pixels of the original images beside that they can be either white or black. For instance, no probability distribution is known on the pixels and no information like "a black pixel is more likely to occur than a white pixel" is known.

An extended visual cryptography scheme for an access structure Γ 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* $\left\{(\mathcal{C}_w^{c_1\cdots c_n}, \mathcal{C}_b^{c_1\cdots c_n})\right\}_{c_1,\ldots,c_n \in \{b,w\}}$ *constitutes a* weak $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-EVCS *if there exist values* $\alpha(m)$ *and* $\{t_X\}_{X \in \Gamma_{\mathsf{Qual}}}$ *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* $\alpha(m)$ *are such that for any* $M \in \mathcal{C}_w^{c_1\cdots c_n}$ *we have that* $w(M_X) \leq t_X - \alpha(m) \cdot m$*; whereas, for any* $M \in \mathcal{C}_b^{c_1\cdots c_n}$ *it results that* $w(M_X) \geq t_X$*.*

2. Any (forbidden) set $X = \{i_1, \ldots, i_p\} \in \Gamma_{\mathsf{Forb}}$ has no information on the shared image.
   Formally, for any $c_{i_1}, \ldots, c_{i_p} \in \{b, w\}$ *the pair of collections* $\cup_{i \in \{1,\ldots,n\}\setminus X} \cup_{c_i \in \{b,w\}} \mathcal{D}_t^{c_1,\ldots,c_n}$ *with* $t = \{b, w\}$*, where* $\mathcal{D}_t^{c_1,\ldots,c_n}$ *is obtained by restricting each* $n \times m$ *matrix in* $\mathcal{C}_t^{c_1,\ldots,c_n}$ *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 innocent looking 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*
   $$\min_{M \in \mathcal{M}_b} w(M_i) > \max_{M \in \mathcal{M}_w} w(M_i),$$
   where $\mathcal{M}_b = \cup_{c_1,\ldots,c_{i-1},c_{i+1},\ldots,c_n \in \{b,w\}} \mathcal{C}_w^{c_1\cdots c_{i-1} b c_{i+1}\cdots c_n}$
   and $\mathcal{M}_w = \cup_{c_1,\ldots,c_{i-1},c_{i+1},\ldots,c_n \in \{b,w\}} \mathcal{C}_w^{c_1\cdots c_{i-1} w c_{i+1}\cdots c_n}$.

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 and only the original images associated to a non qualified subset of participants one cannot gain any information on the shared image. Finally, the third condition implies that the original images are not "modified", that is, after we encode the n original innocent looking images by using the 2^n pairs of collections $(\mathcal{C}_w^{c_1\cdots c_n}, \mathcal{C}_b^{c_1\cdots c_n})$, where $c_1, \ldots, c_n \in \{b, w\}$, any user will recognize the image on his transparency.

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 the pairs of collections $\left\{(\mathcal{C}_w^{c_1\cdots c_n}, \mathcal{C}_b^{c_1\cdots c_n})\right\}$, 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 the same parameter m only to avoid overburdening the notation. From an arbitrary EVCS we can obtain an EVCS having the same parameter m for all the collections $\left\{(\mathcal{C}_w^{c_1\cdots c_n}, \mathcal{C}_b^{c_1\cdots c_n})\right\}$.

Next example shows how to realize a 2 out of 2 weak EVCS.

Example 3.2 The following collections $\mathcal{C}_c^{c_1 c_2}$, where $c, c_1, c_2 \in \{b, w\}$, realize a 2 out of 2 weak EVCS.

$$\mathcal{C}_w^{ww} = \left\{ \begin{bmatrix} 1001 \\ 1010 \end{bmatrix} \right\} \qquad \mathcal{C}_b^{ww} = \left\{ \begin{bmatrix} 1001 \\ 0110 \end{bmatrix}, \begin{bmatrix} 0101 \\ 1010 \end{bmatrix} \right\}$$

$$\mathcal{C}_w^{wb} = \left\{ \begin{bmatrix} 1001 \\ 1011 \end{bmatrix}, \begin{bmatrix} 0101 \\ 0111 \end{bmatrix}, \begin{bmatrix} 0101 \\ 0111 \end{bmatrix} \right\} \qquad \mathcal{C}_b^{wb} = \left\{ \begin{bmatrix} 1001 \\ 0111 \end{bmatrix}, \begin{bmatrix} 0101 \\ 1011 \end{bmatrix} \right\}$$

$$\mathcal{C}_w^{bw} = \left\{ \begin{bmatrix} 1011 \\ 1010 \end{bmatrix}, \begin{bmatrix} 0111 \\ 0110 \end{bmatrix}, \begin{bmatrix} 1110 \\ 0110 \end{bmatrix} \right\} \qquad \mathcal{C}_b^{bw} = \left\{ \begin{bmatrix} 1011 \\ 0110 \end{bmatrix}, \begin{bmatrix} 0111 \\ 1010 \end{bmatrix} \right\}$$

$$\mathcal{C}_w^{bb} = \left\{ \begin{bmatrix} 1011 \\ 1011 \end{bmatrix}, \begin{bmatrix} 0111 \\ 0111 \end{bmatrix} \right\} \qquad \mathcal{C}_b^{bb} = \left\{ \begin{bmatrix} 1011 \\ 0111 \end{bmatrix}, \begin{bmatrix} 0111 \\ 1011 \end{bmatrix}, \begin{bmatrix} 1110 \\ 0111 \end{bmatrix} \right\}.$$

Notice that for any choice of $c_1, c_2 \in \{b, w\}$ and for any $M \in \mathcal{C}_w^{c_1c_2}$ we have that $w(M_{\{1,2\}}) = 3$; whereas for any $M \in \mathcal{C}_b^{c_1c_2}$ it results that $w(M_{\{1,2\}}) = 4$. Therefore, Property 1. of Definition 3.1 is satisfied and the participants 1 and 2 can recover the shared image. Moreover, for $i = 1, 2$ and $c, c_1, c_2 \in \{b, w\}$, let $\mathcal{D}_{c,i}^{c_1c_2}$ be the set of vectors obtained by restricting each matrix in $\mathcal{C}_c^{c_1c_2}$ to row i. We have that:

$$\begin{aligned}
\mathcal{D}_{w,1}^{ww} \cup \mathcal{D}_{w,1}^{wb} &= \{[1001], [1001], [0101], [0101]\} = \mathcal{D}_{b,1}^{ww} \cup \mathcal{D}_{b,1}^{wb} \\
\mathcal{D}_{w,1}^{bw} \cup \mathcal{D}_{w,1}^{bb} &= \{[1011], [0111], [1110], [1011], [0111]\} = \mathcal{D}_{b,1}^{bw} \cup \mathcal{D}_{b,1}^{bb} \\
\mathcal{D}_{w,2}^{ww} \cup \mathcal{D}_{w,2}^{bw} &= \{[1010], [1010], [0110], [0110]\} = \mathcal{D}_{b,2}^{ww} \cup \mathcal{D}_{b,2}^{bw} \\
\mathcal{D}_{w,2}^{wb} \cup \mathcal{D}_{w,2}^{bb} &= \{[1011], [0111], [0111], [1011], [0111]\} = \mathcal{D}_{b,2}^{wb} \cup \mathcal{D}_{b,2}^{bb}.
\end{aligned}$$

Hence, Property 2. of Definition 3.1 is satisfied and any participant cannot gain any information on the shared image.
Finally, for $c \in \{b, w\}$ and for $i = 1, 2$, if $c_i = w$ then $w(M_i) = 2$; whereas if $c_i = b$ then $w(M_i) = 3$. Thus, Property 3. of Definition 3.1 is satisfied and any participant will recognize the original innocent looking image on his transparency.

$\triangle$

3.1 A Stronger Model for EVCS

In the previous section we dealt with extended visual cryptography schemes in which the participants in a forbidden set cannot gain any information on the shared image by inspecting their shares and the original images associated to them. We can consider a stronger security condition by stating 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. So, given an access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$, we define a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-EVCS as follows.

Definition 3.3 *Let* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ *be an access structure on a set of* n *participants. A* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$*-EVCS is a weak* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$*-EVCS with the following additional property:*

1. *For any choices of* $c_1, \ldots, c_n \in \{b, w\}$*, the pair of collections* $(\mathcal{C}_w^{c_1\cdots c_n}, \mathcal{C}_b^{c_1\cdots c_n})$ *constitutes a* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$*-VCS.*

The first condition is related to the security of the scheme, it implies that by inspecting the images associated to a non qualified subset of participants one cannot gain any information on the shared image, even though they know the original images of all n participants we started with. This is due to the fact that, for any $c_1, \ldots, c_n \in \{b, w\}$, the pair of collections $(\mathcal{C}_w^{c_1\cdots c_n}, \mathcal{C}_b^{c_1\cdots c_n})$ constitutes a visual cryptography scheme. The second condition implies that a qualified set of users, belonging to Γ_{Qual}, stacking their transparencies can correctly recover the secret image and that the original images are not "modified", that is, after we encode the n original innocent looking images by using the 2^n pairs of collections $(\mathcal{C}_w^{c_1\cdots c_n}, \mathcal{C}_b^{c_1\cdots c_n})$, where $c_1, \ldots, c_n \in \{b, w\}$, any user will recognize the image on his transparency.

It is worthwhile to notice 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 $t_X \le t_X^{c_1\cdots c_n}$ and $t_X^{c_1\cdots c_n} - \alpha^{c_1\cdots c_n}(m) \cdot m \le t_X - \alpha(m) \cdot m$, 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 $(\mathcal{C}_w^{c_1\cdots c_n}, \mathcal{C}_b^{c_1\cdots c_n})$.

It is easy to see that the 2 out of 2 EVCS given in Example 3.2 does not satisfy the stronger conditions of Definition 3.4. Indeed, any pairs of collections $\mathcal{C}_w^{c_1c_2}$ and $\mathcal{C}_b^{c_1c_2}$, where $c_1, c_2 \in \{b, w\}$, does not form a 2 out of 2 threshold VCS as Property 2. of Definition 2.1 is not satisfied..

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 4. The resulting family of pairs of collections of matrices are the same as that proposed in [8].

Example 3.4 The collections $\mathcal{C}_c^{c_1c_2}$, 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.

$$
\begin{array}{lclclcl}
S_w^{ww} & = & \begin{bmatrix} 1001 \\ 1010 \end{bmatrix} & \text{and} & S_b^{ww} & = & \begin{bmatrix} 1001 \\ 0110 \end{bmatrix} \\
S_w^{wb} & = & \begin{bmatrix} 1001 \\ 1011 \end{bmatrix} & \text{and} & S_b^{wb} & = & \begin{bmatrix} 1001 \\ 0111 \end{bmatrix} \\
S_w^{bw} & = & \begin{bmatrix} 1011 \\ 1010 \end{bmatrix} & \text{and} & S_b^{bw} & = & \begin{bmatrix} 1011 \\ 0110 \end{bmatrix} \\
S_w^{bb} & = & \begin{bmatrix} 1011 \\ 1011 \end{bmatrix} & \text{and} & S_b^{bb} & = & \begin{bmatrix} 1011 \\ 0111 \end{bmatrix}.
\end{array}
$$

△

In this paper we consider only schemes satisfying the conditions of Definition 3.4 as it is generally better to use the strongest security condition in designing any cryptographic protocol.

4 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 $(X, \mathcal{B})$, where $\mathcal{B} \subseteq 2^X$. (In other words, a hypergraph is a set of subsets of a given set.) Members of X are called *vertices* and members of $\mathcal{B}$ 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 $H = (X, \mathcal{B})$ is a function $\phi : X \rightarrow \{1, \ldots, q\}$ such that

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

for all $B \in \mathcal{B}$ such that $|B| \geq 2$. (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 $\chi(H) \leq |X|$ for any hypergraph $H = (X, \mathcal{B})$. 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 Figure 1, uses an arbitrary q-colouring ϕ of the hypergraph $(\mathcal{P}, \Gamma_0)$. 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 Figure 1 on all the pixels in the images.

Input:

1. An access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ on a set $\mathcal{P}$ 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 $(\mathcal{P}, \Gamma_0)$.

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 $\mathcal{C}_c^{c_1 \cdots c_n}$ 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 $\mathcal{C}_c^{c_1 \cdots c_n}$.

Output: The matrix M.

Figure 1. The protocol to generate the shares for EVCSs

In the previous protocol the collections $\mathcal{C}_c^{c_1 \cdots c_n}$ are obtained by permuting, in all possible ways, the columns of the matrix $S_c^{c_1 \cdots c_n}$. Because of Lemma 2.3 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 subpixels.

The construction presented in Example 3.4 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:

$$S^0 = \begin{bmatrix} 10 \\ 10 \end{bmatrix} \text{ and } S^1 = \begin{bmatrix} 10 \\ 01 \end{bmatrix}.$$

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

$$D = \begin{cases} \begin{bmatrix} 01 \\ 10 \end{bmatrix} & \text{if } c_1 = c_2 = w \\ \begin{bmatrix} 01 \\ 11 \end{bmatrix} & \text{if } c_1 = w \text{ and } c_2 = b \\ \begin{bmatrix} 11 \\ 10 \end{bmatrix} & \text{if } c_1 = b \text{ and } c_2 = w \\ \begin{bmatrix} 11 \\ 11 \end{bmatrix} & \text{if } c_1 = c_2 = b. \end{cases}$$

Here is another small example to illustrate the construction.

Example 4.1 Let $\mathcal{P} = \{1,2,3,4,5\}$ and let $\Gamma_{\mathsf{Qual}} = cl(\Gamma_0)$, where $\Gamma_0 = \{\{1,2,3,4\},\{1,5\}\}$. Assume that $\Gamma_{\mathsf{Forb}} = 2^{\mathcal{P}} \backslash \Gamma_{\mathsf{Qual}}$. A visual cryptography scheme for $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ can be obtained using the following basis matrices.

$$S_0 = \begin{bmatrix} 00001111 \\ 00110011 \\ 01010101 \\ 01101001 \\ 00001111 \end{bmatrix} \quad S_1 = \begin{bmatrix} 00001111 \\ 00110011 \\ 01010101 \\ 10010110 \\ 11110000 \end{bmatrix}.$$

Let $H = (\mathcal{P}, \Gamma_0)$. 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 $\mathcal{C}_w^{wbwww}$ and $\mathcal{C}_b^{wbwww}$ are obtained by permuting the columns of the following basis matrices S_w^{wbwww} and S_b^{wbwww}, respectively.

$$S_w{}^{wbwww} = \begin{bmatrix} 0000111101 \\ 0011001111 \\ 0101010110 \\ 0110100110 \\ 0000111110 \end{bmatrix} \quad S_w{}^{wbwww} = \begin{bmatrix} 0000111101 \\ 0011001111 \\ 0101010110 \\ 1001011010 \\ 1111000010 \end{bmatrix}.$$

$\triangle$

Let us now show that the construction given in Figure 1 actually produces an extended VCS. First we observe that, by Lemma 2.3, it results that any pair of collections $(\mathcal{C}_w^{c_1\cdots c_n}, \mathcal{C}_b^{c_1\cdots c_n})$ 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 $\mathcal{C}_w^{c_1\cdots c_n}$ and $\mathcal{C}_b^{c_1\cdots c_n}$ 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 $w(D_X) = q$. Suppose that this is not the case. Then some component of D_X is zero, say the jth component. It follows that $\phi(i_1) = \ldots = \phi(i_{|X|}) = j$, which contradicts the fact that ϕ is a q-colouring of the hypergraph $(\mathcal{P}, \Gamma_0)$.

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

$$w(M_X) \leq t_X + q - \alpha'(m+q) \cdot (m+q),$$

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 i-th participant is encoded into $m + q$ sub-pixels of which $w(S_i^0) + q - 1$ are black; whereas, a black pixel in the image of the i-th participants is encoded into $m + q$ sub-pixels of which $w(S_i^1) + q = w(S_i^0) + q$ are black. Therefore, participant i is still able to distinguish the image on his transparency.

Therefore, the next theorem holds.

Theorem 4.2 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set $\mathcal{P}$ 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 $(\mathcal{P}, \Gamma_0)$, then there exists a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m+q)$-EVCS.*

5 Applications

In the construction of Figure 1, we would like to minimize q, i.e., by taking $q = \chi(H)$ where $H = (\mathcal{P}, \Gamma_0)$. 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 o 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 [7] it has been proved that for some $\epsilon > 0$ 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 $\epsilon > 0$ the chromatic number cannot be approximated by a factor of $n^{1/5-\epsilon}$ unless $NP = ZPP$. Other results on the hardness of approximating the chromatic number can be found in [4].

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 $H = (X, \mathcal{B})$ is a hypergraph. For a vertex $x \in X$, define the *degree* of x to be

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

(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 $H = (\mathcal{P}, \Gamma_0)$ we have that $d_{max}(H) \leq |\Gamma_0|$.

The following result can be found in [5, p. 431], for example.

Theorem 5.1 *Suppose H is a hypergraph. Then $\chi(H) \leq d_{max}(H) + 1$.*

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

5.1 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 $\chi(K_n^k) = \lceil \frac{n}{k-1} \rceil$. 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 $|\phi^{-1}(j)| \leq k-1$ for $1 \leq j \leq q$.

Hence, the next theorem holds.

Theorem 5.2 *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 $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m + \lceil \frac{n}{k-1} \rceil)$-EVCS.*

Results on VCS for threshold access structures can be found in [1] and [8]. The next corollary is an immediate consequence of Theorem 5.2 and [8, Lemma 3].

Corollary 5.3 *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.*

Here is another example.

Example 5.4 Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be a $(3,4)$-threshold access structure. A visual cryptography scheme for $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ can be obtained using the following basis matrices presented in [1]:

$$S_0 = \begin{bmatrix} 000111 \\ 001011 \\ 001101 \\ 001110 \end{bmatrix} \quad S_1 = \begin{bmatrix} 111000 \\ 110100 \\ 110010 \\ 110001 \end{bmatrix}.$$

A 2-colouring of K_4^3 can be obtained by defining $\phi(1) = \phi(2) = 1$ and $\phi(3) = \phi(4) = 2$. So we will get an extended VCS with $m = 8$.

The collections $\mathcal{C}_w^{wwww}$ and $\mathcal{C}_b^{wwww}$ are obtained by permuting the columns of the basis matrices S_w^{wwww} and S_b^{wwww}, respectively, where

$$S_w{}^{wwww} = \begin{bmatrix} 00011101 \\ 00101101 \\ 00110110 \\ 00111010 \end{bmatrix} \qquad S_w{}^{wwww} = \begin{bmatrix} 11100001 \\ 11010001 \\ 11001010 \\ 11000110 \end{bmatrix}.$$

$\triangle$

5.2 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 4.2, the following result is obtained.

Theorem 5.5 *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 the Appendix.

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Visual Cryptography for General Access Structures*, accepted for publication in *Information and Computation*. A preliminary version is also available from *ECCC*, Electronic Colloquium on Computational Complexity (TR96–012), wia WWW using `http://www.eccc.uni-trier.de/eccc/`.

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Constructions and Bounds for Visual Cryptography*, to appear in "23rd International Colloquium on Automata, Languages and Programming" (ICALP '96), F. M. auf der Heide and B. Monien Eds., "Lecture Notes in Computer Science", Springer–Verlag, Berlin, 1996.

[3] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *New Schemes for Visual Cryptography*, preprint, 1996.

[4] M. Bellare, O. Goldreich, and M. Sudan, *Free Bits, PCPs and Non-Approximability – Towards Tight Results*, Proceedings of the 36th IEEE Symp. on Foundations of Computer Science, pp. 422–431, 1995.

[5] C. Berge, *Graphs and Hypergraphs* (second edition), North-Holland, 1976.

[6] S. Droste, *New Results on Visual Cryptography*, accepted for presentation at CRYPTO '96.

[7] M. Fürer, *Improving Hardness Results for Approximating the Chromatic Number*, Proceedings of the 36th IEEE Symp. on Foundations of Computer Science, pp. 414–421, 1995.

[8] M. Naor and A. Shamir, *Visual Cryptography*, in "Advances in Cryptology – Eurocrypt '94", A. De Santis Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp. 1–12, 1995.

Appendix

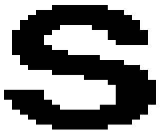
Example of an Extended Visual Cryptography Scheme

In this appendix 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.

Secret Image



Share of participant 1

Share of participant 2

Share of participant 3

Image of participants 1 and 2

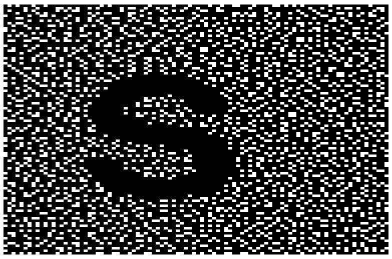


Image of participants 2 and 3

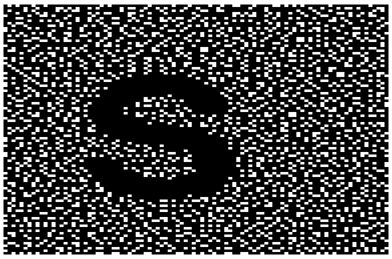


Image of participants 1, 2, and 3

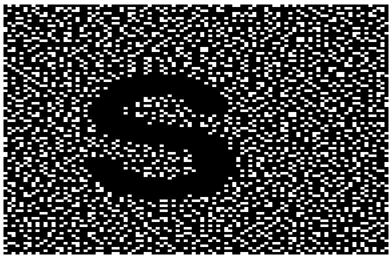


Image of participants 1 and 3