Visual Cryptography for General Access Structures[1]

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/phd/ateniese/ateniese.html

[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

May 2, 1996

[1]A very preliminary version of this work has been presented at ICALP '96 [1]. Research of C. Blundo and A. De Santis is partially supported by the Italian Ministry of University and Research (M.U.R.S.T.) and by the Italian National Council for Research (C.N.R.). Research of D. R. Stinson is supported by NSF grant CCR-9402141.

Abstract

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.

In this paper we propose two techniques to construct visual cryptography schemes for general access structures. We analyze the structure of visual cryptography schemes and we prove bounds on the size of the shares distributed to the participants in the scheme. We provide a novel technique to realize k out of n threshold visual cryptography schemes. Our construction for k out of n visual cryptography schemes is better with respect to pixel expansion than the one proposed in [11] and for the case of 2 out of n is the best possible. Finally, we consider graph-based access structures, i.e., access structures in which any qualified set of participants contains at least an edge of a given graph whose vertices represent the participants of the scheme.

Index terms : Visual Cryptography, Secret Sharing, and Data Security.

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.

The best way to understand visual cryptography is by resorting to an example. Suppose that there are four participants, that is $\mathcal{P} = \{1, 2, 3, 4\}$, and that the qualified sets are all subsets of $\mathcal{P}$ containing at least one of the three sets $\{1, 2\}$, $\{2, 3\}$, or $\{3, 4\}$. Hence, the family of qualified sets is

$$\Gamma_{\mathsf{Qual}} = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}.$$

We will stipulate that all remaining subsets of $\mathcal{P}$ are forbidden.

We want to encode the secret image "IC". The four shares generated by a visual cryptography scheme for Γ_{Qual} are given in the Appendix. They look like random patterns and, indeed, no individual share provides any information, even to an infinitely powerful computer, on the original image. To decrypt the secret image the reader should xerox each pattern on a separate transparency, stack together the transparencies associated to participants in any qualified set, and project the result with an overhead projector. If the transparencies are aligned carefully, then the reader will get the images showed in the remaining part of the Appendix.

This new cryptographic paradigm has been recently introduced by Naor and Shamir [11]. 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.

A possible application, mentioned in [11], is the following. The 2 out of 2 visual cryptography scheme can be thought of as a private key cryptosystem. We encode the secret printed message into two random looking shares. One of the two shares will be a printed page of ciphertext which can be sent by mail or fax, whereas the other share serves as the secret key. The original image is revealed by stacking together the two transparencies. This system is similar to the one-time pad, as each page of ciphertext is decoded by using a different transparency. However, it does not require any cryptographic computation — the decoding is done by the human visual system.

Visual cryptography schemes with extended capabilities have been analyzed in [3]. The authors present a general technique to implement extended visual cryptography schemes which uses hypergraph colourings.

In this paper we extend Naor and Shamir's model to general access structures, where an access structure is a specification of all qualified and forbidden subsets of participants. We propose two different techniques to construct visual cryptography schemes for any access structure. We analyze the structure of visual cryptography schemes and we prove bounds on the size of the shares distributed to the participants in the scheme. We provide a novel technique to realize k out of n threshold visual cryptography schemes. Our construction for k out of n visual cryptography schemes is better with respect to pixel expansion than the one proposed in [11] and for the case of 2 out of n is the best possible. Our construction for 2 out of n schemes has pixel expansion of only about $\log n$ (see Theorem 7.3) while the scheme proposed in [11] has pixel expansion n. Also, we consider graph-based access structures, i.e., access structures in which any qualified set of participants contains at least one edge of a given graph whose vertices represent the participants of the scheme.

2 The Model

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:

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

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 a share completely "white" or even nothing as his 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, unless otherwise specified, 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.

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 subpixels. The resulting structure can be described by an $n \times m$ Boolean matrix $S = [s_{ij}]$ where $s_{ij} = 1$ iff the j-th subpixel 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.

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 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 $M \in \mathcal{C}_0$, *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 $X = \{i_1, i_2, \dots, i_p\} \in \Gamma_{\mathsf{Forb}}$ 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 $i_1, i_2, \dots, i_p$ 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 subpixels. To share a white (black, resp.) pixel, we randomly choose one of the matrices in $\mathcal{C}_0$ ($\mathcal{C}_1$, resp.), and distribute row i to participant i. The chosen matrix defines the m subpixels in each of the n transparencies. Notice that in the previous definition $\mathcal{C}_0$ ($\mathcal{C}_1$) is a multiset of $n \times m$ boolean matrices, therefore we allow a matrix to appear more than once in $\mathcal{C}_0$ ($\mathcal{C}_1$). Finally, 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 shared image. 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, $\alpha(m) \geq 1/m$. 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.

There are few differences between the model of visual cryptography we propose and the one presented by Naor and Shamir [11]. Our model is a generalization of the one proposed in [11], since with each set $X \in \Gamma_{\mathsf{Qual}}$ we associate a (possibly) different threshold t_X. Further, the access structure is not required to be strong in our model.

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.

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 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}.

In view of the above observations, it suffices to construct VCS for strong access structures. However, we will sometimes give constructions for arbitrary access structures as well.

2.1 The Size of the Collections $\mathcal{C}_0$ and $\mathcal{C}_1$

In this paper we consider only VCS in which the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ have the same size, i.e., $|\mathcal{C}_0| = |\mathcal{C}_1| = r$. Actually, this is not a restriction at all. Indeed, given an access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$, we will show how to obtain, from an arbitrary VCS for $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$, a

VCS having the same parameters m, $\alpha(m)$, and $\{(X, t_X)\}_{X \in \Gamma_{\mathsf{Qual}}}$, with equally sized $\mathcal{C}_0$ and $\mathcal{C}_1$.

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 rows 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.

Now, suppose that $|\mathcal{C}_0| = r_0$ and $|\mathcal{C}_1| = r_1 \neq r_0$. Let $X \in \Gamma_{\mathsf{Forb}}$ and let $M \in \mathcal{C}_0 \cup \mathcal{C}_1$. For $i \in \{0,1\}$, let η_X^i denote the number of times that the matrix $M[X]$ appears in the collection $\{A[X] : A \in \mathcal{C}_i\}$. From Property 2. of Definition 2.1 we have that $\eta_X^0/r_0 = \eta_X^1/r_1$. We construct the collections $\mathcal{C}_0'$ and $\mathcal{C}_1'$ of a new $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS, termed Σ', by taking r_1 copies of each matrix in $\mathcal{C}_0$ and r_0 copies of each matrix in $\mathcal{C}_1$, respectively, obtaining $|\mathcal{C}_0'| = |\mathcal{C}_1'| = r = r_0 \cdot r_1$.

We have to show that Properties 1 and 2 of Definition 2.1 are satisfied. Clearly, Property 1 of Definition 2.1 holds. Let $X \in \Gamma_{\mathsf{Forb}}$ and let $M \in \mathcal{C}_0' \cup \mathcal{C}_1'$. For $i \in \{0,1\}$, let μ_X^i denote the number of times that the matrix $M[X]$ appears in the collection $\{A[X] : A \in \mathcal{C}_i'\}$. It results that $\mu_X^0 = \eta_X^0 \cdot r_1$ and $\mu_X^1 = \eta_X^1 \cdot r_0$. Therefore,

$$\frac{\mu_X^0}{r} = \frac{\eta_X^0 \cdot r_1}{r_0 \cdot r_1} = \frac{\eta_X^0}{r_0} = \frac{\eta_X^1}{r_1} = \frac{\eta_X^1 \cdot r_0}{r_1 \cdot r_0} = \frac{\mu_X^1}{r}.$$

Thus, Property 2. of Definition 2.1 is satisfied. It is worthwhile to notice that the relative difference $\alpha(m)$, the pixel expansion m, and set of thresholds $\{(X, t_X)\}_{X \in \Gamma_{\mathsf{Qual}}}$ do not change when we go from Σ to Σ'. Hence, without loss of generality, in this paper we restrict our attention to VCS in which the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ have the same size.

2.2 Basis Matrices

Most of 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 $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS with relative difference $\alpha(m)$ and set of thresholds $\{(X, t_X)\}_{X \in \Gamma_{\mathsf{Qual}}}$ is realized using the two $n \times m$ 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 (it is equal to $m!$) and it is denoted by r. This technique has been introduced in [11]. 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.)).

We give two examples to illustrate the definitions, the use of basis matrices, and the way the subpixels are arranged.

Example 2.3 Suppose $n = 4$, so $\mathcal{P} = \{1, 2, 3, 4\}$. Define

$$\Gamma_{\mathsf{Qual}} = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 2, 3\}\}$$

and

$$\Gamma_{\mathsf{Forb}} = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 3\}, \{1, 4\}, \{2, 4\}\}.$$

Then $\Gamma_0 = \Big\{\{1, 2\}, \{2, 3\}, \{3, 4\}\Big\}$.

We will construct a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, 3)$-VCS using basis matrices. The basis matrices S^0 and S^1 are as follows:

$$S^0 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

In this scheme, $\alpha(m) = 1/3$, so the contrast is one. Let's first look at the qualified subsets. It is easy to check that the following values hold with regard to Property 1 of Definition 2.2.

$$\begin{aligned} t_{\{1,2\}} &= 3 \\ t_{\{2,3\}} &= 2 \\ t_{\{3,4\}} &= 3, \text{ and} \\ t_{\{1,2,3\}} &= 3. \end{aligned}$$

Property 2 of Definition 2.2 is easily verified for the forbidden sets. Finally, the sets $\{1, 2, 4\}$, $\{1, 3, 4\}$, $\{2, 3, 4\}$, and $\{1, 2, 3, 4\}$ are neither forbidden nor qualified, so the scheme is not a scheme for a strong access structure. △

Example 2.4 Suppose $\mathcal{P} = \{1, 2, 3, 4, 5, 6\}$ and consider the strong access structures with basis $\Gamma_0 = \Big\{\{i, j\} : i, j \in \mathcal{P} \text{ and } i \neq j\Big\}$. This access structure is based on the complete graph with 6 vertices and it is equivalent to a 2 out of 6 threshold structure. The following basis matrices represent a VCS for the strong access structure on the set of participants $\mathcal{P}$ with basis Γ_0.

$$S^0 = \begin{bmatrix} 1100 \\ 1100 \\ 1100 \\ 1100 \\ 1100 \\ 1100 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 1010 \\ 1001 \\ 1100 \\ 0110 \\ 0101 \\ 0011 \end{bmatrix}.$$

In this scheme any pixel of the original image is encoded into four subpixels. To do not distort the aspect ratio of the original image it is convenient to arrange the subpixels in a 2×2 array where each share has the form depicted in Figure 1. These shares correspond to the rows of the basis matrices S^0 and S^1, respectively. The subpixels are disposed in a clock-wise fashion starting from the upper-left corner of the 2×2 array. Clearly, to any permutation of the columns of S^0 and S^1 will correspond a new re-arrangement of the subpixels into the 2×2 array.

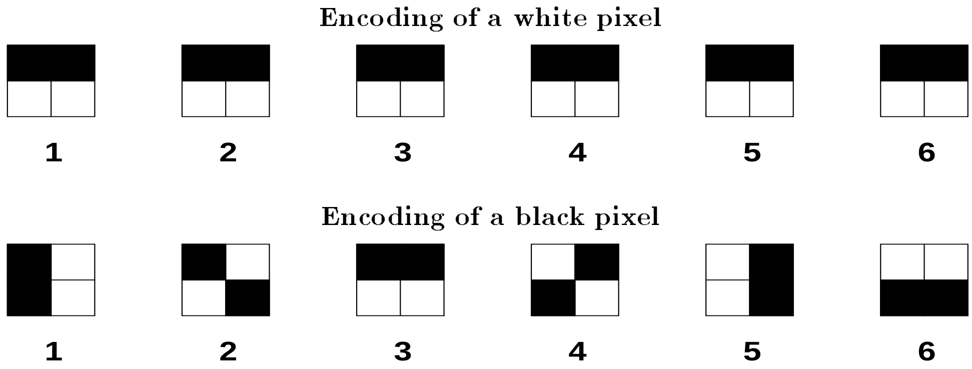


Figure 1: Shares of a 2 out of 6 threshold VCS.

$\triangle$

In the previous example we have seen how to arrange the subpixels forming a share in order to avoid the distortion of the aspect ratio of the original image. Thus, the best results are obtained when the pixel expansion m is a square. If this is not the case, we can expand the shares by "padding" the share with m' white subpixels in such a way that $m + m'$ is a square and then we can apply the technique seen in Example 2.4. This construction works (see Lemma 5.3), but we get a VCS with worse relative difference than the one we started with. If m is not a square, then a second method to realize a VCS is to consider c copies of the share in such a way that $c \cdot m$ is a square and then to apply the technique seen in Example 2.4. A third construction is to let each subpixel of the share to occupy a m-th of a square surface. For example, each subpixel can have a rectangular shape of height 1 and of width $1/m$. This is the way the images of the example given in the Appendix are obtained.

3 An (n, n)-Threshold Scheme

A (k, n)-threshold VCS realizes the strong access structure with basis

$$\Gamma_0 = \{B \subseteq \mathcal{P} : |B| = k\}.$$

Thus, the original message is visible (that is, Property 1. of Definition 2.1 is satisfied) if any k of n participants stack their transparencies, but totally invisible (that is, Property 2. of Definition 2.1 is satisfied) if fewer than k transparencies are stacked together or analysed by any other method. In this section we recall some of the results presented in [11] for (n, n)-threshold VCS. In such a scheme, the original message is visible if and only if all n transparencies are stacked together, but totally invisible if fewer than n transparencies are stacked together or analysed by any other method.

The construction of an (n, n)-threshold VCS is obtained by means of the construction of the basis matrices S^0 and S^1 defined as follows: S^0 is the matrix whose columns are all the boolean n-vectors having an even number of '1's, and S^1 is the matrix whose columns are all the boolean n-vectors having an odd number of '1's.

Lemma 3.1 ([11]) *The above scheme is an (n, n)-threshold VCS with parameters $m = 2^{n-1}$, $\alpha(m) = 1/2^{n-1}$ and $r = 2^{n-1}!$*

Example 3.2 Let $n = 4$. Then, the two basis matrices are:

$$S^0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

$\triangle$

The scheme realized using the previous construction is optimal with respect to the values of m and $\alpha(m)$, as stated in the next theorem.

Theorem 3.3 ([11]) *In any (n, n)-threshold VCS, $\alpha(m) \leq 1/2^{n-1}$ and $m \geq 2^{n-1}$.*

In general, we will be interested in minimizing m for a given access structure. Hence, we define $m^*(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ to be the smallest value m such that an $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS exists.

Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set $\mathcal{P}$ of participants. Given a subset of participants $\mathcal{P}' \subseteq \mathcal{P}$, we define the access structure *induced by* $\mathcal{P}'$ to be the families of sets defined as follows:

$$\begin{aligned} \Gamma[\mathcal{P}']_{\mathsf{Qual}} &= \{X \in \Gamma_{\mathsf{Qual}} : X \subseteq \mathcal{P}'\}, \text{ and} \\ \Gamma[\mathcal{P}']_{\mathsf{Forb}} &= \{X \in \Gamma_{\mathsf{Forb}} : X \subseteq \mathcal{P}'\}. \end{aligned}$$

The following lemma is immediate.

Lemma 3.4 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set $\mathcal{P}$ of participants, and let $(\Gamma[\mathcal{P}']_{\mathsf{Qual}}, \Gamma[\mathcal{P}']_{\mathsf{Forb}})$ be the induced access structure on the subset of participants $\mathcal{P}'$. Then $m^*(\Gamma[\mathcal{P}']_{\mathsf{Qual}}, \Gamma[\mathcal{P}']_{\mathsf{Forb}}) \leq m^*(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$.*

The next corollary is a consequence of Theorem 3.3 and Lemma 3.4.

Corollary 3.5 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure. Suppose that $X \in \Gamma_0$, and suppose that $Y \in \Gamma_{\mathsf{Forb}}$ for all $Y \subseteq X$, $Y \neq X$. Then $m^*(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}) \geq 2^{|X|-1}$.*

4 General Constructions

In this section we will present two construction techniques to realize visual cryptography schemes for any access structure.

4.1 A Construction for VCS Using Cumulative Arrays

The first construction we consider is based on the cumulative array method introduced in [13]. Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be a strong access structure on the set of participants $\mathcal{P} = \{1, 2, \ldots, n\}$. Let Z_M denote the collection of the maximal forbidden sets of Γ:

$$Z_M = \{B \in \Gamma_{\mathsf{Forb}} : B \cup \{i\} \in \Gamma_{\mathsf{Qual}} \text{ for all } i \in \mathcal{P} \setminus B\}.$$

A *cumulative map* (β, T) for Γ_{Qual} is a finite set T along with a mapping $\beta : \mathcal{P} \longrightarrow 2^T$ such that for $Q \subseteq \mathcal{P}$ we have that

$$\bigcup_{a \in Q} \beta(a) = T \Longleftrightarrow Q \in \Gamma_{\mathsf{Qual}}.$$

We can construct a cumulative map (β, T) for any Γ_{Qual} by using the collection of the maximal forbidden sets $Z_M = \{F_1, \ldots, F_t\}$ as follows. Let $T = \{T_1, \ldots, T_t\}$ and for any $i \in \mathcal{P}$ let

$$\beta(i) = \{T_j \mid i \notin F_j, 1 \leq j \leq t\}. \tag{1}$$

It is easy to see that for any $X \in \Gamma_{\mathsf{Qual}}$ we have

$$\bigcup_{i \in X} \beta(i) = T;$$

whereas any set $X \in \Gamma_{\mathsf{Forb}}$ will be missing at least one $T_j \in T$.

From the cumulative mapping (1) for Γ_{Qual}, we can obtain a *cumulative array* for Γ_{Qual}, as follows. A cumulative array is a $|\mathcal{P}| \times |T|$ boolean matrix, denoted by CA, such that $CA(i,j) = 1$ if and only if $i \notin F_j$.

Example 4.1 Let $\mathcal{P} = \{1,2,3,4\}, \Gamma_0 = \Big\{\{1,2\},\{2,3\},\{3,4\}\Big\}$, $Z_M = \Big\{\{1,4\},\{1,3\},\{2,4\}\Big\}$, and let $F_1 = \{1,4\}, F_2 = \{1,3\}$, and $F_3 = \{2,4\}$. Therefore, $|T| = 3$. The cumulative array for Γ_{Qual} is the following:

$$CA = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

$\triangle$

At this point we can realize a visual cryptography scheme for any strong access structure. Our technique is based on the (n,n)-threshold VCS of Section 3. Let Z_M be set of the maximal forbidden sets and let $t = |Z_M|$. Let CA be the cumulative array for Γ_{Qual} obtained using the cumulative map (1). Let $\widehat{S}^0$ and $\widehat{S}^1$ be the basis matrices for a (t,t)-threshold VCS. The basis matrices S^0 and S^1 for a VCS for the access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ can be constructed as follows. For any fixed i let $j_{i,1}, \ldots, j_{i,g_i}$ be the integers j such that $CA(i,j) = 1$. The i-th row of S^0 (S^1, resp.) consists of the *or* of the rows $j_{i,1}, \ldots, j_{i,g_i}$ of $\widehat{S}^0$ ($\widehat{S}^1$, resp.). An example will help in illustrating this technique.

Example 4.1 (cont.) Let $\mathcal{P} = \{1,2,3,4\}$, $\Gamma_0 = \Big\{\{1,2\},\{2,3\},\{3,4\}\Big\}$, and $Z_M = \Big\{\{1,4\},\{1,3\},\{2,4\}\Big\}$. Hence, $|T| = 3$. Let $\widehat{S}^0$ and $\widehat{S}^1$ be

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

The basis matrices S^0 and S^1 in a VCS realizing the strong access structure with basis Γ_0 are:

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

The second row of S^0 is the *or* of rows 1 and 2 of $\widehat{S}^0$, that is,

$$[0, 1, 1, 1] = [0, 1, 1, 0] \ or \ [0, 1, 0, 1],$$

and the third row of S^0 is the *or* of rows 1 and 3 of $\widehat{S}^0$. The first and the fourth rows of S^0 are equal to rows 3 and 2 of $\widehat{S}^0$, respectively, and similarly for S^1.

$\triangle$

The next theorem holds.

Theorem 4.2 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be a strong access structure, and let Z_M be the family of the maximal forbidden sets in Γ_{Forb}. Then there exists a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS with $m = 2^{|Z_M|-1}$ and $t_X = m$ for any $X \in \Gamma_{\mathsf{Qual}}$.*

4.2 Constructing VCS from Smaller Schemes

In this section we present a construction for visual cryptography schemes using small schemes as building blocks in the construction of larger schemes.

Let $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$ and $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}})$ be two access structures on a set of n participants $\mathcal{P}$. If a participant $i \in \mathcal{P}$ is non-essential for $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$, we assume that $i \in \Gamma'_{\mathsf{Forb}}$ and that i does not receive nothing as share. Analogously for $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}})$. Suppose there exist a $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}}, m')$-VCS and a $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}}, m'')$-VCS with basis matrices R^0, R^1 and T^0, T^1, respectively. We will show how to construct a VCS for the access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}) = (\Gamma'_{\mathsf{Qual}} \cup \Gamma''_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}} \cap \Gamma''_{\mathsf{Forb}})$. From the matrices R^0, R^1, T^0, and T^1 we construct two pairs of matrices, $(\widehat{R}^0, \widehat{R}^1)$ and $(\widehat{T}^0, \widehat{T}^1)$, each consisting of n rows, as follows. Let us first show how to construct $\widehat{R}^0$. For $i = 1, \ldots, n$, the i-th row of $\widehat{R}^0$ has all zeroes as entries if the participant i is not an essential participant of $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$; otherwise, it is the row of R^0 corresponding to participant i. The matrices $\widehat{R}^1$, $\widehat{T}^0$, and $\widehat{T}^1$ are constructed similarly. Finally, the basis matrices S^0 (S^1, resp.) for $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ will be realized by concatenating the matrices $\widehat{R}^0$ and $\widehat{T}^0$ ($\widehat{R}^1$ and $\widehat{T}^1$, resp.). (That is, $S^0 = \widehat{R}^0 \circ \widehat{T}^{0\prime}$ and $S^1 = \widehat{R}^1 \circ \widehat{T}^1$, where $\circ$ denotes the operator "concatenation" of two matrices.) In Theorem 4.4 we will prove that the scheme obtained using this method realizes a VCS. An example will help in illustrating the previous technique.

Example 4.3 Let $\mathcal{P} = \{1, 2, 3, 4, 5\}$ and let $\Gamma_0 = \Big\{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{1, 5\}, \{2, 5\}\Big\}$. We can construct a visual cryptography scheme for the strong access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$

having basis Γ_0 by using VCS for the strong access structures with bases $\Gamma'_0 = \Big\{\{1,2\},\{1,5\}\Big\}$ and $\Gamma''_0 = \Big\{\{2,3\},\{3,4\},\{4,5\},\{2,5\}\Big\}$, respectively.

$$R^0 = \begin{bmatrix} 10 \\ 10 \\ 10 \end{bmatrix}, \; R^1 = \begin{bmatrix} 10 \\ 01 \\ 01 \end{bmatrix} \quad \text{and} \quad T^0 = \begin{bmatrix} 10 \\ 10 \\ 10 \\ 10 \end{bmatrix}, \; T^1 = \begin{bmatrix} 10 \\ 01 \\ 10 \\ 01 \end{bmatrix}.$$

From the above matrices we obtain the matrices $\widehat{R}^0$, $\widehat{R}^1$, $\widehat{T}^0$, and $\widehat{T}^1$.

$$\widehat{R}^0 = \begin{bmatrix} 10 \\ 10 \\ 00 \\ 00 \\ 10 \end{bmatrix}, \; \widehat{R}^1 = \begin{bmatrix} 10 \\ 01 \\ 00 \\ 00 \\ 01 \end{bmatrix} \quad \text{and} \quad \widehat{T}^0 = \begin{bmatrix} 00 \\ 10 \\ 10 \\ 10 \\ 10 \end{bmatrix}, \; \widehat{T}^1 = \begin{bmatrix} 00 \\ 10 \\ 01 \\ 10 \\ 01 \end{bmatrix}.$$

Concatenating the matrix $\widehat{R}^0$ with $\widehat{T}^0$ and the matrix $\widehat{R}^1$ with $\widehat{T}^1$, we obtain the following basis matrices S^0 and S^1 for a visual cryptography scheme for the strong access structure with basis Γ_0:

$$S^0 = \begin{bmatrix} 1000 \\ 1010 \\ 0010 \\ 0010 \\ 1010 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 1000 \\ 0110 \\ 0001 \\ 0010 \\ 0101 \end{bmatrix}.$$

$\triangle$

The next theorem holds.

Theorem 4.4 *Let* $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$ *and* $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}})$ *be two access structures on a set of* n *participants* $\mathcal{P}$*. Suppose there exist a* $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}}, m')$*-VCS and a* $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}}, m'')$*-VCS with basis matrices* R^0*,* R^1 *and* T^0*,* T^1*, respectively. Then the previous construction yields a* $(\Gamma'_{\mathsf{Qual}} \cup \Gamma''_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}} \cap \Gamma''_{\mathsf{Forb}}, m' + m'')$*-VCS. If the original access structures are both strong, then so is the resulting access structure.*

Proof. Let $m = m' + m''$. Let $\{(X, t'_X)\}_{X \in \Gamma'_{\mathsf{Qual}}}$ and $\{(X, t''_X)\}_{X \in \Gamma''_{\mathsf{Qual}}}$ be the set of thresholds satisfying Definition 2.2 for the access structures $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$ and $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}})$, respectively. Finally, let $\alpha'(m')$ and $\alpha''(m'')$ be the relative differences of the two VCSs. Define $\alpha(m)$ to be

$$\alpha(m) = \frac{\min\{\alpha'(m') \cdot m', \alpha''(m'') \cdot m''\}}{m}.$$

We have to show that the matrices S^0 and S^1, constructed using the previously described technique, are basis matrices for the access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}) = (\Gamma'_{\mathsf{Qual}} \cup \Gamma''_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}} \cap \Gamma''_{\mathsf{Forb}})$.

Let X be a subset of participants. First, suppose that $X \in \Gamma'_{\mathsf{Qual}} \cap \Gamma''_{\mathsf{Qual}}$ and let $t_X = t'_X + t''_X$. It results that

$$\begin{aligned} w(S^0_X) &= w(\widehat{R}^0_X \circ \widehat{T}^0_X) \\ &= w(\widehat{R}^0_X) + w(\widehat{T}^0_X) \\ &= w(R^0_X) + w(T^0_X) \\ &\leq t'_X - \alpha'(m') \cdot m' + t''_X - \alpha''(m'') \cdot m'' \\ &\leq t_X - \alpha(m) \cdot m, \end{aligned}$$

whereas

$$\begin{aligned} w(S^1_X) &= w(\widehat{R}^1_X \circ \widehat{T}^1_X) \\ &= w(\widehat{R}^1_X) + w(\widehat{T}^1_X) \\ &\geq t'_X + t''_X \\ &= t_X. \end{aligned}$$

If $X \in \Gamma'_{\mathsf{Qual}} \backslash \Gamma''_{\mathsf{Qual}}$, then let $t_X = t'_X + w(\widehat{T}^0_X)$. It results that

$$\begin{aligned} w(S^0_X) &= w(\widehat{R}^0_X \circ \widehat{T}^0_X) \\ &= w(\widehat{R}^0_X) + w(\widehat{T}^0_X) \\ &\leq t'_X - \alpha'(m') \cdot m' + w(\widehat{T}^0_X) \\ &\leq t'_X - \alpha(m) \cdot m + w(\widehat{T}^0_X) \\ &= t_X - \alpha(m) \cdot m, \end{aligned}$$

whereas

$$\begin{aligned} w(S^1_X) &= w(\widehat{R}^1_X \circ \widehat{T}^1_X) \\ &= w(\widehat{R}^1_X) + w(\widehat{T}^1_X) \\ &\geq t'_X + w(\widehat{T}^1_X) \\ &= t'_X + w(\widehat{T}^0_X) \\ &= t_X. \end{aligned}$$

If $X \in \Gamma''_{\mathsf{Qual}} \backslash \Gamma'_{\mathsf{Qual}}$, then let $t_X = t''_X + w(\widehat{R}^0_X)$. We can prove that $w(S^0_X) \leq t_X - \alpha(m) \cdot m$ and $w(S^1_X) \geq t_X$. Using the reasoning applied to the previous case, Property 1. of Definition 2.2 is satisfied.
Now, suppose that $X \in \Gamma'_{\mathsf{Forb}} \cap \Gamma''_{\mathsf{Forb}}$. We have to show that $S^0[X] = S^1[X]$ up to a column permutation. We have that

$$\begin{aligned} S^0[X] &= \widehat{R}^0[X] \circ \widehat{T}^0[X] \\ &= \widehat{R}^1[X] \circ \widehat{T}^1[X] \\ &= S^1[X], \end{aligned}$$

where the second equality is satisfied up to a column permutation. Hence, Property 2. of Definition 2.2 is satisfied, too. It is easy to see that if the original access structures are strong, then so is the resulting access structure. Therefore, the theorem holds. $\square$

The construction technique employed in the proof of Theorem 4.4 does not work for general VCS (i.e., if they are not constructed from basis matrices). That is, given a $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}}, m')$-VCS and a $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}}, m'')$-VCS the "concatenation" of the matrices of the two schemes does not give rise to a $(\Gamma'_{\mathsf{Qual}} \cup \Gamma''_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}} \cap \Gamma''_{\mathsf{Forb}}, m' + m'')$-VCS. Indeed, consider the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ of a possible $(2,2)$-threshold VCS, denoted by Σ, obtained as follows. The collection $\mathcal{C}_0$ is realized considering the matrices obtained by permuting the columns of the matrices

$$\begin{bmatrix} 100 \\ 010 \end{bmatrix} \qquad \begin{bmatrix} 110 \\ 110 \end{bmatrix}$$

whereas the collection $\mathcal{C}_1$ is obtained by considering the matrices obtained by permuting the columns of the matrices

$$\begin{bmatrix} 100 \\ 011 \end{bmatrix} \qquad \begin{bmatrix} 110 \\ 001 \end{bmatrix}.$$

Suppose that we use Σ to realize VCSs for the strong access structures having bases $\{\{1,2\}\}$ and $\{\{2,3\}\}$. To construct the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ of a VCS for the strong access structure having basis $\{\{1,2\},\{2,3\}\}$ we cannot just "concatenate" the matrices of the two schemes. Indeed, it is easy to see that

$$M = \begin{bmatrix} 110000 \\ 110110 \\ 000110 \end{bmatrix} \in \mathcal{C}_0 \quad \text{and} \quad M' = \begin{bmatrix} 110000 \\ 001100 \\ 000011 \end{bmatrix} \in \mathcal{C}_1.$$

Hence, we get $w(M_{\{1,2\}}) = w(M'_{\{1,2\}}) = 4$ contradicting Property 1. of Definition 2.1. Therefore, the construction technique employed in the proof of Theorem 4.4 does not work for general VCSs.

It is not difficult to see that given a $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}}, m')$-VCS and a $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}}, m'')$-VCS the "concatenation" of all matrices of the two schemes gives rise to a $(\Gamma'_{\mathsf{Qual}} \cup \Gamma''_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}} \cap \Gamma''_{\mathsf{Forb}}, m' + m'')$-VCS if and only if for all $X \in \Gamma'_{\mathsf{Qual}} \cup \Gamma''_{\mathsf{Qual}}$ the following condition is satisfied.

$$\min_{M \in \mathcal{C}'_1} w(\widehat{M}_X) + \min_{M \in \mathcal{C}''_1} w(\widehat{M}_X) > \max_{M \in \mathcal{C}'_0} w(\widehat{M}_X) + \max_{M \in \mathcal{C}''_0} w(\widehat{M}_X).$$

Recall that, for $M \in \mathcal{C}_0 \cup \mathcal{C}_1$, $\widehat{M}$ is the matrix in which the i-th row has all zeroes as entries if the participant i is not an essential participant; otherwise, it is the row of M corresponding to participant i, as defined at the beginning of Section 4.2. The previous condition states that for any $X \in \Gamma'_{\mathsf{Qual}} \cup \Gamma''_{\mathsf{Qual}}$ and for any $M \in \mathcal{C}_1$ and $M' \in \mathcal{C}_0$ it results that $w(M_X) > w(M'_X)$. Therefore, there will be always a difference between a white and a black pixel. That is, the relative difference will be positive. More precisely, let $m = m' + m''$ and let

$$W_{\mathtt{min}}(X) = \min_{M \in \mathcal{C}'_1} w(\widehat{M}_X) + \min_{M \in \mathcal{C}''_1} w(\widehat{M}_X)$$

and

$$W_{\mathtt{max}}(X) = \max_{M \in \mathcal{C}'_0} w(\widehat{M}_X) + \max_{M \in \mathcal{C}''_0} w(\widehat{M}_X).$$

The contrast $\alpha(m)$ is equal to

$$\alpha(m) = \min_{X \in \Gamma'_{\mathsf{Qual}} \cup \Gamma''_{\mathsf{Qual}}} \frac{W_{\mathtt{min}}(X) - W_{\mathtt{max}}(X)}{m}.$$

The next corollary is an immediate consequence of Theorem 4.4.

Corollary 4.5 *Let* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ *be an access structure. If* $\Gamma_{\mathsf{Qual}} = \cup_{i=1}^{q} \Gamma_{(i,\mathsf{Qual})}$, $\Gamma_{\mathsf{Forb}} = \cap_{i=1}^{q} \Gamma_{(i,\mathsf{Forb})}$, *and, for* $i = 1, \ldots, q$, *there exists a* $(\Gamma_{(i,\mathsf{Qual})}, \Gamma_{(i,\mathsf{Forb})}, m_i)$*-VCS constructed using basis matrices, then there exists a* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$*-VCS constructed using basis matrices, where* $m = \sum_{i=1}^{q} m_i$. *If the* q *original access structures are strong then so is the resulting access structure.*

From Lemma 3.1 and Corollary 4.5 the following theorem holds.

Theorem 4.6 *Let* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ *be a strong access structure having basis* Γ_0. *There exists a* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$*-VCS where* $m = \sum_{X \in \Gamma_0} 2^{|X|-1}$.

The previous theorem states a general result on the existence of VCS for any strong access structure. For special classes of access structures it is possible to achieve a smaller value of m, as we will show in Section 6 for threshold access structures, and in Section 7 for graph-based access structures.

5 On the Structure of VCS

In this section we provide some useful properties of VCS. First, we investigate the case of "isolated" participants. Then, we show how to construct VCS for any non-connected access structure using VCS for its connected parts. Finally, we prove that any matrix M in the collection $\mathcal{C}_0 \cup \mathcal{C}_1$ has to contain some predefined sub-matrices, which we call "unavoidable patterns".

5.1 Isolated Participants

In this section we show that we do not need to consider access structures containing "isolated" participants, i.e., we can suppose that $|X| \geq 2$ for any $X \in \Gamma_{\mathsf{Qual}}$.

This is shown as follows. Suppose that $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is an access structure on participant set $\mathcal{P}$, and suppose that $x \notin \mathcal{P}$. Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the collections of matrices in a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS.

First, we show how to construct a VCS for the access structure $(\Gamma_{\mathsf{Qual}} \cup \{\{x\}\}, \Gamma_{\mathsf{Forb}})$.

Lemma 5.1 *Let* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ *be an access structure on a set of participants* $\mathcal{P}$, *and let* $x \notin \mathcal{P}$. *If there exists a* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$*-VCS, then there exists a* $(\Gamma_{\mathsf{Qual}} \cup \{\{x\}\}, \Gamma_{\mathsf{Forb}}, m)$*-VCS.*

Proof. Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the collections of matrices in a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS. Then, for any $M \in \mathcal{C}_0$, adjoin a new row (for participant x) consisting entirely of '0's. Similarly, for any $M' \in \mathcal{C}_1$, adjoin a new row (for participant x) consisting entirely of '1's. $\square$

Of course, Lemma 5.1 can be applied as many times as desired, if there is more than one isolated participant.

We now give a modification of Lemma 5.1 which shows how to construct a VCS in which every subset of participants containing x is qualified.

Lemma 5.2 *Let* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ *be an access structure on a set of participants* $\mathcal{P}$*, and let* $x \notin \mathcal{P}$*. If there exists a* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$*-VCS, then there exists a* $(\Gamma'_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m+1)$*-VCS, where*

$$\Gamma'_{\mathsf{Qual}} = \Gamma_{\mathsf{Qual}} \cup \{X \cup \{x\} : X \subseteq \mathcal{P}\}.$$

Proof. Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the collections of matrices in a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS. Then, for any $M \in \mathcal{C}_0$, adjoin a new row (for participant x) consisting entirely of '0's, and adjoin a column of '0's. Similarly, for any $M' \in \mathcal{C}_1$, adjoin a new row (for participant x) consisting entirely of '1's, and a column of '0's, except that the entry in row x and column $m+1$ is a '1'. □

As with the previous lemma, Lemma 5.2 can be iterated.

5.2 Non-Connected Access Structures

An access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ on a set of participants $\mathcal{P}$ is said to be *connected* if there is no partition of $\mathcal{P}$ into two non-empty sets $\mathcal{P}'$ and $\mathcal{P}''$ such that $\Gamma_0 \subseteq 2^{\mathcal{P}'} \cup 2^{\mathcal{P}''}$. The next technical lemma will be used in the construction of VCSs for non-connected access structures, given VCSs for its connected parts.

Lemma 5.3 *Let* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ *be an access structure. 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* $n \times p$ *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* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m+p)$*-VCS.*

Proof. Since we concatenate the same matrix D to any $M \in \mathcal{C}_0 \cup \mathcal{C}_1$, 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 $\mathcal{C}_0$ and $\mathcal{C}_1$ to $\mathcal{C}'_0$ and $\mathcal{C}'_1$. Only the relative difference $\alpha'(m')$ changes, becoming $\alpha'(m') = (\alpha(m) \cdot m)/(m+t)$. □

The next example will help in illustrating the technique employed in the previous lemma.

Example 5.4 The following collections $\mathcal{C}_0$ and $\mathcal{C}_1$ represent a $(2,2)$-threshold VCS with $m = 2$.

$$\mathcal{C}_0 = \left\{ \begin{bmatrix} 10 \\ 10 \end{bmatrix}, \begin{bmatrix} 01 \\ 01 \end{bmatrix} \right\} \qquad \mathcal{C}_1 = \left\{ \begin{bmatrix} 10 \\ 01 \end{bmatrix}, \begin{bmatrix} 01 \\ 10 \end{bmatrix} \right\}.$$

Setting $D = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ we get $\mathcal{C}'_0 = \left\{ \begin{bmatrix} 101 \\ 101 \end{bmatrix}, \begin{bmatrix} 011 \\ 011 \end{bmatrix} \right\}$ and $\mathcal{C}'_1 = \left\{ \begin{bmatrix} 101 \\ 011 \end{bmatrix}, \begin{bmatrix} 011 \\ 101 \end{bmatrix} \right\}$.

The collections $\mathcal{C}'_0$ and $\mathcal{C}'_1$ constitute a 2 out of 2 threshold VCS with $m = 3$.

△

Let $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$ and $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}})$ be two access structures on disjoint sets of participants $\mathcal{P}'$ and $\mathcal{P}''$, respectively. Define the *sum* of the two access structures on the set of participants $\mathcal{P}' \cup \mathcal{P}''$ to be $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$, where

$$\Gamma_{\mathsf{Qual}} = \Gamma'_{\mathsf{Qual}} \cup \Gamma''_{\mathsf{Qual}}$$

and

$$\Gamma_{\mathsf{Forb}} = \{X \cup Y : X \in \Gamma'_{\mathsf{Forb}}, Y \in \Gamma''_{\mathsf{Forb}}\}.$$

If an access structure is not connected, then we can realize a VCS for it simply by constructing VCS for its connected parts and then by putting together the schemes in a suitable way, as shown in the next theorem.

Theorem 5.5 *Let $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$ and $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}})$ be two access structures on disjoint sets of participants $\mathcal{P}'$ and $\mathcal{P}''$, respectively, and let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be their sum. If there exist a $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}}, m')$-VCS and a $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}}, m'')$-VCS, then there is a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS, where $m = \max\{m', m''\}$.*

Proof. Let $\mathcal{C}'_0$, $\mathcal{C}'_1$ and $\mathcal{C}''_0$, $\mathcal{C}''_1$ be the collections of matrices in the VCSs for access structures $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$ and $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}})$, respectively. Without loss of generality, suppose that $|\mathcal{C}'_0| = |\mathcal{C}'_1| = r'$, $|\mathcal{C}''_0| = |\mathcal{C}''_1| = r''$ and $m' > m''$. From Lemma 5.3 there exists a $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}}, m')$-VCS. Let $\mathcal{C}'''_0$ and $\mathcal{C}'''_1$ be the collections of matrices in this $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}}, m')$-VCS. The collections of matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ of a VCS for the access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ are constructed as follows.

$$\mathcal{C}_0 = \{M : M[\mathcal{P}'] \in \mathcal{C}'_0,\ M[\mathcal{P}''] \in \mathcal{C}'''_0\} \ \text{ and } \ \mathcal{C}_1 = \{M : M[\mathcal{P}'] \in \mathcal{C}'_1,\ M[\mathcal{P}''] \in \mathcal{C}'''_1\}.$$

Notice that $|\mathcal{C}_0| = |\mathcal{C}_1| = r = r' \cdot r''$ as from any matrix T in $\mathcal{C}'_0$ (resp. $\mathcal{C}'_1$) we get r'' matrices to insert in $\mathcal{C}_0$ (resp. $\mathcal{C}_1$) by "padding" T with all the matrices in $\mathcal{C}'''_0$ (resp. $\mathcal{C}'''_1$) one at a time. It is immediate to verify that Property 1. of Definition 2.1 is satisfied. Let's verify Property 2. of Definition 2.1 Let $X \in \Gamma'_{\mathsf{Forb}}$ ($X \in \Gamma''_{\mathsf{Forb}}$, resp.) and let $M \in \mathcal{C}'_0 \cup \mathcal{C}'_1$ ($M \in \mathcal{C}'''_0 \cup \mathcal{C}'''_1$, resp.). By η^i_X (μ^i_X, resp.), where $i \in \{0,1\}$, we denote the number of times that the matrix $M[X]$ appears in the collection $\{A[X] : A \in \mathcal{C}'_i\}$ ($\{A[X] : A \in \mathcal{C}'''_i\}$, resp.). From Property 2. of Definition 2.1 we have that $\eta^0_X = \eta^1_X$ and $\mu^0_X = \mu^1_X$. Finally, for $M \in \mathcal{C}_0 \cup \mathcal{C}_1$, let γ^i_X, where $i \in \{0,1\}$, denote the number of times that the matrix $M[X]$ appears in the collection $\{A[X] : A \in \mathcal{C}_i\}$. Recall that $|\mathcal{C}_0| = |\mathcal{C}_1| = r = r' \cdot r''$. To prove that Property 2. of Definition 2.1 is satisfied we have to show that for any $X \in \Gamma_{\mathsf{Forb}}$ it holds that $\gamma^0_X = \gamma^1_X$. Let $X \in \Gamma_{\mathsf{Forb}}$. If $X \subseteq \mathcal{P}' \backslash \mathcal{P}''$ (the case $X \subseteq \mathcal{P}'' \backslash \mathcal{P}'$ is analogous), then

$$\gamma^0_X = \eta^0_X \cdot r'' = \eta^1_X \cdot r'' = \gamma^1_X.$$

If $X = Y \cup Z$ where $Y \in \Gamma'_{\mathsf{Forb}}$ and $Z \in \Gamma''_{\mathsf{Forb}}$, then

$$\gamma^0_X = \eta^0_Y \cdot \mu^0_Z = \eta^1_Y \cdot \mu^1_Z = \gamma^1_X.$$

Hence the theorem follows. $\square$

The next example will help in illustrating the technique employed in the previous theorem.

Example 5.6 Suppose that $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$ is a $(2,2)$-threshold access structure on participant set $\mathcal{P}' = \{1,2\}$, and $(\Gamma''_{\mathsf{Qual}}, \Gamma''_{\mathsf{Forb}})$ is a $(2,2)$-threshold access structure on participant set $\mathcal{P}' = \{3,4\}$. The sum of these two access structures is $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$, where

$$\Gamma_{\mathsf{Qual}} = \{\{1,2\},\{3,4\}\}$$

and

$$\Gamma_{\mathsf{Forb}} = \{\{1\},\{2\},\{3\},\{4\},\{1,3\},\{1,4\},\{2,3\},\{2,4\}\}.$$

A VCS for the access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is obtained by considering the following collections $\mathcal{C}_0$ and $\mathcal{C}_1$.

$$\mathcal{C}_0 = \left\{ \begin{bmatrix} 10 \\ 10 \\ 10 \\ 10 \end{bmatrix}, \begin{bmatrix} 01 \\ 01 \\ 01 \\ 01 \end{bmatrix}, \begin{bmatrix} 10 \\ 10 \\ 01 \\ 01 \end{bmatrix}, \begin{bmatrix} 01 \\ 01 \\ 10 \\ 10 \end{bmatrix} \right\}.$$

$$\mathcal{C}_1 = \left\{ \begin{bmatrix} 10 \\ 01 \\ 10 \\ 01 \end{bmatrix}, \begin{bmatrix} 01 \\ 10 \\ 10 \\ 01 \end{bmatrix}, \begin{bmatrix} 10 \\ 01 \\ 01 \\ 10 \end{bmatrix}, \begin{bmatrix} 01 \\ 10 \\ 01 \\ 10 \end{bmatrix} \right\}.$$

The access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ has $\Gamma_0 = \Gamma_{\mathsf{Qual}}$. It is interesting to observe that the VCS constructed above is not a VCS for the strong access structure where Γ_{Qual} is the closure of Γ_0, and by a result that we prove later (Theorem 5.12), it can be shown that there is no VCS with $m = 2$ for the strong access structure having basis Γ_0. It can also be shown that there is no VCS with $m = 2$ constructed from basis matrices with $m = 2$, for the access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$. $\triangle$

5.3 Unavoidable Patterns

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 $\mathcal{P}$. Recall that, for $X \subseteq \mathcal{P}$, M_X denotes the m-vector obtained considering the *or* of the rows 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.

Lemma 5.7 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set of participants $\mathcal{P}$. Let $X, Y \subseteq \mathcal{P}$ be two non-empty subsets of participants, such that $X \cap Y = \emptyset$, $X \in \Gamma_{\mathsf{Forb}}$ and $X \cup Y \in \Gamma_{\mathsf{Qual}}$. Then in any $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS, for any matrix $M \in \mathcal{C}_1$ it holds that*

$$w(M_{XY}) - w(M_X) \geq \alpha(m) \cdot m.$$

Proof. Let M be any matrix in $\mathcal{C}_1$. From Property 1. of Definition 2.1 we have that $w(M_{XY}) \geq t_{XY}$. Since $X \in \Gamma_{\mathsf{Forb}}$, then from Property 2. of Definition 2.1, there is at least one matrix $M' \in \mathcal{C}_0$ such that $M[X] = M'[X]$. Therefore, we have

$$\begin{aligned} w(M_X) &= w(M'_X) \\ &\leq w(M'_{XY}) \\ &\leq t_{XY} - \alpha(m) \cdot m \\ &\leq w(M_{XY}) - \alpha(m) \cdot m, \end{aligned}$$

where the second inequality of the above expression derives from Property 1. of Definition 2.1. Thus, the lemma is proved. $\square$

The matrices in $\mathcal{C}_0 \cup \mathcal{C}_1$ have to contain some predefined patterns which we call *unavoidable patterns*. For instance, suppose $X \in \Gamma_{\mathsf{Qual}}$ and $X \setminus \{i\} \in \Gamma_{\mathsf{Forb}}$. Then for any $M \in \mathcal{C}_1$, the matrix $M[X]$ contains at least $\alpha(m) \cdot m$ columns with a '1' in the i-th row and '0's in the other rows. This is an immediate consequence of Lemma 5.7. Indeed, by considering $X = Y \cup \{i\}$ we get

$$w(M_{Y \cup \{i\}}) - w(M_Y) \geq \alpha(m) \cdot m.$$

Therefore, there must be at least $\alpha(m) \cdot m$ columns in $M[X]$ with a '1' in row i and '0's in the other rows.

The next corollaries are immediate consequences of the existence of unavoidable patterns.

Recall that a participant i is an essential participant if there exists a set $X \subseteq \mathcal{P}$ such that $X \cup \{i\} \in \Gamma_{\mathsf{Qual}}$ but $X \notin \Gamma_{\mathsf{Qual}}$. We say that i is a *strongly essential participant* if there exists a set $X \subseteq \mathcal{P}$ such that $X \cup \{i\} \in \Gamma_{\mathsf{Qual}}$ and $X \in \Gamma_{\mathsf{Forb}}$.

Corollary 5.8 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set of participants $\mathcal{P}$. Suppose that i is a strongly essential participant, and suppose that $\{i\} \in \Gamma_{\mathsf{Forb}}$. Then in any $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS, for any matrix $M \in \mathcal{C}_0 \cup \mathcal{C}_1$ it holds that*

$$w(M_i) \geq \alpha(m) \cdot m.$$

Proof. Let X be a subset such that $X \cup \{i\} \in \Gamma_{\mathsf{Qual}}$ and $X \in \Gamma_{\mathsf{Forb}}$. For any matrix $M \in \mathcal{C}_1$, because of the unavoidable patterns (Lemma 5.7), the matrix $M[X]$ contains at least $\alpha(m) \cdot m$ columns with a '1' in the i-th row and '0's in the other rows. Therefore, $w(M_i) \geq \alpha(m) \cdot m$. Since $\{i\} \in \Gamma_{\mathsf{Forb}}$, the result also holds for any matrix $M \in \mathcal{C}_0$ by Property 2. of Definition 2.1. $\square$

Corollary 5.9 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure, Suppose that $X \in \Gamma_{\mathsf{Qual}}$ and $X \setminus \{i\} \in \Gamma_{\mathsf{Forb}}$ for all $i \in X$. Then, in any $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS , we have $t_X \geq |X| \cdot \alpha(m) \cdot m$.*

Proof. Let $i \in X$, and define $Y = X \setminus \{i\}$. Let $M \in \mathcal{C}_0$. From Property 1. of Definition 2.1 it results that $w(M_Y) \leq w(M_X) \leq t_X - \alpha(m) \cdot m$. From Property 2. of Definition 2.1 we have that there exists at least a matrix $M' \in \mathcal{C}_1$ such that $w(M'_Y) = w(M_Y)$. Because of the unavoidable patterns, we have that

$$w(M'_Y) \geq |Y| \cdot \alpha(m) \cdot m = (|X| - 1)\alpha(m) \cdot m.$$

Hence, we get that $t_X \geq |X| \cdot \alpha(m) \cdot m$. $\square$

The next lemma states the existence of other unavoidable patterns in any matrix in $\mathcal{C}_0 \cup \mathcal{C}_1$. Basically, it says that for any $Y \in \Gamma_{\mathsf{Forb}}$ and for any $M \in \mathcal{C}_0 \cup \mathcal{C}_1$, the matrix $M[Y]$ contains at least $\alpha(m) \cdot m$ columns whose entries are all equal to zero.

Lemma 5.10 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be a strong access structure, and suppose that $Y \in \Gamma_{\mathsf{Forb}}$. Then, in any $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS, for any matrix $M \in \mathcal{C}_0 \cup \mathcal{C}_1$ it holds that*

$$w(M_Y) \leq \min\{t_X : Y \subset X,\ X \in \Gamma_{\mathsf{Qual}}\} - \alpha(m) \cdot m.$$

Proof. Because of Property 2. of Definition 2.1, we prove the lemma only for $M \in \mathcal{C}_0$. Let $X \in \Gamma_{\mathsf{Qual}}$, $Y \subset X$. From Property 1. of Definition 2.1 we get $w(M_X) \leq t_X - \alpha(m) \cdot m$. Since $Y \subseteq X$ we have that $w(M_Y) \leq w(M_X)$, and the result follows. $\square$

The next lemma shows the existence of unavoidable patterns in any matrix $M \in \mathcal{C}_0$. It states that for any $X \in \Gamma_{\mathsf{Qual}}$ and any $M \in \mathcal{C}_0$, the matrix $M[X]$ contains at least $\alpha(m) \cdot m$ columns with entries all equal to '0'.

Lemma 5.11 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set $\mathcal{P}$ of participants. Suppose $X \in \Gamma_{\mathsf{Qual}}$. Then, in any $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS for any $M \in \mathcal{C}_0$, the matrix $M[X]$ has at least $\alpha(m) \cdot m$ columns with entries all equal to zero.*

Proof. From Property 1. of Definition 2.1, we have the following:

$$w(M_X) \leq t_X - \alpha(m) \cdot m \leq m - \alpha(m) \cdot m.$$

Therefore, the lemma holds. $\square$

We now look at a consequence of the unavoidable patterns for $(2, n)$-threshold access structures. In a VCS for such an access structure, the rows of any matrix $M \in \mathcal{C}_1$ represent a Sperner family[1]. In fact, let $M \in \mathcal{C}_1$ be an $n \times m$ boolean matrix and let $G = \{g_1, \ldots, g_m\}$ be a ground set. For $i = 1, \ldots, n$, row i of M represents the subset $A_i = \{g_q : M(i, q) = 1\}$ of G. Since any two rows of M contain the patterns $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, then the sets $A_1, \ldots, A_n$ constitute a Sperner family in the ground set G. Therefore, the rows of the matrix M represent a Sperner family. This will be exploited further in Theorem 6.6 and in Section 7. The scheme given in Example 2.4 is constructed from a Sperner family in a ground set containing four elements.

The next two theorems provide a characterization of VCS having $m = 2$ and of $(3, 3)$-threshold VCS with $m = 4$. Both theorems are based on the existence of unavoidable patterns.

Theorem 5.12 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be a strong access structure on the set of participants $\mathcal{P}$ containing no isolated participants. If there exists a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, 2)$-VCS, then the basis Γ_0 is the edge-set of a complete bipartite graph.*

Proof. Suppose there exists a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, 2)$-VCS. Then for any $X \in \Gamma_0$ it results that $|X| = 2$. Indeed, there are no isolated participants, and hence $|X| \geq 2$. On the other hand, $|X| \leq 2$, since otherwise Corollary 3.5 would imply that $m \geq 4$. Therefore, Γ_0 is the edge-set of some graph G with vertex-set $\mathcal{P}$.
We first show that the graph G is connected. Indeed, suppose by contradiction that there exists a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, 2)$-VCS and that G is not connected. Therefore, there exists a partition of $\mathcal{P}$ into two non-empty sets $\mathcal{P}'$ and $\mathcal{P}''$ such that $\Gamma_0 \subseteq 2^{\mathcal{P}'} \cup 2^{\mathcal{P}''}$. Let $\{i, j\} \in \Gamma_{\mathsf{Qual}} \cap 2^{\mathcal{P}'}$ and $\ell \in \mathcal{P}''$. Because of the unavoidable patterns and since the access structure does not contain isolated participants, we have that for any $M \in \mathcal{C}_1$ the matrix $M[\{i, j, \ell\}]$ is equal, up to a column permutation, to one of the following two matrices

$$M' = \begin{bmatrix} M'[i] \\ M'[j] \\ M'[\ell] \end{bmatrix} = \begin{bmatrix} 10 \\ 01 \\ 01 \end{bmatrix} \qquad M'' = \begin{bmatrix} M''[i] \\ M''[j] \\ M''[\ell] \end{bmatrix} = \begin{bmatrix} 10 \\ 01 \\ 10 \end{bmatrix}.$$

[1]A Sperner family $\mathcal{SF}$ over a ground set G is a family $\mathcal{SF} = \{A_1, \ldots, A_t\}$ of subsets of G such that A_j is not a subset of A_j for $i \neq j$, for other information see [9].

Since the access structure is strong and $w(M'_{\{i,j,\ell\}}) = w(M''_{\{i,j,\ell\}}) = 2$, from Property 1. of Definition 2.1, it result that for any $\widehat{M} \in \mathcal{C}_0$ the matrix $\widehat{M}[X \cup \{\ell\}]$ is equal, up to a column permutation, to

$$\begin{bmatrix} 10 \\ 10 \\ 10 \end{bmatrix}.$$

In this case we have that $w(M'_{\{i,\ell\}}) > w(\widehat{M}_{\{i,\ell\}})$ and $w(M''_{\{j,\ell\}}) > w(\widehat{M}_{\{j,\ell\}})$ contradicting Property 2. of Definition 2.1 since $\{i,\ell\}$ and $\{j,\ell\}$ belong to Γ_{Forb}. Therefore, Γ_0 is the edge-set of some connected graph G.

Now, suppose that G is not a complete multipartite graph. Then from Theorem 4.2 in [5], G contains an induced subgraph which is isomorphic either to H or to P_3, where $V(H) = V(P_3) = \{1,2,3,4\}$, $E(H) = \Big\{\{1,2\},\{2,3\},\{3,4\},\{2,4\}\Big\}$, and $E(P_3) = \Big\{\{1,2\},\{2,3\},\{3,4\}\Big\}$.

First, suppose that G is isomorphic to H. The graph H contains K_3 as induced subgraph which can represent the basis of a $(2,3)$-threshold structure. There does not exist a Sperner family on a ground set of cardinality two (see [9] for details). Hence by consideration of the unavoidable patterns and Lemma 3.4, it must be the case that $m \geq 3$.

Next, we prove that if G is isomorphic to P_3, then $m \geq 3$. Let Γ'_{Qual} be the closure of $\Gamma'_0 = \Big\{\{1,2\},\{2,3\},\{3,4\}\Big\}$. Suppose by contradiction that there exists a $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}}, 2)$-VCS. Let $M \in \mathcal{C}_1$. Since $\{1,2\}$, $\{2,3\}$, $\{3,4\} \in \Gamma'_0$, because of the unavoidable patterns the matrix M has to be equal, up to a column permutation, to

$$M = \begin{bmatrix} 10 \\ 01 \\ 10 \\ 01 \end{bmatrix}.$$

From Property 2. of Definition 2.1 any row of any matrix $M' \in \mathcal{C}_0$ has weight 1. From Property 1. of Definition 2.1, for any $X \in \Gamma'_0$, we have that $w(M_X) > w(M'_X)$. Hence, the matrix M' is equal, up to a column permutation, to

$$M' = \begin{bmatrix} 10 \\ 10 \\ 10 \\ 10 \end{bmatrix}.$$

Considering the matrices M and M' we have that $w(M_{14}) > w(M'_{14})$ contradicting Property 2. of Definition 2.1 since $\{1,4\} \in \Gamma'_{\mathsf{Forb}}$. Thus, there does not exist a $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}}, 2)$-VCS where Γ'_{Qual} is the closure of $\Gamma'_0 = \Big\{\{1,2\},\{2,3\},\{3,4\}\Big\}$.

Finally, suppose that G is a complete multipartite graph having at least three parts. The graph G contains K_3 as induced subgraph, and, as above, $m \geq 3$.

Therefore, Γ_0 is the edge-set of a complete bipartite graph.

□

The condition of above theorem is necessary and sufficient. We will see in Theorem 7.5 that, for any strong access structure having as basis the edge-set of a complete bipartite graph, there exists a visual cryptography scheme with $m = 2$.

By exploiting the unavoidable patterns the following theorem proves that in any $(3,3)$-threshold VCS with $m = 4$ all matrices have a (specified) unique form up to a column permutation. To be specific, any matrix $M \in \mathcal{C}_0$ has as its columns all the boolean 3-vectors having an even number of '1's; whereas, any matrix $M' \in \mathcal{C}_1$ has as its columns all the boolean 3-vectors having an odd number of '1's.

Theorem 5.13 *Let* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ *be the access structure of a* $(3,3)$*-threshold VCS on the set of participants* $\mathcal{P} = \{1,2,3\}$*. In any* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, 4)$*-VCS all matrices have a unique form up to a column permutation. That is, any matrix* $M \in \mathcal{C}_1$ *and any matrix* $M' \in \mathcal{C}_0$ *is equal, up to a column permutation, (respectively) to*

$$M = \begin{bmatrix} 1001 \\ 0101 \\ 0011 \end{bmatrix} \qquad M' = \begin{bmatrix} 0110 \\ 0101 \\ 0011 \end{bmatrix}.$$

Proof. First, let $M \in \mathcal{C}_1$. Because of the unavoidable patterns we have that, up to a column permutation,

$$M = \begin{bmatrix} 1 & 0 & 0 & \star \\ 0 & 1 & 0 & \star \\ 0 & 0 & 1 & \star \end{bmatrix},$$

where $\star$ denotes the presence of either a one or a zero. Assume that the fourth entry of a row of M is zero: Without loss of generality, suppose that $M[1] = [1,0,0,0]$. Because of the unavoidable patterns (see Lemma 5.11), any matrix in $\mathcal{C}_0$ has a column with all entries equal to zero. From Property 2. of Definition 2.1 there exists at least a matrix $M' \in \mathcal{C}_0$ such that $w(M'_1) = 1$. Therefore, the matrix M', up to a column permutation, looks like

$$M' = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & \star & \star & \star \\ 0 & \star & \star & \star \end{bmatrix}.$$

By consideration of two rows of M, it is immediate to see that other unavoidable patterns of any matrix in the collection $\mathcal{C}_0$ are the following columns

$$\begin{bmatrix} 1 \\ 0 \\ \star \end{bmatrix} \quad \begin{bmatrix} 1 \\ \star \\ 0 \end{bmatrix} \quad \begin{bmatrix} \star \\ 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} \star \\ 0 \\ 1 \end{bmatrix}.$$

From Property 2. of Definition 2.1 and from the existence of the unavoidable patterns, the matrix M' has to be, up to a column permutation, the following

$$M' = \begin{bmatrix} 0100 \\ 0010 \\ 0001 \end{bmatrix}.$$

The matrix M' and Property 2. of Definition 2.1 imply that any matrix $M \in \mathcal{C}_1$ with $w(M_1) = 1$ is equal, up to a column permutation, to

$$M = \begin{bmatrix} 1000 \\ 0100 \\ 0010 \end{bmatrix},$$

leading to a contradiction, i.e., $w(M_{123}) = w(M'_{123}) = 3$. Therefore, any matrix $M \in \mathcal{C}_1$ does not have a row of weight 1, and it is equal, up to a column permutation, to

$$M = \begin{bmatrix} 1001 \\ 0101 \\ 0011 \end{bmatrix}.$$

Hence, any matrix $M' \in \mathcal{C}_0$ is equal, up to column permutation, to

$$M' = \begin{bmatrix} 0110 \\ 0101 \\ 0011 \end{bmatrix},$$

which proves that for any (3,3)-threshold VCS with $m = 4$, any matrix $M \in \mathcal{C}_0$ has as columns all the boolean 3-vectors having an even number of '1's; whereas, any matrix $M' \in \mathcal{C}_1$ has as columns all the boolean 3-vectors having an odd number of '1's. $\square$

6 Threshold Schemes

In this section, we study (k, n)-threshold VCS. We can construct such schemes by using the two techniques described in Sections 4.1 and 4.2. By using the technique based on cumulative arrays we obtain a (k, n)-threshold VCS in which $m = 2^{\binom{n}{k-1}-1}$ and $t_X = m$ for any set X of cardinality k; whereas by using the technique of Section 4.2 we obtain a (k, n)-threshold VCS in which $m = \binom{n}{k} \cdot 2^{k-1}$ and t_X has the same value for any set X of cardinality k.

In the following section we describe a method to construct threshold VCSs achieving better results.

6.1 A More Efficient Construction for Threshold Schemes

In this section we describe a construction for threshold VCSs based on *perfect hashing* [8, 10, 4].

Definition 6.1 *A starting matrix $SM(n, \ell, k)$ is a $n \times \ell$ matrix whose entries are elements of a ground set $\{a_1, \ldots, a_k\}$, with the property that, for any subset of k rows, there exists at least one column such that the entries in the k given rows of that column are all distinct.*

Given a matrix $SM(n, \ell, k)$ we can construct a (k, n)-threshold VCS as follows: The $n \times (\ell \cdot 2^{k-1})$ basis matrices S^0 and S^1 are constructed by replacing the symbols $a_1, \ldots, a_k$, respectively, with the 1-st,..., k-th rows of the corresponding basis matrices of the (k, k)-threshold VCS described in Section 3. The scheme obtained is a (k, n)-threshold VCS as the following theorem shows.

Theorem 6.2 *If there exists a $SM(n, \ell, k)$ then there exists a (k, n)-threshold VCS with $m = \ell \cdot 2^{k-1}$.*

Proof. Let S_k^0 and S_k^1 be basis matrices of the (k, k)-threshold VCS described in Section 3 and let $SM(n, \ell, k)$ be a starting matrix whose entries are elements of a set $\{a_1, \ldots, a_k\}$. Finally, let M_0 and M_1 be two $n \times (\ell \cdot 2^{k-1})$ matrices constructed by replacing the symbols

$a_1, \ldots, a_k$, with the 1-st,$\ldots$, k-th rows of the basis matrices S_k^0 and S_k^1, respectively. In the previous construction, when we replace the symbols $a_1, \ldots, a_k$ of SM with the rows of S_k^0 (S_k^1, resp.) the column i of SM is expanded into an $n \times 2^{k-1}$ matrix referred to as the *basic block* $B_{0,i}$ ($B_{1,i}$, resp.). We will show that the matrices M_0 and M_1 are basis matrices of a (k, n)-threshold VCS.

Fix any $d \geq k$ rows of a basic block $B_{0,i}$ ($B_{1,i}$, resp.). Either these rows comprise all the rows of S_k^0 (S_k^1, resp.), where any row of S_k^0 (S_k^1, resp.) can appear more than once, and thus their "or" has weight $2^{k-1} - 1$ (2^{k-1}, resp.), or they contain at most $k - 1$ distinct rows of S_k^0 (S_k^1, resp.) whose "or" has the same weight in both basic blocks $B_{0,i}$ and $B_{1,i}$. Therefore, Property 1. of Definition 2.2 is satisfied.

To prove that Property 2. of Definition 2.2 is satisfied we have to show that for any set $X \subseteq \{1, \ldots, n\}$ of cardinality at most $k - 1$, $M_0[X]$ is equal to $M_1[X]$ up to a column permutation. This is true since, for any $i \in \{1, \ldots, \ell\}$, it holds that $B_{0,i}[X]$ is equal to $B_{1,i}[X]$ up to a column permutation. $\square$

Example 6.3 To construct a $(2, n)$-threshold VCS consider the matrix $SM(n, \lceil \log n \rceil, 2)$ in which the $\lceil \log n \rceil$ entries in row i are equal to $a_{1+b^i_{\lceil \log n \rceil - 1}}, \cdots, a_{1+b_1^i}, a_{1+b_0^i}$, where the bits b_j^i are the coefficients in the binary representation of $i - 1$, that is

$$i - 1 = b_0^i + b_1^i 2 + \cdots + b^i_{\lceil \log n \rceil - 1} 2^{\lceil \log n \rceil - 1}.$$

The two basis matrices are constructed by substituting 01 for a_1 and a_2 in SM to obtain S^0 and 01 and 10 for a_1 and a_2 in SM to obtain S^1, respectively.

The resulting scheme has $m = 2 \cdot \lceil \log n \rceil$ which is a considerable improvement compared to the scheme proposed in [11] where $m = n$. However, we will provide in Section 7 an even better construction, which is in fact optimal with respect to m.

Here are two examples to illustrate. If $n = 4$ we obtain the two 4×4 matrices:

$$S^0 = \begin{bmatrix} 10 & 10 \\ 10 & 10 \\ 10 & 10 \\ 10 & 10 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 10 & 10 \\ 10 & 01 \\ 01 & 10 \\ 01 & 01 \end{bmatrix}.$$

If $n = 8$ we obtain the two 8×6 matrices:

$$S^0 = \begin{bmatrix} 10 & 10 & 10 \\ 10 & 10 & 10 \\ 10 & 10 & 10 \\ 10 & 10 & 10 \\ 10 & 10 & 10 \\ 10 & 10 & 10 \\ 10 & 10 & 10 \\ 10 & 10 & 10 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 10 & 10 & 10 \\ 10 & 10 & 01 \\ 10 & 01 & 10 \\ 10 & 01 & 01 \\ 01 & 10 & 10 \\ 01 & 10 & 01 \\ 01 & 01 & 10 \\ 01 & 01 & 01 \end{bmatrix}.$$

$\triangle$

Example 6.4 A $(3,6)$-threshold VCS can be constructed considering the matrix $SM(6,3,3)$:

$$SM = \begin{bmatrix} a_1a_2a_3 \\ a_1a_3a_2 \\ a_2a_1a_3 \\ a_2a_3a_1 \\ a_3a_1a_2 \\ a_3a_2a_1 \end{bmatrix}.$$

Substituting 0011, 0101, 0110 for a_1, a_2, a_3 in SM to obtain S^0 and 0011, 0101, 1001 for a_1, a_2, a_3 in SM to obtain S^1 we obtain the two 6×12 matrices:

$$S^0 = \begin{bmatrix} 0011 & 0101 & 0110 \\ 0011 & 0110 & 0101 \\ 0101 & 0011 & 0110 \\ 0101 & 0110 & 0011 \\ 0110 & 0011 & 0101 \\ 0110 & 0101 & 0011 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 0011 & 0101 & 1001 \\ 0011 & 1001 & 0101 \\ 0101 & 0011 & 1001 \\ 0101 & 1001 & 0011 \\ 1001 & 0011 & 0101 \\ 1001 & 0101 & 0011 \end{bmatrix}.$$

$\triangle$

Example 6.5 A $(3,9)$-threshold visual cryptography scheme can be constructed considering the matrix SM(9,4,3):

$$SM = \begin{bmatrix} a_1a_1a_1a_1 \\ a_1a_2a_3a_2 \\ a_1a_3a_2a_3 \\ a_2a_1a_3a_3 \\ a_2a_2a_2a_1 \\ a_2a_3a_1a_2 \\ a_3a_1a_2a_2 \\ a_3a_2a_1a_3 \\ a_3a_3a_3a_1 \end{bmatrix}.$$

The above 9×4 matrix SM is equivalent to the classical affine plane of order three, see for example [9], and is a special case of a general construction given in [4]. This matrix is also described by Elias in [12] in a different context. Substituting 0011, 0101, 0110 for a_1, a_2, a_3 in SM to obtain S^0 and 0011, 0101, 1001 for a_1, a_2, a_3 in SM to obtain S^1 we obtain the two 9×16 matrices:

$$S^0 = \begin{bmatrix} 0011 & 0011 & 0011 & 0011 \\ 0011 & 0101 & 0110 & 0101 \\ 0011 & 0110 & 0101 & 0110 \\ 0101 & 0011 & 0110 & 0110 \\ 0101 & 0101 & 0101 & 0011 \\ 0101 & 0110 & 0011 & 0101 \\ 0110 & 0011 & 0101 & 0101 \\ 0110 & 0101 & 0011 & 0110 \\ 0110 & 0110 & 0110 & 0011 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 0011 & 0011 & 0011 & 0011 \\ 0011 & 0101 & 1001 & 0101 \\ 0011 & 1001 & 0101 & 1001 \\ 0101 & 0011 & 1001 & 1001 \\ 0101 & 0101 & 0101 & 0011 \\ 0101 & 1001 & 0011 & 0101 \\ 1001 & 0011 & 0101 & 0101 \\ 1001 & 0101 & 0011 & 1001 \\ 1001 & 1001 & 1001 & 0011 \end{bmatrix}.$$

$\triangle$

The SM matrix is a representation of a *Perfect Hash Family* (or PHF). Fredman and Komlós [8] proved that for any PHF it holds that $\ell = \Omega(k^{k-1}/k!)\log n$. They also proved the weaker but simpler bound $\ell = \Omega(1/\log k)\log n$. Mehlhorn [10] proved that there exist PHFs with $\ell = O(ke^k)\log n$. These bounds are in general, non-constructive, but in [4] there can be found some (constructive) recursive constructions for PHFs with $\ell = O\left((\log n)^{\log(\binom{k}{2}+1)}\right)$.

Naor and Shamir [11] showed that there exist (k,n)-threshold visual cryptography schemes with $m = 2^{O(k\log k)} \cdot \log n$. Our construction produces a smaller value of m than their construction, but this has been achieved by relaxing the condition that all thresholds t_X are equal as required in [11].

In the following we provide a lower bound on the pixel expansion m for any (k,n)-threshold VCS. Let $\mathcal{C}_0$ and $\mathcal{C}_1$ the collections of $n \times m$ boolean matrices of a (k,n)-threshold VCS on the set $\mathcal{P}$ of n participants. Moreover, let $G = \{g_1, \ldots, g_m\}$ be a ground set of m elements and let $M \in \mathcal{C}_1$. For $i = 1, \ldots, n$, row i of M represents the set $A_i = \{g_p : M(i,p) = 1\}$. Because of the unavoidable patterns, for any set $Y = \{j_1, \ldots, j_k\} \subseteq \{1, \ldots, n\}$, the matrix $M[Y]$, for each row $i \in \{1, \ldots, k\}$, has at least a column with a '1' in the i-th row and '0's in the other rows. This implies that the sets $A_{j_1}, \ldots, A_{j_k}$ are such that the union of any $k-1$ of them does not contain the remaining one. Hence, any matrix $M \in \mathcal{C}_1$ represents a family $\mathcal{A} = \{A_1, \ldots, A_n\}$ of subsets over the ground set G having the property that the union of any $k-1$ of them does not cover any of the remaining set (i.e, $A_{j_1} \not\subseteq A_{j_2} \cup \cdots \cup A_{j_k}$ for any distinct $j_1, \ldots, j_k \in \{1, \ldots, n\}$). Such set $\mathcal{A}$ is called a $(k-1)$-cover-free family [7] over a ground set of m elements. Therefore, for fixed n, the pixel expansion m is lower bounded by the size $\psi(n,k)$ of the smallest ground set G for which a $(k-1)$-cover-free family consisting of n sets exists.

Theorem 6.6 *In any (k,n)-threshold VCS the pixel expansion is $m \geq \psi(n,k)$.*

In the following we derive a simple lower bound on the value $\psi(n,k)$. Let $\mathcal{A} = \{A_1, \ldots, A_n\}$ be a $(k-1)$-cover-free family over a ground set $G = \{g_1, \ldots, g_\psi\}$, where $\psi = \psi(n,k)$. Let $\mathcal{F}$ be a family of subsets over the ground set G constructed from $\mathcal{A}$ as follows.

$$\mathcal{F} = \left\{\cup_{i=1}^{k-1} A_{j_i} : \{j_1, \ldots, j_{k-1}\} \subset \{1, \ldots, n\} \text{ and } A_{j_1}, \ldots, A_{j_{k-1}} \in \mathcal{A}\right\}.$$

That is, $\mathcal{F}$ comprises all the unions of any $k-1$ sets in $\mathcal{A}$. Hence, $|\mathcal{F}| = \binom{n}{k-1}$. It is immediate to see that $\mathcal{F}$ is a Sperner family over the ground set G. It is well-known (see for example [9]) that the maximum size of a Sperner family $\mathcal{F}$ in a ground set G of cardinality ψ is at most $\binom{\psi}{\lfloor\psi/2\rfloor}$; and equality occurs if and only if $\mathcal{F}$ consists of all subsets of G of cardinality $\left\lfloor\frac{\psi}{2}\right\rfloor$ (or all subsets of G of cardinality $\left\lceil\frac{\psi}{2}\right\rceil$). Hence, it has to be that $|\mathcal{F}| \leq \binom{\psi}{\lfloor\psi/2\rfloor}$ which implies that

$$\binom{n}{k-1} \leq \binom{\psi}{\lfloor\psi/2\rfloor}.$$

Since $\binom{\psi}{\lfloor\psi/2\rfloor} \leq 2^\psi$ and $\binom{n}{k-1} \geq (\frac{n}{k-1})^{k-1}$ we have that in any $(k-1)$-cover-free family $\psi = \Omega(k\log(n/k))$.

In [7] it has been proved a stronger asymptotic result: A $(k-1)$-cover-free family $\mathcal{CF}$ over a ground set of m elements exists only if

$$|\mathcal{CF}| \leq e^{(1+o(1))m/(k-1)}.$$

From the above arguments and because of Theorem 6.6 we get the following necessary conditions on the pixel expansion for a (k, n)-threshold VCS to exist.

Corollary 6.7 *In any (k, n)-threshold VCS with pixel expansion m, it results that*

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

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

7 VCS for Graph Access Structures

In this section, we study access structures based on graphs. We first recall some terminology from graph theory. Given a graph $G = (V(G), E(G))$ a *vertex cover* of G is a subset of vertices $A \subseteq V(G)$ such that every edge in $E(G)$ is incident with at least one vertex in A. The *complete graph* K_n is the graph on n vertices in which any two vertices are joined by an edge. A graph $G' = (V(G'), E(G'))$ is a subgraph of a given graph $G = (V(G), E(G))$ if $V(G') \subseteq V(G)$ and $E(G') \subseteq E(G)$. A *clique* of a graph G is any complete subgraph of G. The *complete multipartite graph* $K_{a_1,a_2,\ldots,a_n}$ is a graph on $\sum_{i=1}^{n} a_i$ vertices, in which the vertex set is partitioned into subsets of size a_i $(1 \leq i \leq n)$ called *parts*, such that vw is an edge if and only if v and w are in different parts. An alternative way to characterize a complete multipartite graph is to say that the complementary graph is a vertex-disjoint union of cliques. Note that the complete graph K_n can be thought of as a complete multipartite graph with n parts of size 1.

Let $\mathcal{P}$ denote the set of participants, and let G be a graph on vertex set $V(G) = \mathcal{P}$, having edge set $E(G)$. From G, we can define a (strong) access structure $\Gamma(G) = (\Gamma(G)_{\mathsf{Qual}}, \Gamma(G)_{\mathsf{Forb}})$ by specifying that the basis is $E(G)$. Thus a subset X of participants is qualified if the induced subgraph $G[X]$ contains at least one edge (and X is forbidden, otherwise). As is always the case, we are interested in the minimum value m for which such a VCS exists. We will use the notation $m^*(G)$ to denote the value $m^*(\Gamma(G)_{\mathsf{Qual}}, \Gamma(G)_{\mathsf{Forb}})$ in this section.

Example 7.1 Consider the "prism" graph G_6 on six vertices, depicted in Figure 2., having edges 12, 13, 23, 14, 25, 36, 45, 46, and 56.

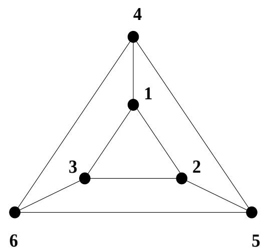


Figure 2: The graph G_6

Define S^0 and S^1 as follows:

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

Then it is straightforward to verify that S^0 and S^1 are basis matrices of a VCS for the strong access structure $\Gamma(G_6)$. Hence, $m^*(G_6) \leq 3$. $\triangle$

In the case where $G = K_n$ (a complete graph), we are talking about $(2, n)$-threshold VCS. By Theorem 6.6 and Corollary 6.7, a $(\Gamma(K_n), m)$-VCS implies the existence of a Sperner family of size n over a ground set of size m, and hence $n \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$. A converse result is also true, as we now show.

Theorem 7.2 *Suppose that the sets $B_1, \ldots, B_n$ form a Sperner family in a ground set $G = \{g_1, \ldots, g_m\}$ of cardinality m. Then $m^*(K_n) \leq m$.*

Proof. We define basis matrices for a VCS with strong access structure $\Gamma(K_n)$. For $1 \leq i \leq n$ and $1 \leq j \leq m$, define

$$S^0(i,j) = \begin{cases} 1 & \text{if } 1 \leq j \leq |B_i| \\ 0 & \text{if } |B_i| + 1 \leq j \leq m. \end{cases}$$

Also, for $1 \leq i \leq n$ and $1 \leq j \leq m$, define

$$S^1(i,j) = \begin{cases} 1 & \text{if } g_j \in B_i \\ 0 & \text{if } g_j \notin B_i. \end{cases}$$

It is easy to see that we obtain the desired VCS by this construction. $\square$

Next theorem holds.

Theorem 7.3 *The value $m^*(K_n)$ is the smallest integer m such that $n \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$.*

Thus $m^*(K_2) = 2$; $m^*(K_3) = 3$; $m^*(K_n) = 4$ for $n = 4, 5, 6$; $m^*(K_n) = 5$ for $n = 7, 8, 9, 10$; etc.

Theorem 7.3 proves a lower bound on the value of $m^*(K_n)$ which is met with equality when the VCS for Γ is constructed from a Sperner family in a ground set of m elements. In such a scheme we have $\alpha(m) = 1/m$. In [2] the authors propose k out of n visual cryptography schemes achieving a greater relative difference. In the case of 2 out of n visual cryptography schemes the scheme given in [2] achieves the best possible value for the relative difference.

Let $\omega(G)$ denote the maximum size of a clique in a graph G. The following result is an immediate consequence of Lemma 3.4 and Corollary 6.7.

Theorem 7.4 *Let G be a graph. Then there exists a $(\Gamma(G), m)$-VCS only if $\omega(G) \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$.*

Recall the graph G_6 considered in Example 7.1. It is easy to see that $\omega(G_6) = 3$, and thus it follows that $m^*(G_6) = 3$.

A modification of Theorem 7.3, using the well-known "splitting technique" from secret sharing schemes [6], together with Theorem 7.4, can be used to prove the following result for complete multipartite graphs.

Theorem 7.5 *There exists a $(K_{a_1,\ldots,a_n}, m)$-VCS if and only if $n \le \binom{m}{\lfloor \frac{m}{2} \rfloor}$.*

Proof. Let S^0 and S^1 be the basis matrices for a $(\Gamma(K_n), m)$-VCS, where $n \le \binom{m}{\lfloor \frac{m}{2} \rfloor}$. Then for every q, $1 \le q \le n$, replicate row q of S^0 and S^1 a_q times. The result is a $(\Gamma(K_{a_1,\ldots,a_n}), m)$-VCS.

Conversely, suppose that a $(\Gamma(K_{a_1,\ldots,a_n}), m)$-VCS exists. It is easy to see that $\omega(K_{a_1,\ldots,a_n}) = n$. Therefore it follows from Theorem 7.4 that $n \le \binom{m}{\lfloor \frac{m}{2} \rfloor}$. □

For a graph G, let $\beta(G)$ denote the minimum cardinality of a vertex cover of G. Given a graph G on vertex set $\mathcal{P}$, for any $x \in \mathcal{P}$, define

$$Inc(x) = \{y \in \mathcal{P} : xy \in E(G)\}.$$

$Inc(x)$ represents the set of all vertices adjacent to x. For any participant $x \in \mathcal{P}$, let $G_x = (V_x, E_x)$ be the subgraph of G where

$$V_x = \{x\} \cup Inc(x)$$

and

$$E_x = \{xy \in E(G)\}.$$

We will refer to G_x as the *star graph* with centre x.

Exploiting the construction used in Theorem 4.4 we can prove the following theorem.

Theorem 7.6 *For any graph G, we have that $m^*(G) \le 2\beta(G)$.*

Proof. Let $X \subseteq \mathcal{P}$ be a vertex cover of G having cardinality $\beta(G)$. For each $x \in X$, there exists a $(\Gamma(G_x), 2)$-VCS by Theorem 7.5.

Note that $\cup_{x \in X} E_x = E(G)$, where $E_x \subseteq E(G)$ for all $x \in X$. Hence, if we apply Corollary 4.5, we obtain a $(\Gamma(G), 2\beta(G))$-VCS. □

If G is bipartite, with bipartition (V_1, V_2), we get the following corollary.

Corollary 7.7 *Suppose G is a bipartite graph having bipartition (V_1, V_2). Then $m^*(G) \le 2 \times \min\{|V_1|, |V_2|\}$.*

Proof. V_1 and V_2 are both vertex covers of G, so $\beta(G) \le \min\{|V_1|, |V_2|\}$. Apply Theorem 7.6. □

8 A Decomposition Construction to Achieve Higher Contrast

Given an access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$, consider a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS having contrast one, that is constructed using basis matrices S^0 and S^1. To construct a VCS for $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ having higher contrast $c > 1$, we could simply concatenate c copies of S^0 and S^1 to get a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m \cdot c)$-VCS with contrast c. In this section we describe a general technique to construct VCS having any higher contrast, which provides better schemes with respect to the value of m. This technique was introduced by Stinson [14] in the context of secret sharing schemes and it is referred to as a (γ, λ)-decomposition.

For the rest of this section, we confine our attention to strong access structures. Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be a strong access structure having basis Γ_0 and let $\lambda, \gamma \geq 1$ be integers. A (γ, λ)-*decomposition* of Γ_0 consists of a collection $\{\Gamma^1, \ldots, \Gamma^\gamma\}$ such that the following properties are satisfied:

1. $\Gamma^q \subseteq \Gamma_0$ for $1 \leq q \leq \gamma$
2. $\lambda\Gamma_0 \subseteq \cup_{q=1}^{\gamma} \Gamma^q$ (i.e., the multiset union of the Γ^q's contains every basis subset at least λ times).

The following theorem holds.

Theorem 8.1 *Let Γ_0 be the basis of a strong access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$. Let $\{\Gamma^1, \ldots, \Gamma^\gamma\}$ be a (γ, λ)-decomposition of Γ_0. For $1 \leq i \leq \gamma$, let $(\Gamma^i_{\mathsf{Qual}}, \Gamma^i_{\mathsf{Forb}})$ be the access structure having basis Γ^i. Suppose, for $i = 1, \ldots, \gamma$, that there is a $(\Gamma^i_{\mathsf{Qual}}, \Gamma^i_{\mathsf{Forb}}, m_i)$-VCS constructed using basis matrices. Then there is a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS, constructed from basis matrices, having contrast at least λ, where $m = \sum_{i=1}^{\gamma} m_i$.*

Proof. The construction used in the proof of this theorem is similar to the one employed in Theorem 4.4. For $i = 1, \ldots, \gamma$, let $S^{0,i}$ and $S^{1,i}$ be the basis matrices of a VCS for the access structure $(\Gamma^i_{\mathsf{Qual}}, \Gamma^i_{\mathsf{Forb}})$. From $S^{0,i}$ and $S^{1,i}$ we construct a pair of matrices, $(\widehat{S}^{0,i}, \widehat{S}^{1,i})$, consisting of n rows. Let us show how to construct $\widehat{S}^{0,i}$. For $j = 1, \ldots, n$, the j-th row of $\widehat{S}^{0,i}$ has all zeroes as entries if the participant j is not an essential participant of $(\Gamma^i_{\mathsf{Qual}}, \Gamma^i_{\mathsf{Forb}})$; otherwise, it is the row of $S^{0,i}$ corresponding to participant j. The matrix $\widehat{S}^{1,i}$ is constructed similarly. Finally, the matrices S^0 and S^1 for $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ will be realized by concatenating the matrices $\widehat{S}^{0,1}, \ldots, \widehat{S}^{0,\gamma}$ and the matrices $\widehat{S}^{1,1}, \ldots, \widehat{S}^{1,\gamma}$, respectively (i.e., $S^0 = \widehat{S}^{0,1} \circ \cdots \circ \widehat{S}^{0,\gamma}$ and $S^1 = \widehat{S}^{1,1} \circ \cdots \circ \widehat{S}^{1,\gamma}$).
Let $m = \sum_{i=1}^{\gamma} m_i$. For $i = 1, \ldots, \gamma$, let $\{(X, t^i_X)\}_{X \in \Gamma^i_0}$ be the set of thresholds satisfying Definition 2.1 for the access structure $(\Gamma^i_{\mathsf{Qual}}, \Gamma^i_{\mathsf{Forb}})$, and let $\alpha_i(m_i)$ be the relative difference of this VCS. Define $\alpha(m)$ to be

$$\alpha(m) = \frac{\lambda}{m} \cdot \min_{1 \leq i \leq \gamma} \{\alpha_i(m_i) \cdot m_i\}. \tag{2}$$

We have to show that the matrices S^0 and S^1, constructed using the previously described technique, are basis matrices of a VCS for the access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$, having contrast at least λ.

Let $X \in \Gamma_0$ be a set of participants. Let $Y \subseteq \{1, \ldots, \gamma\}$ be the set of maximum cardinality such that $X \in \cap_{i \in Y} \Gamma_0^i$. Since $\{\Gamma^1, \ldots, \Gamma^\gamma\}$ is a (γ, λ)-decomposition of Γ_0, we have that $|Y| \geq \lambda$. Let $W = \{1, \ldots, \gamma\} \setminus Y$ and define

$$t_X = \sum_{i \in Y} t_X^i + \sum_{i \in W} w(S_X^{0,i}).$$

It results that

$$\begin{aligned}
w(S_X^0) &= w(\widehat{S}_X^{0,1} \circ \cdots \circ \widehat{S}_X^{0,\gamma}) \\
&= \sum_{i \in Y} w(\widehat{S}_X^{0,i}) + \sum_{i \in W} w(\widehat{S}_X^{0,i}) \\
&= \sum_{i \in Y} w(S_X^{0,i}) + \sum_{i \in W} w(S_X^{0,i}) \\
&\leq \sum_{i \in Y} (t_X^i - \alpha_i(m_i) \cdot m_i) + \sum_{i \in W} w(S_X^{0,i}) \\
&\leq \sum_{i \in Y} t_X^i - \lambda \cdot \min_{i \in Y} \{\alpha_i(m_i) \cdot m_i\} + \sum_{i \in W} w(S_X^{0,i}) \\
&\leq t_X - \alpha(m) \cdot m.
\end{aligned}$$

Whereas,

$$\begin{aligned}
w(S_X^1) &= w(\widehat{S}_X^{1,1} \circ \cdots \circ \widehat{S}_X^{1,\gamma}) \\
&= \sum_{i \in Y} w(\widehat{S}_X^{1,i}) + \sum_{i \in W} w(\widehat{S}_X^{1,i}) \\
&= \sum_{i \in Y} w(S_X^{1,i}) + \sum_{i \in W} w(S_X^{1,i}) \\
&\geq \sum_{i \in Y} t_X^i + \sum_{i \in W} w(S_X^{0,i}) \\
&= t_X.
\end{aligned}$$

Hence, Property 1. of Definition 2.2 is satisfied.
Now, suppose that $X \notin \cup_{i=1}^{\gamma} \Gamma^i$. We have to show that $S^0[X] = S^1[X]$ up to a column permutation. For $i = 1, \ldots, \gamma$, up to a column permutation, we have that $\widehat{S}^{0,i}[X] = \widehat{S}^{1,i}[X]$. Hence, it results that

$$S^0[X] = \widehat{S}^{0,1}[X] \circ \cdots \circ \widehat{S}^{0,\gamma}[X] = \widehat{S}^{1,1}[X] \circ \cdots \circ \widehat{S}^{1,\gamma}[X] = S^1[X],$$

where the second equality is satisfied up to a column permutation. Hence, Property 2. of Definition 2.2 is satisfied, too. From (2) it follows that the resulting scheme has contrast $\alpha(m) \cdot m$ at least λ. □

Let G be a graph on vertex set $\mathcal{P}$ of cardinality n, and define the access structure $\Gamma(G)$ as in Section 7. Recall also from Section 7 that G_x is defined to be the star graph with centre x, for $x \in \mathcal{P}$. It is not difficult to see that $\{G_x : x \in \mathcal{P}\}$ is an $(n, 2)$-decomposition of G. Applying Theorem 8.1, we obtain a visual cryptography scheme for $\Gamma(G)$ having contrast 2, with $m = 2n$ and $\alpha(m) = \frac{1}{n}$. The next theorem holds.

Theorem 8.2 *Let G be a graph on a set of n vertices. Then there exists a $(\Gamma(G), 2n)$-VCS with contrast equal to 2.*

The previous theorem gives a $(\Gamma(G), 2n)$-VCS with contrast 2. Using two copies of the VCS constructed in Theorem 7.6 we would get a $(\Gamma(G), 4\beta(G))$-VCS with contrast 2, where $\beta(G)$ is the size of the minimum vertex cover of G. Therefore, for $\beta(G) > n/2$ the $(n, 2)$-decomposition provides a VCS with shorter shares.

Example 8.3 To demonstrate the techniques presented in Theorems 4.4 and 8.1, consider the access structure $\Gamma(C_n)$, where C_n is a cycle on n vertices, and $n \geq 5$. From Theorem 7.6, there is a $(\Gamma(C_n), 2\lceil n/2 \rceil)$-VCS with contrast one. Two copies of this scheme produce a $(\Gamma(C_n), 4\lceil n/2 \rceil)$-VCS with contrast two.

On the other hand, from Theorem 8.2 there exists a $(\Gamma(C_n), 2n)$-VCS with contrast two. Therefore, for odd values of $n \geq 5$, the decomposition construction produces a VCS with contrast two with shorter length of shares.

$\triangle$

9 VCS for Strong Access Structures on at Most Four Participants

In this section we give upper and lower bounds on the minimum value $m^*(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ for all strong access structures on at most four participants. We consider only connected access structures without isolated participants. The bounds on m^* are summarized in Table 1.

The results are obtained as follows:

- Access structures $1, 2, 3, 6, 7, 9$, and 10 represent complete multipartite graphs and the optimal value of m^* is determined by Theorem 7.5.
- The optimal value of m^* for access structures 4 and 18 is determined by Lemma 3.1 and Theorem 3.3.
- Since access structure 8 is an induced subgraph of the graph G_6, The upper bound $m^* \leq 3$ can be obtained from Example 7.1 by applying Lemma 3.4.
- For the all the remaining access structures the upper bounds on m^* are obtained using the basis matrices given in Table 2. For all the above schemes, we have $\alpha(m) \cdot m = 1$.
- The lower bound $m^* \geq 3$ for the access structures 5 and 8 is determined by Lemma 5.12.
- The lower bound $m^* \geq 4$ for the access structures $11, 13$, and 14 comes from Corollary 3.5.
- The lower bound $m^* \geq 5$ for the access structure 12 comes from Theorem 9.2 (see below).
- The lower bound $m^* \geq 5$ for the access structures $15, 16$, and 17 comes from Theorem 9.1 (see below).

Theorem 9.1 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be a strong access structure on participant set $\mathcal{P} = \{1, 2, 3, 4\}$ such that $\{1, 2, 4\}, \{1, 3, 4\} \in \Gamma_0$. If there exists a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, 4)$-VCS, then there is no $X \in \Gamma_0$ such that $\{2, 3\} \subseteq X$.*

Proof. From Lemma 3.4 any $(\Gamma_{\textsf{Qual}}, \Gamma_{\textsf{Forb}}, 4)$-VCS contains (induced) a VCS for the strong access structures Γ' and Γ'' having basis $\Gamma'_0 = \{\{1,2,4\}\}$ and $\Gamma''_0 = \{\{1,3,4\}\}$, respectively. Therefore, from Theorem 5.13 any matrix $M \in \mathcal{C}_1$ and any matrix $M' \in \mathcal{C}_0$ are equal, up to a column permutation, respectively, to

$$M = \begin{bmatrix} 1001 \\ 0101 \\ 0101 \\ 0011 \end{bmatrix} \qquad M' = \begin{bmatrix} 0110 \\ 0101 \\ 0101 \\ 0011 \end{bmatrix}.$$

If this is the case, then, for any $M \in \mathcal{C}_1$ the matrix $M[23]$ does not contain the columns $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Because of the unavoidable patterns, there is no $X \in \Gamma_0$ such that $\{2,3\} \subseteq X$. Thus, the theorem holds. $\square$

access structure	n	basis subsets	m^*
1	2	12	$m^* = 2$
2	3	$12, 23$	$m^* = 2$
3	3	$12, 13, 23$	$m^* = 3$
4	3	123	$m^* = 4$
5	4	$12, 23, 34$	$m^* = 3$
6	4	$12, 13, 14$	$m^* = 2$
7	4	$12, 14, 23, 34$	$m^* = 2$
8	4	$12, 23, 24, 34$	$m^* = 3$
9	4	$12, 13, 14, 23, 24$	$m^* = 3$
10	4	$12, 13, 14, 23, 24, 34$	$m^* = 4$
11	4	$123, 14$	$m^* = 4$
12	4	$123, 14, 34$	$m^* = 5$
13	4	$134, 122, 23, 24$	$m^* = 4$
14	4	$123, 124$	$m^* = 4$
15	4	$124, 134, 23$	$m^* = 5$
16	4	$123, 124, 134$	$5 \leq m^* \leq 6$
17	4	$123, 124, 134, 234$	$5 \leq m^* \leq 6$
18	4	1234	$m^* = 8$

Table 1: VCS for strong access structures on at most four participants.

The next theorem proves that for the strong access structure 12, a VCS with $m = 4$ does not exist.

Theorem 9.2 *Let* $(\Gamma_{\textsf{Qual}}, \Gamma_{\textsf{Forb}})$ *be the strong access structure on participant set* $\mathcal{P} = \{1,2,3,4\}$ *having basis* $\Gamma_0 = \{123, 14, 34\}$. *Then there is no* $(\Gamma_{\textsf{Qual}}, \Gamma_{\textsf{Forb}}, 4)$*-VCS.*

Proof. Suppose by contradiction that there exists a $(\Gamma_{\textsf{Qual}}, \Gamma_{\textsf{Forb}}, 4)$-VCS. From Lemma 3.4 and Theorem 5.13 any matrix $M \in \mathcal{C}_1$ and any matrix $M' \in \mathcal{C}_0$ are equal, up to a column permutation, respectively, to

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ \star & \star & \star & \star \end{bmatrix} \qquad M' = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & \star & \star & \star \end{bmatrix},$$

where $\star$ denotes the presence of either a one or a zero. Notice that for any matrix $M' \in \mathcal{C}_0$ it holds that $w(M'_{124}) = w(M'_{234}) = 3$. Since the scheme is for the strong access structure having basis Γ_0, for any matrix $M \in \mathcal{C}_1$, we must have $w(M_{124}) = w(M_{234}) = 4$. Hence, any matrix $M \in \mathcal{C}_1$ is equal, up to a column permutation to

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & \star & 1 & \star \end{bmatrix}.$$

For any matrix $M \in \mathcal{C}_1$ we have that $w(M_{24}) = 4$. Since $24 \in \Gamma_{\mathsf{Forb}}$ is has to be $w(M'_{24}) = 4$ for at least one matrix $M' \in \mathcal{C}_0$. This is a contradiction since for any $M' \in \mathcal{C}_0$ it holds that $w(M'_{24}) \leq 3$. Therefore, the theorem holds. $\square$

10 Conclusion

In this paper we have analyzed visual cryptography schemes. We have extended the Naor and Shamir's model to general access structures and we have proposed two techniques to construct visual cryptography schemes for general access structures. We proved lower bounds on the size of the shares distributed to the participants in the scheme. We provided a novel technique to realize k out of n threshold visual cryptography schemes. Our construction for k out of n visual cryptography schemes is better with respect to pixel expansion than the one proposed in [11] and for the case of 2 out of n is the best possible. Finally, we considered graph-based access structures giving both lower and upper bounds on the size of the shares.

Acknowledgements

We would like to express our gratitude to Ugo Vaccaro for illuminating discussions. Many thanks go to Carmine Di Marino who implemented some of 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, *Constructions and Bounds for Visual Cryptography*, to appear in the proceedings of the "23rd International Colloquium on Automata, Languages and Programming" (ICALP '96), Friedhelm Meyer auf der Heide Ed., "Lecture Notes in Computer Science", Springer–Verlag, Berlin, 1996.

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

[3] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Extended Schemes for Visual Cryptography*, preprint, 1995.

[4] M. Atici, S. S. Magliveras, D. R. Stinson, and W.-D. Wei, *Some Recursive Constructions for Perfect Hash Families*, to appear in Journal of Combinatorial Designs.

[5] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro, *Graph Decomposition and Secret Sharing Schemes*, Journal of Cryptology, Vol. 8, pp. 39-64, 1995.

access structure	S^0	S^1
#5	$\begin{bmatrix} 100 \\ 110 \\ 110 \\ 010 \end{bmatrix}$	$\begin{bmatrix} 100 \\ 011 \\ 110 \\ 001 \end{bmatrix}$
#11	$\begin{bmatrix} 0011 \\ 0101 \\ 0110 \\ 0011 \end{bmatrix}$	$\begin{bmatrix} 0011 \\ 0101 \\ 1001 \\ 1100 \end{bmatrix}$
#12	$\begin{bmatrix} 01100 \\ 11000 \\ 10100 \\ 00100 \end{bmatrix}$	$\begin{bmatrix} 10001 \\ 11000 \\ 10100 \\ 00010 \end{bmatrix}$
#13	$\begin{bmatrix} 0011 \\ 0111 \\ 0101 \\ 0110 \end{bmatrix}$	$\begin{bmatrix} 0011 \\ 1110 \\ 0101 \\ 1001 \end{bmatrix}$
#14	$\begin{bmatrix} 0011 \\ 0101 \\ 0110 \\ 0110 \end{bmatrix}$	$\begin{bmatrix} 0011 \\ 0101 \\ 1001 \\ 1001 \end{bmatrix}$
#15	$\begin{bmatrix} 01100 \\ 10100 \\ 10100 \\ 11000 \end{bmatrix}$	$\begin{bmatrix} 10001 \\ 10010 \\ 10100 \\ 11000 \end{bmatrix}$
#16	$\begin{bmatrix} 000111 \\ 110101 \\ 110011 \\ 110110 \end{bmatrix}$	$\begin{bmatrix} 111000 \\ 110101 \\ 110011 \\ 110110 \end{bmatrix}$
#17	$\begin{bmatrix} 000111 \\ 001011 \\ 001101 \\ 001110 \end{bmatrix}$	$\begin{bmatrix} 111000 \\ 110100 \\ 110010 \\ 110001 \end{bmatrix}$

Table 2: Basis matrices for VCS for strong access structures on at most four participants.

[6] E. F. Brickell and D. R. Stinson, *Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes*, Journal of Cryptology, Vol. 5, pp. 153-166, 1992.

[7] P. Erdös, P. Frankl, and Z. Füredi, *Families of Finite Sets in Which no Set is Covered by the Union of r Others*, Israel Journal of Mathematics, Vol. 51, pp. 79–89, 1985.

[8] M. L. Fredman and J. Komlós, *On the Size of Separating System and Families of Perfect Hash Functions*, SIAM J. Alg. Disc. Meth., Vol 5, N. 1, March 1984.

[9] J. H. van Lint and R. M. Wilson, A Course in Combinatorics, Cambridge University Press, 1992.

[10] K. Mehlhorn, *On the Program Size of Perfect and Universal Hash Functions*, in Proceedings of 23rd Annual IEEE Symposium on Foundation of Computer Science, pp. 170–175, 1982.

[11] 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.

[12] P. Elias, *Zero Error Capacity Under List Decoding*, IEEE Trans. Inform. Theory, Vol. 34, N. 5, pp. 1070–1074, 1988.

[13] G. J. Simmons, W. Jackson, and K. Martin, *The Geometry of Shared Secret Schemes,* Bulletin of the ICA, Vol. 1, pp. 71–88, 1991.

[14] D. R. Stinson, *Decomposition Constructions for Secret Sharing Schemes*, IEEE Trans. Inform. Theory, Vol. 40, N. 1, pp. 118–125, 1994.

Appendix

Example of a Visual Cryptography Scheme

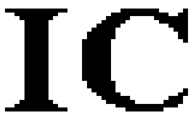
In this appendix an example of the secret image, the shares corresponding to single participants, and few groups of participants are depicted. The family of qualified sets is

$$\Gamma_{\mathsf{Qual}} = \{\{1,2\},\{2,3\},\{3,4\},\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\},\{1,2,3,4\}\}.$$

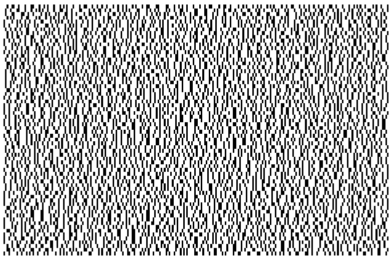
All remaining subsets of participants are forbidden.

The visual cryptography scheme used for this example is described in Table 2 of Section 9.

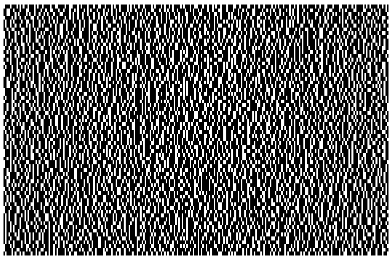
Secret Image



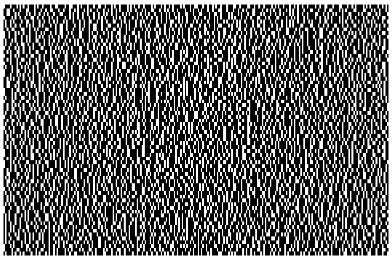
Share of participant 1



Share of participant 2



Share of participant 3



Share of participant 4

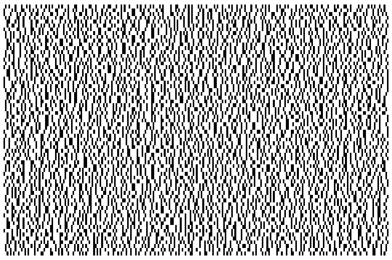


Image of participants 1 and 2

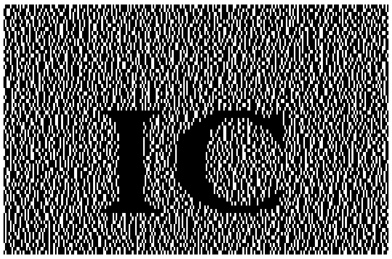


Image of participants 2 and 3

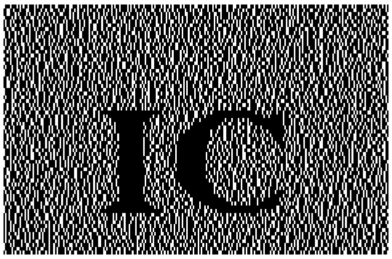


Image of participants 3 and 4

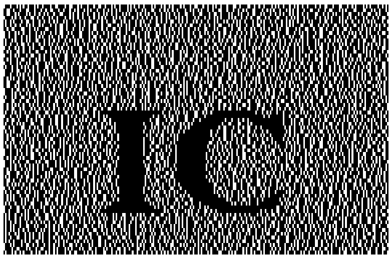


Image of participants 1 and 3