On the Contrast in Visual Cryptography Schemes

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

[1] 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/}

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

September 27, 1996

Abstract

A visual cryptography scheme is a method to encode a secret image SI into shadow images called shares such that certain qualified subsets of shares enable the "visual" recovery of the secret image. The "visual" recovery consists of xeroxing the shares onto transparencies, and then stacking them. The shares of a qualified set will reveal the secret image without any cryptographic computation.
In this paper we analyze the contrast of the reconstructed image in k out of n visual cryptography schemes. (In such a scheme any k shares will reveal the image, but no set of $k-1$ shares gives any information about the image.) In the case of 2 out of n threshold schemes we give a complete characterization of schemes having optimal contrast and minimum pixel expansion in terms of certain balanced incomplete block designs. In the case of k out of n threshold schemes with $k \geq 3$ we obtain upper and lower bounds on the optimal contrast.

1 Introduction

A visual cryptography scheme for a set $\mathcal{P}$ of n participants is a method to encode a secret image SI into n shadow images called shares, where each participant in $\mathcal{P}$ receives one share. Certain qualified subsets of participants can "visually" recover the secret image, but other, forbidden, sets of participants have no information (in an information-theoretic sense) on SI. A "visual" recovery for a set $X \subseteq \mathcal{P}$ consists of xeroxing the shares given to the participants in X onto transparencies, and then stacking them. The participants in a qualified set X will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation.

This cryptographic paradigm was introduced by Naor and Shamir [12]. They analyzed the case of a k out of n threshold visual cryptography schemes, in which the secret image is visible if and only if any k transparencies are stacked together. Further results on k out of n threshold visual cryptography schemes can be found in [1, 2, 8].

The model by Naor and Shamir has been extended in [1, 2] to general access structures (an access structure is a specification of all qualified and forbidden subsets of participants), where general techniques to construct visual cryptography schemes for any access structure have been proposed.

Some other generalizations of the basic model have been considered:

- In implementing visual cryptography schemes it might be useful to conceal the existence of the secret message, namely, the shares given to participants in the scheme should not look like a random bunch of pixels, but they should be innocent looking images (a house, a dog, a tree, ...). This can be thought of as a form of information hiding or steganography and it is referred to as an *extended* visual cryptography scheme. Naor and Shamir [12] first considered this method of concealing the existence of the secret message for the case of 2 out of 2 threshold VCS. In [3] an efficient solution of the problem for general access structures was given.

- Droste [8] considered the problem of sharing more than one secret image among a set of participants. For example, in the appendix of [8], a 2 out of 3 threshold visual cryptography scheme is presented in which each pair of transparencies reveals a different secret image. A construction is given to obtain visual cryptography schemes in which different subsets of transparencies reveal different secret images. This construction also provides a method of obtaining extended visual cryptography schemes; however, it is not as efficient as the method in [3].

- In [13] an alternative reconstruction method for visual cryptography schemes is studied. This method yields a higher contrast in the reconstructed image for 2 out of n threshold schemes, but the technique is not applicable to k out of n threshold schemes with $k \geq 3$.

- Visual cryptography schemes to encrypt coloured images are given in [11, 14, 15].

In this paper we analyze the contrast of the reconstructed image for k out of n visual cryptography schemes. (This contrast is measured by the *relative difference* of the scheme, defined in the next section.) In the case of 2 out of n threshold schemes we obtain an exact formula for the optimal relative difference. We also show how to realize this optimal relative difference with the minimum possible pixel expansion. (A scheme has *pixel expansion m* if each pixel of the original image is encoded as m subpixels on each transparency.) In fact, we give a complete characterization of the optimal schemes in terms of certain balanced incomplete block designs.

In the case of k out of n threshold schemes with $k \geq 3$, we obtain upper and lower bounds on the optimal relative difference. The lower bounds are derived from explicit constructions. The upper bounds are obtained from a structural result which relates the relative difference of a k out of n threshold scheme to the relative difference of a $k-1$ out of $n-1$ threshold scheme. This structural result also gives lower bounds on the pixel expansion of k out of n threshold schemes. Finally, we give necessary and sufficient conditions for pair of $n \times m$

matrices to be the basis matrices of a k out of n threshold visual cryptography scheme with pixel expansion m. (Basis matrices are the most important method of constructing visual cryptography schemes; see Section 2.1 for the definition.)

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:

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

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

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

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

and we say that Γ_{Qual} is the *closure* of Γ_0. On the other hand, if $\Gamma_0 = \Gamma_{\mathsf{Qual}}$, then the access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is said to be *weak*.

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 secret image 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 according to 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 values $\alpha(m)$ and $\{t_X\}_{X \in \Gamma_{\mathsf{Qual}}}$ satisfying:*

1. Any (qualified) set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Qual}}$ can recover the shared image by stacking their transparencies.
   Formally, for any $M \in \mathcal{C}_0$, the "or" V of rows $i_1, i_2, \ldots, i_p$ satisfies $w(V) \leq t_X - \alpha(m) \cdot m$; whereas, for any $M \in \mathcal{C}_1$ it results that $w(V) \geq t_X$.

2. Any (forbidden) set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Forb}}$ has no information on the shared image.
   Formally, the two collections of $p \times m$ matrices $\mathcal{D}_t$, with $t \in \{0, 1\}$, obtained by restricting each $n \times m$ matrix in $\mathcal{C}_t$ to rows $i_1, i_2, \ldots, i_p$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Each pixel of the original image will be encoded into n pixels, each of which consists of m subpixels. To share a white (black, resp.) pixel, the dealer randomly chooses one of the matrices in $\mathcal{C}_0$ ($\mathcal{C}_1$, resp.), and distributes row i to participant i. Thus, the chosen matrix defines the m subpixels in each of the n transparencies. Notice that in the previous definition $\mathcal{C}_0$ 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 image shared by the dealer. The value $\alpha(m)$ is called *relative difference*, the number $\alpha(m) \cdot m$ is referred to as the *contrast* of the image, and the set $\{t_X\}_{X \in \Gamma_0}$ is called the *set of thresholds*. We want the contrast to be as large as possible and at least one, that is, $\alpha(m) \geq 1/m$. The second property is called *security*, since it implies that, even by inspecting all their shares, a forbidden set of participants cannot gain any information in deciding whether the shared pixel was white or black.

Suppose $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is a strong access structure and suppose $\mathcal{C}_0$ and $\mathcal{C}_1$ are the collections of matrices in a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS with relative difference $\alpha(m)$. Then we can also view $\mathcal{C}_0$ and $\mathcal{C}_1$ as a visual cryptography scheme for the related weak access structure $(\Gamma_0, \Gamma_{\mathsf{Forb}})$. More precisely, $\mathcal{C}_0$ and $\mathcal{C}_1$ comprise a $(\Gamma_0, \Gamma_{\mathsf{Forb}}, m)$-VCS with relative difference at least $\alpha(m)$.

There are few differences between the model of visual cryptography we propose and the one presented by Naor and Shamir [12]. Our model is a generalization of the one proposed in [12], 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 so this is to take $(\Gamma'_{\mathsf{Qual}}, \Gamma'_{\mathsf{Forb}})$ to be the strong access structure having as basis Γ_0, where Γ_0 consists of the minimal sets in Γ_{Qual}, as usual.

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

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.

2.1 Basis Matrices

All 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 $\{t_X\}_{X \in \Gamma_{\mathsf{Qual}}}$ is realized using the $n \times m$* basis matrices *S^0 and S^1 if the following two conditions hold.*

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

The collections $\mathcal{C}_0$ and $\mathcal{C}_1$ are obtained by permuting the columns of the corresponding basis matrix (S^0 for $\mathcal{C}_0$, and S^1 for $\mathcal{C}_1$) in all possible ways. Note that, in this case, the size of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ is the same and it is denoted by r. This technique was first introduced in [12]. 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.)).

3 Threshold Schemes

A (k, n)-threshold structure is any access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ in which

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

and

$$\Gamma_{\mathsf{Forb}} = \{B \subseteq \mathcal{P} : |B| \le k - 1\}.$$

In any (k, n)-threshold VCS the image 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 analyzed by any other method. In a strong (k,n)-threshold VCS the image remains visible if more than k participants stack their transparencies.

Naor and Shamir showed (see Theorem 5.3 in [12]) that there exist (k,n)-threshold visual cryptography schemes with $m = 2^{O(k \log k)} \cdot \log n$ and $\alpha(m) = 2^{-\Omega(k)}$. The construction presented in [1] (see Theorem 6.2) yields schemes with $m = O(k(2e)^k \log n)$. The value of m is less than the one in the Naor and Shamir construction, but this was achieved by relaxing the condition that all values t_X are equal.

Droste [8] gave an algorithm to construct basis matrices for (k,n)-threshold visual cryptography schemes. It can be shown that this algorithm always constructs schemes with $\alpha(m) = 1/m$ and $m \geq n$. For small values of k and n, the schemes obtained are quite efficient. However, for n large with respect to k, the value of m is much larger than in the schemes obtained in [1, 12].

In this paper we will present a technique to realize (k,n)-threshold visual cryptography scheme achieving a bigger value of the relative difference when $k < n$. In the case of $(2,n)$-threshold visual cryptography schemes, we obtain the best possible value for the relative difference (see Theorem 4.2).

The construction of a (k,k)-threshold VCS is obtained (see [12]) by means of the construction of the basis matrices T_k^0 and T_k^1 defined as follows: T_k^0 is the matrix whose columns are all the boolean k-vectors having an even number of '1's, and T_k^1 is the matrix whose columns are all the boolean k-vectors having an odd number of '1's. In such a scheme we have that the pixel expansion m is equal to 2^{k-1}. In [12] it was proved that the (k,k)-threshold VCS obtained from this construction is uniform, that is, for every $1 \leq p \leq k-1$ the "or" of any p rows of T_k^0 and T_k^1 has weight $f(p)$ for some function f.

The next lemma was proved in [1]; we repeat its proof here for the reader's convenience.

Lemma 3.1 *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. $\square$

One immediate consequence of this lemma is the existence, in the matrices belonging to $\mathcal{C}_1$, of some predefined patterns referred to as *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 can be seen by applying Lemma 3.1 with $X = Y \cup \{i\}$. In fact, 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.

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 3.2 *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 $\mathcal{P}'$. If there exists a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS, then there exists a $(\Gamma[\mathcal{P}']_{\mathsf{Qual}}, \Gamma[\mathcal{P}']_{\mathsf{Forb}}, m)$-VCS.*

4 $(2, n)$-threshold VCSs with Optimal Contrast

In this section we describe $(2, n)$-threshold visual cryptography schemes achieving a greater relative difference than the ones presented in [1, 2, 8, 12]. The $n \times m$ basis matrix S^1 is realized by considering all the binary n-vectors of weight $\lfloor n/2 \rfloor$. Hence, $m = \binom{n}{\lfloor n/2 \rfloor}$ and any row in S^1 has weight equal to $\binom{n-1}{\lfloor n/2 \rfloor - 1}$. The $n \times m$ basis matrix S^0 is realized by considering n equal rows of weight $\binom{n-1}{\lfloor n/2 \rfloor - 1}$. Clearly, Property 2. of Definition 2.2 is satisfied. We have to prove that these basis matrices satisfy Property 1. of Definition 2.2, too. Consider any $q \geq 2$ distinct indices, say $i_1, \ldots, i_q$, and let $X = \{i_1, \ldots, i_q\}$. We now compute the difference $w(S^1_X) - w(S^0_X)$. It is easy to see that for any $q \geq 2$ it results that $w(S^0_X) = \binom{n-1}{\lfloor n/2 \rfloor - 1}$. Moreover, for $q > n - \lfloor n/2 \rfloor = \lceil n/2 \rceil$, we have that $w(S^1_X) = m$. For $2 \leq q \leq \lceil n/2 \rceil$, it is immediate to see that $w(S^1_X)$ is equal to m minus the number of columns having as entries all zeroes in the rows indexed by $i_1, \ldots, i_q$. Hence one can compute

$$w(S^1_X) = \binom{n}{\lfloor n/2 \rfloor} - \binom{n-q}{\lfloor n/2 \rfloor}.$$

Since, for any $1 \leq k \leq n$, it holds that

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k},$$

we obtain that

$$w(S^1_X) - w(S^0_X) = \begin{cases} \binom{n-1}{\lfloor n/2 \rfloor} - \binom{n-q}{\lfloor n/2 \rfloor} & \text{if } 2 \leq q \leq \lceil n/2 \rceil \\ \\ \binom{n-1}{\lfloor n/2 \rfloor} & \text{if } \lceil n/2 \rceil < q \leq n. \end{cases}$$

The above quantity $w(S^1_X) - w(S^0_X)$ does not depend on the actual set X but only on its size. Let $\beta(q) = w(S^1_X) - w(S^0_X)$. The quantity $\beta(q)$ is not decreasing and reaches its minimum at $q = 2$. Define $\alpha(m) = \beta(2)/m$. Hence

$$\alpha(m) \cdot m = \binom{n}{\lfloor n/2 \rfloor} - \binom{n-2}{\lfloor n/2 \rfloor} - \binom{n-1}{\lfloor n/2 \rfloor - 1} = \binom{n-2}{\lfloor n/2 \rfloor - 1}.$$

Since $m = \binom{n}{\lfloor n/2 \rfloor}$, we get that

$$\alpha(m) = \frac{\binom{n-2}{\lfloor n/2 \rfloor - 1}}{\binom{n}{\lfloor n/2 \rfloor}} = \frac{\lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil}{n(n-1)}. \tag{1}$$

For convenience we define $\alpha^*(n) = \frac{\lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil}{n(n-1)}$. Observe that we can express $\alpha^*(n)$ in the following form

$$\alpha^*(n) = \begin{cases} \frac{n}{4n-4} & \text{if } n \text{ is even} \\ \frac{n+1}{4n} & \text{if } n \text{ is odd.} \end{cases}$$

For any set X of at least two participants, if we set $t_X = w(S^1_X)$ and $\alpha(m) = \alpha^*(n)$, then Property 1. of Definition 2.2 is satisfied. Theorem 4.2 proves that the value of $\alpha^*(n)$ is the best possible value for the relative difference of a $(2,n)$-threshold visual cryptography scheme.

From the previous discussion we obtain that by stacking together more than two transparencies of our $(2,n)$-threshold VCS, the image we recover becomes more visible (i.e., the difference between a white and black pixel is larger when we stack together more than two transparencies). When we stack $\lfloor n/2 \rfloor < q \le n$ transparencies we have that

$$\beta(q) = w(S^1_X) - w(S^0_X) = \binom{n}{\lfloor n/2 \rfloor} - \binom{n-1}{\lfloor n/2 \rfloor - 1} = \binom{n-1}{\lfloor n/2 \rfloor}.$$

Since $m = \binom{n}{\lfloor n/2 \rfloor}$, we get that the "relative difference" in this case is equal to

$$\frac{\beta(q)}{m} = 1 - \left\lfloor \frac{n}{2} \right\rfloor \cdot \frac{1}{n} = \begin{cases} \frac{1}{2} & \text{if } n \text{ is even} \\ \frac{1}{2} + \frac{1}{2n} & \text{if } n \text{ is odd.} \end{cases}$$

We summarize the above discussion in the following theorem.

Theorem 4.1 *For any $n \ge 2$, there exists a strong $(2,n)$-threshold visual cryptography scheme with pixel expansion $m = \binom{n}{\lfloor n/2 \rfloor}$ and $\alpha(m) = \alpha^*(n)$.*

In the next theorem, we prove an upper bound on $\alpha(m)$ which shows that the schemes constructed in Theorem 4.1 have optimal relative difference. Note that the bound holds for weak or strong threshold VCS. The proof is essentially the same as the proof of the Plotkin bound from coding theory (see, for example, van Lint [9]).

Theorem 4.2 *Let $n \ge 2$. In any $(2,n)$-threshold visual cryptography scheme with pixel expansion m, it holds that $\alpha(m) \le \alpha^*(n)$.*

Proof. Let $M \in \mathcal{C}_1$. By Lemma 3.1 for any distinct $i, j \in \{1, \ldots, n\}$, the matrix $M[\{i, j\}]$ contains the patterns $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ each appearing at least $\alpha(m) \cdot m$ times. The number of such unavoidable patterns is $2 \cdot \binom{n}{2} \cdot \alpha(m) \cdot m = n(n-1) \cdot \alpha(m) \cdot m$. Clearly, any column of M can "cover" more than one pattern. If a column of M has i entries equal to '1', then it "covers" $i(n-i)$ such patterns. The quantity $i(n-i)$ reaches its maximum for $i = \lfloor n/2 \rfloor$ or $i = \lceil n/2 \rceil$. Therefore, any column in M "covers" at most $\lfloor n/2 \rfloor \lceil n/2 \rceil$ unavoidable patterns. Thus, the number of columns of M has to be at least

$$m \geq \frac{n(n-1) \cdot \alpha(m) \cdot m}{\lfloor n/2 \rfloor \lceil n/2 \rceil}, \tag{2}$$

which proves the theorem. □

Now we analyze the structure of $(2, n)$-threshold VCS with optimal relative difference $\alpha(m)$, that is, schemes for which $\alpha(m) = \alpha^*(n)$. Before we proceed, we need the following definitions from coding theory. An (n, M, d) *code* is a set of M binary n-tuples (called *codewords*) with the property that the Hamming distance between any two codewords is at least d. The integer n is the *length* of the code, M is its *size* and d is its *distance*. A code is *equidistant* if the the Hamming distance between any two codewords is exactly d. A code has *constant weight* equal to κ if the number of 1's in any codeword is exactly κ. Results and tables of the best constant weight codes of length less than 29 can be found in [10, 5].

Lemma 4.3 *Let $(\mathcal{C}_0, \mathcal{C}_1)$ be any $(2, n)$-threshold VCS with pixel expansion m and optimal relative difference $\alpha(m) = \alpha^*(n)$. Let $M \in \mathcal{C}_1$. The following properties hold:*

1. *The weight of any column of M is either $\lfloor n/2 \rfloor$ or $\lceil n/2 \rceil$.*
2. *For any pair of distinct rows of M any unavoidable pattern appears exactly $\alpha(m) \cdot m$ times.*
3. *For any $M \in \mathcal{C}_0 \cup \mathcal{C}_1$ it holds that $w = w(M[1]) = w(M[2]) = \cdots = w(M[n])$, that is, all the rows have the same weight w. Moreover, if n is even, then $w = m/2$; otherwise $\lfloor n/2 \rfloor (m/n) \leq w \leq \lceil n/2 \rceil (m/n)$.*
4. *Any $M \in \mathcal{C}_0$ has $M[1] = M[2] = \cdots = M[n]$.*
5. *For any $M \in \mathcal{C}_1$ the set $\{M[1], M[2], \ldots, M[n]\}$ is a $(m, n, 2 \cdot \alpha^*(n) \cdot m)$ equidistant code with constant weight w.*

Proof. From the proof of Theorem 4.2 one can see that the number of unavoidable patterns in any $M \in \mathcal{C}_1$ is exactly $\lfloor n/2 \rfloor \lceil n/2 \rceil m$, and that any column of M has to "cover" $\lfloor n/2 \rfloor \lceil n/2 \rceil$ unavoidable patterns. Hence, we have that the weight of any column of M is either $\lfloor n/2 \rfloor$ or $\lceil n/2 \rceil$. Moreover, for any distinct $i, j \in \{1, \ldots, n\}$, the matrix $M[\{i, j\}]$ contains the patterns $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ each appearing exactly $\alpha^*(n) \cdot m$ times. Hence, it follows that for any distinct $i, j \in \{1, \ldots, n\}$ and for any $M \in \mathcal{C}_0 \cup \mathcal{C}_1$ it holds that $w(M[i]) = w(M[j])$.
If n is even, then, since the total number of 1's in $M \in \mathcal{C}_1$ is $(nm)/2$, we get that the weight of any row is equal to $m/2$ which implies that m has to be even. If n is odd,

then, since the weight of any column of $M \in \mathcal{C}_1$ is either $\lfloor n/2 \rfloor$ or $\lceil n/2 \rceil$, we have that $\lfloor n/2 \rfloor m \leq w \cdot n \leq \lceil n/2 \rceil m$. Hence, it follows that

$$\left\lfloor \frac{n}{2} \right\rfloor \frac{m}{n} \leq w \leq \left\lceil \frac{n}{2} \right\rceil \frac{m}{n}.$$

For any $M' \in \mathcal{C}_1$ and for any distinct $i, j \in \{1, \ldots, n\}$ it holds that $w(M'_{\{i,j\}}) = w + \alpha^*(n) \cdot m$. Since the contrast of the scheme is $\alpha^*(n) \cdot m$ it has to be that for any $M \in \mathcal{C}_0$ it holds that $w(M_{\{i,j\}}) = w$. From Property 2. of Definition 2.1 for any $M \in \mathcal{C}_0$ it holds that $w = w(M[1]) = \cdots = w(M[n])$, hence we get that $M[1] = M[2] = \cdots = M[n]$.
For any $M \in \mathcal{C}_1$ the rows of M have the same weight w and any two rows of M differ in exactly $2 \cdot \alpha^*(n) \cdot m$ positions. Therefore, the rows of M are the codewords of a $(m, n, 2 \cdot \alpha^*(n) \cdot m)$ equidistant code. □

We are now going to use a matrix $M \in \mathcal{C}_1$ to construct a combinatorial design with certain properties. Again, we need a few definitions. Let v, k and λ be positive integers with $2 \leq k < v$. A (v, k, λ)-*BIBD* (*balanced incomplete block design*) is a pair $(X, \mathcal{B})$, where X is a set of v elements (called *points*) and $\mathcal{B}$ is a collection of subsets of X (called *blocks*), such that each block contains exactly k points and each pair of points is a subset of exactly λ blocks. In a (v, k, λ)-BIBD, each point occurs in exactly $r = \lambda(v-1)/(k-1)$ blocks, and the total number of blocks is $b = vr/k = \lambda(v^2 - v)/(k^2 - k)$. The number r is called the *replication number* of the BIBD.

We record a fact concerning BIBDs that we will use later. Suppose $(X, \mathcal{B})$ is a (v, k, λ)-BIBD. Define a new structure $(X, \mathcal{A})$, where

$$\mathcal{A} = \{X \backslash B : B \in \mathcal{B}\}.$$

It is not difficult to see that $(X, \mathcal{A})$ is a $(v, v-k, b-2r+\lambda)$-BIBD. $(X, \mathcal{A})$ is called the *complement* of $(X, \mathcal{B})$.

Let v and λ be positive integers, and let K be a set of positive integers such that $2 \leq k < v$ for every $k \in K$. A (v, K, λ)-*PBD* (*pairwise balanced design*) is a pair $(X, \mathcal{B})$, where X is a set of v elements (called *points*) and $\mathcal{B}$ is a collection of subsets of X (called *blocks*), such that $|B| \in K$ for every $B \in \mathcal{B}$, and each pair of points is a subset of exactly λ blocks. As with BIBDs, we will use b to denote the number of blocks. Note that it is not necessarily the case in a PBD that there is a fixed integer r such that every point occurs in exactly r blocks. Observe also that a PBD with $|K| = 1$ is a BIBD.

Suppose that $(X, \mathcal{B})$ is a PBD (or a BIBD). The *point-block incidence matrix* of this design is the $v \times b$ matrix M, in which the rows are indexed by X and the columns are indexed by $\mathcal{B}$, where

$$m_{xB} = \begin{cases} 1 & \text{if } x \in B \\ 0 & \text{otherwise.} \end{cases}$$

We have the following results characterizing threshold VCS with optimal pixel expansion in terms of BIBDs and PBDs.

Theorem 4.4 *Suppose n is even. Then there exists a $(2, n)$-threshold VCS with pixel expansion m and (optimal) relative difference $\alpha(m) = \alpha^*(n)$ if and only if there exists an $\left(n, \frac{n}{2}, \frac{m(n-2)}{4n-4}\right)$-BIBD.*

Proof. Suppose that we have a $(2,n)$-threshold VCS with pixel expansion m and optimal relative difference. Let $M \in \mathcal{C}_1$. We will show that the M is the incidence matrix of an $\left(n, \frac{n}{2}, \frac{m(n-2)}{4n-4}\right)$-BIBD, $(X, \mathcal{B})$. The verifications follow from Lemma 4.3 in a straightforward manner. Since M has n rows, we have $|X| = n$, and since M has m columns, we have $|\mathcal{B}| = m$. Since every column of M has weight $n/2$, every block $B \in \mathcal{B}$ has size $n/2$. Since every row of M has weight $m/2$, the design has constant replication number $r = m/2$. Finally, since the Hamming distance between any two rows of M is exactly $2 \cdot \alpha(m) \cdot m$, we see that any two points in X occur in exactly

$$r - \alpha(m) \cdot m = \frac{m}{2} - \frac{mn}{4n-4} = \frac{m(n-1)}{4n-4} = \lambda$$

blocks. Hence the desired BIBD is obtained.
Conversely, suppose we have an $\left(n, \frac{n}{2}, \frac{m(n-2)}{4n-4}\right)$-BIBD. Let M be its point-block incidence matrix. Then we can obtain a (strong) $(2,n)$-threshold VCS with pixel expansion m and optimal relative difference by taking basis matrices S^1 and S^0, where $S^1 = M$ and S^0 is a matrix of n identical rows, each consisting of $m/2$ 1's followed by $m/2$ 0's. $\square$

The following result is proved by the same method; we omit the proof.

Theorem 4.5 *Suppose n is odd. Then there exists a $(2,n)$-threshold VCS with pixel expansion m and (optimal) relative difference $\alpha(m) = \alpha^*(n)$ if and only if there exists an $\left(n, \{\frac{n-1}{2}, \frac{n+1}{2}\}, w - \frac{m(n+1)}{4n}\right)$-PBD such that every point occurs in exactly w blocks, where w is an integer such that*

$$\frac{(n-1)m}{2n} \leq w \leq \frac{(n+1)m}{2n}.$$

4.1 Achieving Optimal Contrast with Minimal Pixel Expansion

In this subsection, we investigate $(2,n)$-threshold VCS with (optimal) relative difference in which the pixel expansion is as small as possible.

First, suppose n is even. By Theorem 4.4, there exists a $\left(n, \frac{n}{2}, \frac{m(n-2)}{4n-4}\right)$-BIBD. In this BIBD, the number of blocks $b = m$. The classical inequality known as Fisher's inequality states that $b \geq v$ in any BIBD. Hence it follows that $m \geq n$. Further, since λ must be an integer, it must be the case that $m(n-2) \equiv 0 \bmod (4n-4)$. Hence $m(n-2) \equiv 0 \bmod (n-1)$, and since $m(n-1) \equiv 0 \bmod (n-1)$, it follows that $m \equiv 0 \bmod (n-1)$. Combining this with the fact that $m \geq n$, we see that $m \geq 2n-2$. Thus, when $m = 2n-2$, we have an $(n, \frac{n}{2}, \frac{n}{2} - 1)$-BIBD, and we have shown the following.

Theorem 4.6 *Suppose n is even and there exists a $(2,n)$-threshold VCS with pixel expansion m and (optimal) relative difference $\alpha(m) = \alpha^*(n)$. Then $m \geq 2n-2$, and $m = 2n-2$ if and only if there exists a $(n, \frac{n}{2}, \frac{n}{2} - 1)$-BIBD.*

We will show that BIBDs with these parameters can often be constructed. However, before proceeding further, we review some more results from design theory.

A Hadamard matrix of order n is an $n \times n$ matrix H in which every entry is ± 1 and $HH^T = nI_n$, where I_n is the $n \times n$ identity matrix. For results on Hadamard matrices, see [4, 7]. We summarize some basic results now. It is well-known that Hadamard matrix of order

n exists only if $n = 1$, $n = 2$, or $n \equiv 0 \bmod 4$. The *Hadamard Matrix Conjecture* conjectures that Hadamard matrices exist for all orders divisible by four. Many constructions are known for Hadamard matrices. In particular, a Hadamard matrix of order $4t$ exists if $4t-1$ is a prime power. Also, it is known that a BIBD with parameters $(4t-1, 2t-1, t-1)$ exists if and only if a Hadamard matrix of order $4t$ exists.

A BIBD with $b = v$ is called *symmetric*, and it is known that any two blocks of a symmetric BIBD intersect in exactly λ points. Note that a (v,k,λ)-BIBD is symmetric if and only if $\lambda(v-1) = k(k-1)$. From a symmetric BIBD, two further BIBDs can be constructed, as follows. Suppose $(X, \mathcal{B})$ is a symmetric (v,k,λ)-BIBD, and let $B_0 \in \mathcal{B}$ be any block. Then is easy to see that

$$(B_0, \{B \cap B_0 : B \in \mathcal{B}, B \neq B_0\})$$

is a $(k, \lambda, \lambda-1)$-BIBD, called a *derived* BIBD. Further,

$$(X \backslash B_0, \{B_0 \backslash B : B \in \mathcal{B}, B \neq B_0\})$$

is seen to be a $(v-k, k-\lambda, \lambda)$-BIBD, called a *residual* BIBD.

A $(2n-1, n-1, \frac{n}{2}-1)$-BIBD is a symmetric BIBD which is equivalent to a Hadamard matrix of order $2n$, by the remark above. From this BIBD, we can construct the $(n, \frac{n}{2}, \frac{n}{2}-1)$-BIBD required in Theorem 4.6 as the residual design. Thus, if the Hadamard matrix conjecture is true, then the desired threshold VCS can be constructed for any even n.

Example 4.1 Suppose $n = 6$. $(\mathbf{Z}_{11}, \mathcal{B})$ is an $(11, 5, 2)$-BIBD, where

$$\mathcal{B} = \{\{0,2,3,4,8\} + i \bmod 11 : i \in \mathbf{Z}_{11}\}.$$

If we compute the residual design of this BIBD with respect to the block $\{0,2,3,4,8\}$, then we obtain a $(6,3,2)$-BIBD, $(X, \mathcal{A})$, where $X = \{1,5,6,7,9,10\}$ and $\mathcal{A}$ consists of the following ten blocks: $\{1,5,9\}$, $\{5,6,10\}$, $\{5,6,7\}$, $\{1,6,7\}$, $\{5,7,9\}$, $\{6,9,10\}$, $\{7,9,10\}$, $\{1,5,10\}$, $\{1,6,9\}$ and $\{1,7,10\}$. If we form the point-block incidence matrix of this BIBD, then we get the following:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

This is the basis matrix S^1 of a $(2,6)$-threshold visual cryptography scheme with pixel expansion $m = 10$ and $\alpha = 3/10$. The matrix S^0 can be taken to be the 6×10 matrix in which every row is equal to (1111100000). $\Box$

We now turn to odd n. Theorem 4.5 says we have an $\left(n, \{\frac{n-1}{2}, \frac{n+1}{2}\}, w - \frac{m(n+1)}{4n}\right)$-PBD such that every point occurs in exactly w blocks, where

$$\frac{(n-1)m}{2n} \leq w \leq \frac{(n+1)m}{2n}. \tag{3}$$

Let x be any point in the PBD, and suppose that x occurs in s blocks of size $(n+1)/2$ and hence in $w-s$ blocks of size $(n-1)/2$. Since x occurs with every other point in exactly $w - m(n+1)/(4n)$ blocks, we obtain

$$s\left(\frac{n-1}{2}\right) + (w-s)\left(\frac{n-3}{2}\right) = \lambda(v-1) = \left(w - \frac{m(n+1)}{4n}\right)(n-1),$$

from which it follows that

$$s = \left(\frac{n+1}{2}\right)\left(w - \frac{m(n-1)}{2n}\right). \tag{4}$$

Now, Fisher's inequality (for BIBDs) that we used above can also be shown to hold for PBDs (see, for example, Beth, Jungnickel and Lenz [4, p. 81]). So we again have $m \geq n$. Let's assume that $m = n$. Then it follows from (3) that $w = (n-1)/2$ or $w = (n+1)/2$, so we have two cases to consider.

In the first case, Equation (4) says that $s = 0$. In other words, the PBD is a BIBD, namely, an $\left(n, \frac{n-1}{2}, \frac{n-3}{4}\right)$-BIBD. This implies that $n \equiv 3 \bmod 4$, and the BIBD is equivalent to a Hadamard matrix of order $n+1$.

In the second case, Equation (4) yields $s = (n+1)/2 = w$. Again, the PBD is a BIBD, this time an $\left(n, \frac{n+1}{2}, \frac{n+1}{4}\right)$-BIBD. As before, this implies that $n \equiv 3 \bmod 4$. Now, the complement of this BIBD is a $\left(n, \frac{n-1}{2}, \frac{n-3}{4}\right)$-BIBD (and vice versa). So we get back to the parameter situation considered in the first case, and we see that an $\left(n, \frac{n+1}{2}, \frac{n+1}{4}\right)$-BIBD is also equivalent to a Hadamard matrix of order $n+1$.

We have shown the following.

Theorem 4.7 *Suppose $n \equiv 3 \bmod 4$ and there exists a $(2,n)$-threshold VCS with pixel expansion m and (optimal) relative difference $\alpha(m) = \alpha^*(n)$. Then $m \geq n$, and $m = n$ if and only if there exists a $\left(n, \frac{n-1}{2}, \frac{n-3}{4}\right)$-BIBD (or, equivalently, a Hadamard matrix of order $n+1$).*

Example 4.2 Suppose $n = 11$. We use the $(11,5,2)$-BIBD constructed in Example 4.1. The point-block incidence matrix of this BIBD is as follows:

$$\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1
\end{pmatrix}.$$

This is the basis matrix S^1 of a $(2,11)$-threshold visual cryptography scheme with pixel expansion $m = 11$ and $\alpha = 3/11$. The matrix S^0 can be taken to be the 11×11 matrix in which every row is equal to (11111000000).

Alternatively, we could construct an $(11, 6, 3)$-BIBD as the complement of the $(11, 5, 2)$-BIBD given above. The resulting basis matrix S^1 would be the formed by interchanging 0's and 1's in the matrix given above, and S^0 would consist of 11 identical rows equal to (11111100000). $\square$

Finally, we need to investigate the case $n \equiv 1 \bmod 4$. In this case, we have $m > n$ since $m = n$ is not possible. Since λ is an integer, it must be the case that $m(n+1) \equiv 0 \bmod (4n)$. From this it follows that $m \equiv 0 \bmod n$, and since $m > n$ we see that $m \geq 2n$.

Let's suppose that $m = 2n$. There are three values for w permitted by (3), namely, $w = n-1, n$ or $n+1$. We consider each possibility in turn. If $w = n-1$, then Equation (4) yields $s = 0$. Our PBD is an $\left(n, \frac{n-1}{2}, \frac{n-3}{2}\right)$-BIBD. If there is a Hadamard matrix of order $2n+2$, then there is a (symmetric) $\left(2n+1, n, \frac{n-1}{2}\right)$-BIBD and our desired BIBD can be constructed as the derived BIBD.

Next we consider $w = n+1$. In this case we compute from Equation (4) that $s = n+1 = w$. Now our PBD is an $\left(n, \frac{n+1}{2}, \frac{n+1}{2}\right)$-BIBD. This BIBD is the complement of the $\left(n, \frac{n-1}{2}, \frac{n-3}{2}\right)$-BIBD just considered.

Finally, there is the possibility that $w = n$. In this case Equation (4) tells us that $s = (n+1)/2$. So each point occurs in $(n+1)/2$ blocks of size $(n+1)/2$ and in $(n-1)/2$ blocks of size $(n-1)/2$. It can further be computed that there are n blocks of size $(n+1)/2$ and n blocks of size $(n-1)/2$, and $\lambda = (n-1)/2$.

Let the PBD that we have described be denoted $(X, \mathcal{B})$. Now, suppose we create a new point $\infty \notin X$, and adjoin ∞ to every block in $\mathcal{B}$ of size $(n-1)/2$. Then it is not difficult to see that we obtain an $\left(n+1, \frac{n+1}{2}, \frac{n-1}{2}\right)$-BIBD. Conversely, from any BIBD with these parameters, if we delete all occurrences of any one point, we obtain a PBD with the parameters we started with.

Our final observation is that a $\left(n+1, \frac{n+1}{2}, \frac{n-1}{2}\right)$-BIBD can be constructed as the residual BIBD of a $\left(2n+1, n, \frac{n-1}{2}\right)$-BIBD, which is equivalent to a Hadamard matrix of order 2n+2 (note that $2n+2 \equiv 0 \bmod 4$).

Summarizing the three cases that arise when $n \equiv 1 \bmod 4$, we have the following.

Theorem 4.8 *Suppose $n \equiv 1 \bmod 4$ and there exists a $(2, n)$-threshold VCS with pixel expansion m and (optimal) relative difference $\alpha(m) = \alpha^*(n)$. Then $m \geq 2n$, and $m = 2n$ if and only if there exists an $\left(n, \frac{n-1}{2}, \frac{n-3}{2}\right)$-BIBD or an $\left(n+1, \frac{n+1}{2}, \frac{n-1}{2}\right)$-BIBD.*

Example 4.3 Suppose $n = 5$. The derived design of the $(11, 5, 2)$-BIBD presented in Example 4.1 with respect to the block $B_0 = \{0, 2, 3, 4, 8\}$ produces the $(5, 2, 1)$-BIBD $(B_0, \mathcal{A}')$, where $\mathcal{A}'$ consists of the following ten blocks: $\{3, 4\}$, $\{2, 4\}$, $\{0, 3\}$, $\{4, 8\}$, $\{2, 8\}$, $\{3, 8\}$, $\{0, 4\}$, $\{0, 8\}$, $\{0, 2\}$ and $\{2, 3\}$. If we form the point-block incidence matrix of this BIBD, then we get the following:

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

This is the matrix S^1 of a $(2,5)$-threshold visual cryptography scheme with pixel expansion $m = 10$ and $\alpha = 3/10$. The matrix S^0 can be taken to be the 5×10 matrix in which every row is equal to (1111000000).

We could have instead used the complement of the $(5,2,1)$-BIBD, which is a $(5,3,3)$-BIBD, to create the matrix S^1. In this case, S^0 would be the matrix in which every row is equal to (1111110000).

Finally, we could have started with a $(6,3,2)$-BIBD (one of which was constructed in Example 4.1), and then deleted a point to form a PBD. If we deleted the point 10 from the BIBD produced in Example 4.1, we would get the PBD having point set $\{1,5,6,7,9\}$ and the following ten blocks: $\{1,5,9\}$, $\{5,6\}$, $\{5,6,7\}$, $\{1,6,7\}$, $\{5,7,9\}$, $\{6,9\}$, $\{7,9\}$, $\{1,5\}$, $\{1,6,9\}$, $\{1,7\}$. This PBD would give rise to the following matrix S^1:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

S^0 would be the matrix in which every row is equal to (1111100000). $\square$

Finally, we summarize our lower bounds on m, as a function of n, for VCS with optimal relative difference. The following is an immediate consequence of Theorems 4.6, 4.7 and 4.8.

Theorem 4.9 *Suppose there exists a $(2,n)$-threshold VCS with pixel expansion m and (optimal) relative difference $\alpha(m) = \alpha^*(n)$. Then*

$$m \geq \begin{cases} 2n-2 & \text{if } n \text{ is even} \\ n & \text{if } n \equiv 3 \bmod 4. \\ 2n & \text{if } n \equiv 1 \bmod 4. \end{cases}$$

Note that all the inequalities in Theorem 4.9 are in fact equalities if the Hadamard Matrix Conjecture is true.

In the next subsection, we will show how to construct schemes with pixel expansion m that is much smaller than in the constructions given so far, while achieving a value of $\alpha(m) \approx 1/4$, which is close to optimal.

4.2 Achieving High Contrast with Smaller Pixel Expansion

We previously studied threshold VCS with optimal relative difference, and determined the minimum pixel expansion of such schemes (modulo the Hadamard Matrix Conjecture). We now prove a lower bound on m for any threshold VCS where $\alpha(m) > 1/4$.

Theorem 4.10 *Let $n \geq 2$. In any $(2,n)$-threshold visual cryptography scheme with pixel expansion m and $\alpha(m) > 1/4$, it holds that $m \geq n-1$.*

Proof. Suppose we have a $(2,n)$-threshold visual cryptography scheme with pixel expansion m and $\alpha(m) > 1/4$. Since $\alpha(m) \cdot m$ is an integer, we have $\alpha(m) \geq \frac{m+1}{4m}$. From Equation (2) in the proof of Theorem 4.2, we have the following:

$$
\begin{aligned}
m &\geq \frac{n(n-1)\cdot\alpha(m)\cdot m}{\lfloor n/2\rfloor\lceil n/2\rceil}\\
&\geq \frac{4(n-1)\cdot\alpha(m)\cdot m}{n}\\
&\geq \frac{4(n-1)(m+1)}{4n}\\
&= \frac{(n-1)(m+1)}{n}.
\end{aligned}
$$

From this it follows that $m \geq n-1$. □

So, if we hope to construct a threshold VCS with $m < n-1$, we must have $\alpha \leq 1/4$. We will be able to construct such schemes from constant weight codes, in a similar fashion as was done in Theorem 4.4. We begin by observing that any constant weight code provides a threshold VCS.

Theorem 4.11 *Suppose $\mathcal{C}$ is an (m,n,d) code having constant weight κ. Then there exists a strong $(2,n)$-threshold visual cryptography scheme with pixel expansion m and $\alpha(m) = d/(2m)$.*

Proof. The $n \times m$ basis matrix S^1 has as its rows the n codewords in $\mathcal{C}$. The basis matrix S^0 consists of n identical rows each of weight κ. □

In the previous subsection, we used constant weight codes derived from incidence matrices of certain BIBDs and PBDs. We now use a class of codes due to Caragiu to construct threshold VCS.

Theorem 4.12 *Suppose q is an odd prime power. Then there exists a strong $(2,(q^2-q)/2)$-threshold visual cryptography scheme with pixel expansion $m = q$ and*

$$\alpha(q) = \frac{1}{4} - \frac{3}{4\sqrt{q}}.$$

Proof. In [6], Caragiu showed the existence of a $(q,(q^2-q)/2, q/2 - 3\sqrt{q}/2)$ code having constant weight $(q-1)/2$, for all odd prime powers q. Apply Theorem 4.11. □

So we obtain $\alpha(m) = 1/4 - \epsilon$, where $\epsilon > 0$ and $\epsilon \to 0$ as $q \to \infty$. In this construction, we have $m = O(\sqrt{n})$, which is a significant improvement over $m = \Omega(n)$, which is the best possible when $\alpha(m) > 1/4$.

5 Some Constructions for (k,n)-threshold VCS

In this section we give some new constructions for (k,n)-threshold visual cryptography schemes having high relative difference $\alpha(m)$. To construct our schemes, we need an *initial matrix* defined as follows.

Definition 5.1 *Let n,ℓ,k be integers such that $k|n$. An* initial matrix *$IM(n,\ell,k)$ is an $n \times \ell$ matrix whose entries are elements of a ground set $A = \{a_1,\ldots,a_k\}$, in which the set of columns is equal to the set of vectors in which each element of A appears n/k times.*

The number of columns, ℓ, of an initial matrix $IM(n,\ell,k)$ is equal to the number of "anagrams" of the word

$$\underbrace{a_1 \dots a_1}_{\frac{n}{k} \text{ times}} \cdots \underbrace{a_i \dots a_i}_{\frac{n}{k} \text{ times}} \cdots \underbrace{a_k \dots a_k}_{\frac{n}{k} \text{ times}},$$

that is

$$\ell = \frac{n!}{\left((\frac{n}{k})!\right)^k}.$$

Given an initial matrix $IM(n,\ell,k)$ 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 $a_1,\dots,a_k$, respectively, with the 1-st,$\dots,k$-th rows of the corresponding basis matrices T_k^0 and T_k^1 of the (k,k)-threshold VCS described in Section 3. The scheme obtained by applying the previous technique is a (k,n)-threshold VCS as Theorem 5.2 shows.

Theorem 5.2 *Let n and k be integers such that $2 \le k \le n$ and $k|n$. Then, there exists a strong (k,n)-threshold VCS with*

$$m = \frac{n!}{\left((\frac{n}{k})!\right)^k} \cdot 2^{k-1} \qquad \textit{and} \qquad \alpha(m) = \frac{\left(\frac{n}{k}\right)^k}{\binom{n}{k} \cdot 2^{k-1}}.$$

Proof. Let T_k^0 and T_k^1 be the basis matrices of the (k,k)-threshold VCS previously described. Let $\mathcal{M}$ be the initial matrix $IM(n,\ell,k)$ whose entries are elements of a set $A = \{a_1,\dots,a_k\}$. Finally, let S^0 and S^1 be two $n \times (\ell \cdot 2^{k-1})$ matrices constructed by replacing the symbols $a_1,\dots,a_k$, with the 1-st,$\dots,k$-th rows of the basis matrices T_k^0 and T_k^1, respectively. In the previous construction, when we replace the symbols $a_1,\dots,a_k$ of $\mathcal{M}$ with the rows of T_k^0 (T_k^1, resp.) the column i of $\mathcal{M}$ 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 S^0 and S^1 are basis matrices of a (k,n)-threshold VCS.
Consider any $q \ge k$ distinct indices, say $i_1,\dots,i_q$, and let $X = \{i_1,\dots,i_q\}$. Notice that the quantity $w(S_X^1) - w(S_X^0)$ does not depend on the actual set X but only on its size. Let $\beta(q) = w(S_X^1) - w(S_X^0)$. Recall that the (k,k)-threshold VCS with basis matrices T_k^0 and T_k^1 is uniform, that is, for every $1 \le p \le k-1$ the "or" of any p rows of T_k^0 and T_k^1 has weight $f(p)$ for some function f. Let us show that $\beta(q)$, with $k \le q \le n$, is a non-decreasing function. First, notice that, for any X of cardinality at least k, the value $w(S_X^1) - w(S_X^0)$ is equal to the number γ_X of columns in $\mathcal{M}[X]$ having as entries all the symbols from the ground set A. Clearly, if we consider a set $Y \supset X$ the number γ_Y of columns in $\mathcal{M}[Y]$ having as entries all the symbols from the ground set A cannot be less than γ_X. Therefore, for any $k \le q \le n$, it results that $\beta(q+1) \ge \beta(q)$. Hence, $\beta(q)$ is a non-decreasing function and it reaches its minimum for $q = k$. Defining $\alpha(m) = \beta(k)/m$ and setting $t_X = w(S_X^1)$ we get that Property 1. of Definition 2.2 is satisfied.
We now compute $\alpha(m) = \beta(k)/m$. Fix any k rows of the initial matrix $\mathcal{M}$, say $g_1,\dots,g_k$, the contrast $\alpha(m) \cdot m$ in this scheme is equal to the number of columns h of $\mathcal{M}$ having the symbols $a_1,\dots,a_k$ in these rows, that is, $\Big\{M[g_1,h], M[g_2,h],\dots,M[g_k,h]\Big\} = A$. Hence, we get that

$$\alpha(m) \cdot m = \frac{k!(n-k)!}{\left(\left(\frac{n-k}{k}\right)!\right)^k}.$$

Since

$$m = \ell \cdot 2^{k-1} = \frac{n! \cdot 2^{k-1}}{((\frac{n}{k})!)^k}$$

it results that

$$\alpha(m) = \frac{\left(\frac{n}{k}\right)^k}{\binom{n}{k} \cdot 2^{k-1}}.$$

We are left with proving that Property 2. of Definition 2.2 is satisfied. Therefore, we have to show that for any set $X \subseteq \{1, \ldots, n\}$ of cardinality at most $k-1$, $S^0[X]$ is equal to $S^1[X]$ 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. Thus, the theorem holds. $\square$

The previous theorem provides a construction for (k,n)-threshold VCS when $k|n$. To realize (k,n)-threshold VCS for any values of the parameters k and n we can construct, using the technique presented in Theorem 5.2, a (k, n_0)-threshold VCS, where $n_0 > n$ is a multiple of k, and then consider only the first n rows of the basis matrices of this scheme. By Lemma 3.2 the scheme obtained in this way is a (k,n)-threshold VCS having the same parameters as the (k, n_0)-threshold VCS. The following theorem states the existence of (k,n)-threshold VCS for any value of k and n.

Theorem 5.3 *Let k and n be integers such that $2 \leq k \leq n$. Then there exists a strong (k,n)-threshold VCS with*

$$m = \frac{n_0!}{((\frac{n_0}{k})!)^k} \cdot 2^{k-1} \qquad \text{and} \qquad \alpha(m) = \frac{\left(\frac{n_0}{k}\right)^k}{\binom{n_0}{k} \cdot 2^{k-1}},$$

where $n_0 = \lceil \frac{n}{k} \rceil \cdot k$.

It is easy to see that a lower bound on the relative difference $\alpha(m)$ achieved in the previous theorem is

$$\alpha(m) \geq \frac{2}{(2e)^k}. \tag{5}$$

We now present a construction that is a modification of Theorem 5.2. It achieves (essentially) the same α but with a much smaller pixel expansion. It uses a combinatorial structure called an orthogonal array. An *orthogonal array $OA_\lambda(t,k,v)$* is a $\lambda v^t \times k$ array, say A, of elements from a set X of cardinality v, with the property that within any t columns of A every possible t-tuple of elements from X occurs in exactly λ rows.

Theorem 5.4 *Suppose there exists an $OA_\lambda(k,n,k)$. Then there exists a strong (k,n)-threshold VCS with $m = \lambda k^k 2^{k-1}$ and*

$$\alpha(m) = \frac{(k-1)!}{(2k)^{k-1}}.$$

Proof. The construction is the same as Theorem 5.2, except that the initial matrix is replaced by the transpose A^T of an $\mathrm{OA}_\lambda(k,n,k)$, A. Note that A^T has n rows and $\lambda \cdot k^k$ columns.

Let's compute the contrast in the resulting (k, n) threshold VCS. Fix any k rows of A^T. Similar to the proof of Theorem 5.2, $\alpha(m) \cdot m$ equals the number of columns of A^T in which k distinct symbols occur in the k given rows. Since A is an orthogonal array, there are λ such columns for every permutation of the k symbols. Hence,

$$\alpha(m) \cdot m = \lambda \cdot k!.$$

Since

$$m = \lambda \cdot k^k 2^{k-1},$$

it follows that

$$\alpha(m) = \frac{(k-1)!}{(2k)^{k-1}},$$

as desired. ∎

Let us compare the values of α obtained in Theorems 5.2 and 5.4. It is easy to see that

$$\frac{\left(\frac{n}{k}\right)^k}{\binom{n}{k} \cdot 2^{k-1}} = \frac{(k-1)!}{(2k)^{k-1}} \cdot \frac{n^k}{n(n-1)\cdots(n-k+1)}.$$

Hence, the value of α in Theorem 5.2 is slightly larger, but for large n, they are essentially the same.

We need some constructions for orthogonal arrays. These are obtained easily from codes. Let q be a prime power. An $[n, \ell, d]_q$ *code* is an ℓ-dimensional subspace of $(GF(q))^n$, say $\mathcal{C}$, such that any any two distinct vectors in $\mathcal{C}$ have Hamming distance at least d. The following construction of orthogonal arrays from codes is well-known.

Lemma 5.5 *If there exists an $[n, \ell, d]_q$ code, then there exists an $OA_\lambda(d-1, n, q)$, where $\lambda = q^{n-\ell-d+1}$.*

Proof. Let $\mathcal{C}$ be the hypothesized $[n, \ell, d]_q$ code, and let $\mathcal{C}^\perp$ be the dual code to $\mathcal{C}$ (i.e., the orthogonal complement of $\mathcal{C}$ in $(GF(q))^n$). If we construct the $q^{n-\ell} \times n$ array A whose rows are the codewords in $\mathcal{C}^\perp$, then it can be shown that A is an $\mathrm{OA}_\lambda(d-1, n, q)$ (see, for example, [10, p. 139]). ∎

Thus, we have the following corollary.

Corollary 5.6 *If there exists an $[n, \ell, q+1]_q$ code, then there exists a (q, n)-threshold VCS with $m = q^{n-\ell}2^{q-1}$ and*

$$\alpha(m) = \frac{(q-1)!}{(2q)^{q-1}}.$$

We will use BCH codes as our required ingredient in Corollary 5.6. The following is standard theory of BCH codes; see [9] for more details. Suppose $n = q^t - 1$, where q is a prime power and t is an integer. Let $\beta \in GF(q^t)$ be a primitive element, and define

$$g(x) = \mathrm{lcm}\{m(\beta), m(\beta^2), \ldots, m(\beta^q)\},$$

where $m(\gamma)$ denotes the minimal polynomial of γ ($\gamma \in GF(q^t)$). Then $g(x)$ is the generator polynomial for a $[n, \ell, q+1]_q$ BCH code, where $\ell = n - \deg(g)$. Since $\deg(m(\gamma)) \leq t$ for any $\gamma \in GF(q^t)$ and since $m(\gamma) = m(\gamma^q)$, it follows that $\deg(g) \leq (q-1)t$, and hence $\ell \geq n - (q-1)t$. Thus we have an $[n, n-(q-1)t, q+1]_q$ code.

Now, applying Corollary 5.6, we obtain our main result.

Theorem 5.7 *For any prime power q and any integer $t \geq 2$, there exists a strong (q, n)-threshold VCS with $n = q^t - 1$, $m = (2n+2)^{q-1}$ and*

$$\alpha(m) = \frac{(q-1)!}{(2q)^{q-1}}.$$

This theorem shows that, if k is a prime power, then we can construct (k, n)-threshold VCS where $\alpha(m) = \Omega\left(\frac{\sqrt{k}}{(ek)^k 2^{k-1}}\right)$ and $m = O((2n)^{k-1})$.

We now describe a generalization of Theorem 5.4.

Theorem 5.8 *Suppose there exists a (strong) (k, n_0)-threshold VCS with pixel expansion m_0 and relative difference α_0. Suppose also there exists an $OA_\lambda(k, n, n_0)$. Then there exists a (strong) (k, n)-threshold VCS with $m = \lambda \cdot {n_0}^k \cdot m_0$ and*

$$\alpha(m) = \frac{\alpha_0 \cdot n_0!}{{n_0}^k (n_0 - k)!}.$$

Proof. The construction is the same as Theorem 5.4, except that each symbol a_i ($1 \leq i \leq n_0$) is replaced by the i-th row of a basis matrix of the hypothesized (k, n_0)-threshold VCS. □

We observe that Theorem 5.2 can be generalized in the same way as Theorem 5.4. Also, if we set $n_0 = k$, $\alpha_0 = 1/2^{k-1}$, and $m_0 = 2^{k-1}$ in Theorem 5.8, then we obtain Theorem 5.4.

We give an example to illustrate the application of Theorem 5.8. Suppose $k = 3$. From Theorem 5.4 we get a $(3, n)$-threshold scheme with $\alpha(m) = 1/18$. However, we can also apply Theorem 5.8 with $k = 3$, $n_0 = 4$, $m_0 = 6$, and $\alpha_0 = 1/6$ (see Example 6.1). Then we obtain $(3, n)$-threshold schemes with $\alpha(m) = 1/16$.

6 On the Structure of (k, n)-threshold VCS

In this section we give necessary and sufficient conditions for the existence of weak (k, n)-threshold VCS realized using basis matrices. This allows us to prove a lower bound on the pixel expansion and an upper bound on the relative difference. Both bounds also apply to the case of (k, n)-threshold VCS. Finally, we show how our results on the relative difference can be extended to the general case of schemes realized using collections of $n \times m$ boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$.

Before we state our results we need to set up our notation. Let M be an $n \times m$ matrix and let $X \subseteq \{1, \ldots, n\}$ and $Z \subseteq \{1, \ldots, m\}$. Let $M[X][Z]$ denote the $|X| \times |Z|$ matrix obtained from M by considering its restriction to rows and columns indexed by X and Z, respectively.

Let $n \geq k \geq 2$ and let S^0 and S^1 be the $n \times m$ basis matrices of a weak (k, n)-threshold VCS with relative difference $\alpha(m)$. For $i = 1, \ldots, n$, let $N_i = \{1, \ldots, n\} \backslash \{i\}$, $Z_i = \{j : S^1[i][j] = 1\}$, and let $R_i = \{1, \ldots, n\} \backslash Z_i$, that is, Z_i denotes the set of indices of columns having a one as i-th entry; whereas, R_i denotes the set of indices of columns having a zero as i-th entry. Finally, for $i = 1, \ldots, n$, and for $h = 0, 1$, let

$$A^{i,h} = S^h[N_i][R_i] \qquad \text{and} \qquad B^{i,1-h} = S^h[N_i][Z_i].$$

In other words, the pairs of matrices $A^i = (A^{i,0}, A^{i,1})$ and $B^i = (B^{i,0}, B^{i,1})$ are the sub-matrices of S^0 and S^1 obtained by removing all the columns having a one and a zero, respectively, as i-th entry and removing the row i. For instance, fixing the first row of both basis matrices S^0 and S^1, then, up to a column permutation, the basis matrices S^0 and S^1 are of the following form:

$$S^0 = \left[\begin{array}{c|c} 0\cdots 0 & 1\cdots 1 \\ \hline A^{1,0} & B^{1,1} \end{array}\right] \qquad S^1 = \left[\begin{array}{c|c} 0\cdots 0 & 1\cdots 1 \\ \hline A^{1,1} & B^{1,0} \end{array}\right].$$

For any $Y \subseteq N_i$, let $\Delta_Y^{A^i} = w(A_Y^{i,1}) - w(A_Y^{i,0})$ and let $\Delta_Y^{B^i} = w(B_Y^{i,1}) - w(B_Y^{i,0})$.
We say that the pair of matrices (S^0, S^1) has the *structural property for row i*, if, for any $Y \subseteq N_i$, the following properties hold:

1. If $|Y| \leq k-2$, then, up to a column permutation, $A^{i,0}[Y] = A^{i,1}[Y]$ and $B^{i,0}[Y] = B^{i,1}[Y]$.
2. If $|Y| = k-1$, then, up to a column permutation, $A^{i,0}[Y] \circ B^{i,1}[Y] = A^{i,1}[Y] \circ B^{i,0}[Y]$. Moreover, $\Delta_Y^{A^i} = \Delta_Y^{B^i} \geq \alpha(m) \cdot m$.
3. If $|Y| = k$, then $\Delta_Y^{A^i} - \Delta_Y^{B^i} \geq \alpha(m) \cdot m$.

The next theorem holds.

Theorem 6.1 *Let S^0 and S^1 be two $n \times m$ boolean matrices. The matrices S^0 and S^1 are basis matrices of a weak (k, n)-threshold VCS with pixel expansion m and relative difference $\alpha(m)$ if and only if, for $i = 1, \ldots, n$, the structural property for row i is satisfied.*

Proof. Assume that S^0 and S^1 are basis matrices of a weak (k, n)-threshold VCS with pixel expansion m and relative difference $\alpha(m)$. Now we show that, for $i = 1, \ldots, n$, the structural property for row i is satisfied.
Property 1. and the first part of Property 2. derive from condition 2. of Definition 2.2 which states that, for any $Y \subseteq \{1, \ldots, n\}$ with $|Y| \leq k-1$, the sub-matrices $S^1[Y]$ and $S^0[Y]$ are equal up to a column permutation. Hence, for any $Y \subseteq N_i$ with $|Y| \leq k-2$ the sub-matrices $S^1[Y \cup \{i\}]$ and $S^0[Y \cup \{i\}]$ are equal up to a column permutation. In particular, we have that, up to a column permutation,

$$S^1[Y \cup \{i\}][R_i] = S^0[Y \cup \{i\}][R_i] \text{ and } S^1[Y \cup \{i\}][Z_i] = S^0[Y \cup \{i\}][Z_i],$$

which implies that $A^{i,0}[Y] = A^{i,1}[Y]$ and $B^{i,0}[Y] = B^{i,1}[Y]$.
It is immediate to see that for any $Y \subseteq N_i$ with $|Y| = k-1$ we have

$$A^{i,0}[Y] \circ B^{i,1}[Y] = A^{i,1}[Y] \circ B^{i,0}[Y].$$

Notice that, for any $Y \subseteq \{1, \ldots, n\}$, it holds that

$$w(S_Y^0) = w(A_Y^{i,1}) + w(B_Y^{i,0}) \text{ and } w(S_Y^1) = w(A_Y^{i,0}) + w(B_Y^{i,1}).$$

Therefore, for any $Y \subseteq N_i$ with $|Y| = k-1$, as $w(S_Y^1) = w(S_Y^0)$, we get that $\Delta_Y^{A^i} = \Delta_Y^{B^i}$.
Further,

$$\Delta_Y^{A^i} = w(S_{Y \cup \{i\}}^1) - w(S_{Y \cup \{i\}}^0) \geq \alpha(m) \cdot m,$$

from condition 1. of Definition 2.2. Therefore, $\Delta_Y^{A^i} = \Delta_Y^{B^i} \geq \alpha(m) \cdot m$.
We also prove Property 3. from condition 1. of Definition 2.2. For any $Y \subseteq N_i$ with $|Y| = k$, one has that

$$\Delta_Y^{A^i} - \Delta_Y^{B^i} = w(S_Y^1) - w(S_Y^0) \geq \alpha(m) \cdot m.$$

Now, we prove that if S^0 and S^1 satisfy the structural property for row i (for $i = 1, \ldots, n$), then S^0 and S^1 are basis matrices of a weak (k,n)-threshold VCS with pixel expansion m and relative difference $\alpha(m)$. Indeed, for $Y \subseteq \{1, \ldots, n\}$ with $|Y| = k$, setting $t_Y = w(S_Y^1)$ and using the second part of Property 2. along with Property 3., we get that condition 1. of Definition 2.2 holds. On the other hand, Property 1. and the first part of Property 2. imply that for any $Y \subseteq \{1, \ldots, n\}$ with $|Y| \leq k-1$, the sub-matrices $S^1[Y]$ and $S^0[Y]$ are equal up to a column permutation. Therefore, condition 2. of Definition 2.2 is satisfied. Thus, the theorem holds. $\square$

Corollary 6.2 *S^0 and S^1 are basis matrices of a weak (k,n)-threshold VCS with pixel expansion m and relative difference $\alpha(m)$ if and only if, for $i = 1, \ldots, n$, the pairs of matrices $A^i = (A^{i,0}, A^{i,1})$ and $B^i = (B^{i,0}, B^{i,1})$ are basis matrices of weak $(k-1, n-1)$-threshold VCSs with pixel expansions $m_{A^i} = m - w(S^1[i])$ and $m_{B^i} = w(S^1[i])$ (resp.) and relative differences $\alpha^{A^i}(m_{A^i})$ and $\alpha^{B^i}(m_{B^i})$ (resp.), where*

$$\alpha^{A^i}(m_{A^i}) \cdot m_{A^i} = \alpha^{B^i}(m_{B^i}) \cdot m_{B^i} \geq \alpha(m) \cdot m.$$

Proof. The "only if" part is trivial as it is an immediate consequence of Theorem 6.1, using the fact that Properties 1. and 2. hold for every row i.
Conversely, suppose for $i = 1, \ldots, n$ that A^i and B^i are basis matrices of a weak $(k-1, n-1)$-threshold VCS satisfying the hypotheses of the theorem. Clearly, it is sufficient to prove that Property 3. holds for all i and for all $Y \subseteq N_i$ with $|Y| = k$. Recall that $\Delta_Y^{A^i} - \Delta_Y^{B^i} = w(S_Y^1) - w(S_Y^0)$. Let $j \in Y$ and define $Y_0 = Y \setminus \{j\}$. By definition $w(S_Y^1) - w(S_Y^0) = \Delta_{Y_0}^{A^j}$. Apply Property 2. to row j using the set Y_0 of $k-1$ rows. Then $\Delta_{Y_0}^{A^j} \geq \alpha(m) \cdot m$. Hence, $\Delta_Y^{A^i} - \Delta_Y^{B^i} \geq \alpha(m) \cdot m$, as desired. $\square$

Example 6.1 We give basis matrices for a $(3,4)$-threshold VCS presented in [1]:

$$S^0 = \begin{bmatrix} 000111 \\ 001011 \\ 001101 \\ 001110 \end{bmatrix} \quad S^1 = \begin{bmatrix} 000111 \\ 100110 \\ 010110 \\ 001110 \end{bmatrix}.$$

This VCS has $m = 6$ and $\alpha(m) = 1/6$. From this scheme we obtain two $(2,3)$-threshold VCS. For example, if $i = 1$, then the basis matrices are as follows.

$$A^{1,0} = \begin{bmatrix} 001 \\ 001 \\ 001 \end{bmatrix} \quad A^{1,1} = \begin{bmatrix} 100 \\ 010 \\ 001 \end{bmatrix}$$

and

$$B^{1,0} = \begin{bmatrix} 110 \\ 110 \\ 110 \end{bmatrix} \quad B^{1,1} = \begin{bmatrix} 011 \\ 101 \\ 110 \end{bmatrix}.$$

Both of these $(2,3)$-threshold VCS have $m = 3$ and $\alpha(m) = 1/3$.

Notice that since any strong VCS is also a weak one, we have that any lower bound on the pixel expansion and any upper bound on the relative difference for a weak VCS also applies to the corresponding strong one. We show now that any upper bound on the relative difference for a (k,n)-threshold VCS realized by using basis matrices holds also for a (k,n)-threshold VCS realized using collections of $n \times m$ boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$. Indeed, Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the collections of $n \times m$ boolean matrices of a (k,n)-threshold VCS Σ. Without loss of generality we can assume that $r = |\mathcal{C}_0| = |\mathcal{C}_1|$ (see Section 2.1 of [1]). We can easily realize from $\mathcal{C}_0$ and $\mathcal{C}_1$ a scheme having the same relative difference as Σ. Suppose that $\mathcal{C}_0 = \{M^{0,1}, \ldots, M^{0,r}\}$ and $\mathcal{C}_1 = \{M^{1,1}, \ldots, M^{1,r}\}$. It is immediate to check that $S^0 = M^{0,1} \circ \cdots \circ M^{0,r}$ and $S^1 = M^{1,1} \circ \cdots \circ M^{1,r}$ constitute the basis matrices of a (k,n)-threshold VCS having the same relative difference as Σ. Therefore, any upper bound on the relative difference for a (k,n)-threshold VCS realized by using basis matrices holds also for the (k,n)-threshold VCS realized by using the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ of $n \times m$ boolean matrices.
Let $\alpha(k,n)$ denote the maximum value of the relative difference for which there exists a weak (k,n)-threshold VCS realized using basis matrices. The following theorem states an upper bound on the relative difference of any (k,n)-threshold VCS.

Theorem 6.3 *For any $n \geq k \geq 2$, it holds that*

$$\alpha(k,n) \leq \frac{\alpha(k-1,n-1)}{2}.$$

Moreover, the relative difference $\alpha(m)$ satisfies

$$\alpha(m) \leq \frac{1}{2^k} + \epsilon,$$

where

$$\epsilon = \begin{cases} \frac{1}{2^k(n-k+1)} & \text{if } n-k \text{ is even} \\ \frac{1}{2^k(n-k+2)} & \text{if } n-k \text{ is odd.} \end{cases}$$

Proof. Let Σ be a (k,n)-threshold VCS realized by using basis matrices S^0 and S^1 and let $\alpha(m)$ be the relative difference of Σ. Finally, let $A^i = (A^{i,0}, A^{i,1})$ and $B^i = (B^{i,0}, B^{i,1})$ be the basis matrices of weak $(k-1,n-1)$-threshold VCSs as given by Corollary 6.2. From Corollary 6.2, we have that

$$\alpha^{B^i}(m_{B^i}) \cdot m_{B^i} = \alpha^{A^i}(m_{A^i}) \cdot m_{A^i} \geq \alpha(m) \cdot m,$$

where $m_{A^i} = m - w(S^1[i])$ and $m_{B^i} = w(S^1[i])$. Therefore, recalling that $m = m_{A^i} + m_{B^i}$, we get that

$$\alpha(m) \leq \max\left\{\frac{\alpha^{A^i}(m_{A^i})}{2}, \frac{\alpha^{B^i}(m_{B^i})}{2}\right\},$$

from which we easily derive that $\alpha(k,n) \leq \alpha(k-1,n-1)/2$. Hence, it follows that

$$\alpha(k,n) \leq \frac{\alpha(2,n-k+2)}{2^{k-2}}.$$

$\square$

As a consequence of the previous theorem we have the following results which solve an open problem in [1]. The next result closes the gap on the pixel expansion for the access structures #16 and #17 analyzed in Section 9 of [1].

Theorem 6.4 *Let Γ_1 and Γ_2 be the access structures having basis $\{123, 124, 134, 234\}$ and $\{123, 124, 134\}$, respectively. In any visual cryptography scheme for Γ_1 or Γ_2, the relative difference satisfies $\alpha(m) \leq 1/6$ which implies that the pixel expansion m satisfies $m \geq 6$.*

Proof. The access structure Γ_1 is a $(3,4)$-threshold structure. Hence, by Theorem 6.3, in any $(3,4)$-threshold VCS with pixel expansion m the relative difference $\alpha(m)$ satisfies $\alpha(m) \leq 1/6$. Since in any VCS it must be that $\alpha(m) \cdot m \geq 1$ it has to be the case that $m \geq 6$.
A similar argument applies also to Γ_2 as the same structural property holds for row 1. This is easily seen due to the fact that when participant 1 is removed from the scheme the resulting access structure is a $(2,3)$-threshold structure. □

Recall that we determined the optimal value for the relative difference of $(2,n)$-threshold schemes in Section 4. The next cases to consider are $(3,n)$-threshold schemes. The upper bound from Theorem 6.3 is $\alpha(m) \leq 1/8 + \epsilon$, whereas the best construction we have gives $\alpha(m) \geq 1/16$ (see the end of Section 5).

The next theorem provides a lower bound for the pixel expansion m of any (k,n)-threshold VCS realized by basis matrices. Let $m(k,n)$ denote the minimum value m for which a weak (k,n)-threshold VCS realized by basis matrices exists.

Theorem 6.5 *In any (k,n)-threshold VCS realized by using basis matrices, it holds that*

$$m(k,n) \geq 2 \cdot m(k-1, n-1).$$

Moreover, the pixel expansion m satisfies

$$m \geq 2^{k-2} \cdot \mu,$$

where μ is the smallest integer such that $n \leq \binom{\mu}{\lfloor \frac{\mu}{2} \rfloor} + k - 2$.

Proof. From Corollary 6.2 we get that $m(k,n) \geq 2 \cdot m(k-1,n-1)$ from which we obtain that $m(k,n) \geq 2^{k-2} \cdot m(2, n-k+2)$. Applying Theorem 7.3 of [1], which states that in any $(2,n)$-threshold VCS, the pixel expansion m satisfies $n \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$, the theorem holds. □

The next corollary is an immediate consequence of previous theorem.

Corollary 6.6 *In any (k,n)-threshold VCS realized by using basis matrices, the pixel expansion m satisfies*

$$m \geq 2^{k-2} \cdot \log(n-k+2).$$

We do not know if the lower bound of Corollary 6.6 holds also for (k,n)-threshold VCS not constructed by using basis matrices. However, we can prove the following weaker bound as an immediate corollary of Theorem 6.3, using the fact that $m \geq 1/\alpha(m)$.

Corollary 6.7 *In any (k,n)-threshold VCS the pixel expansion m satisfies*

$$m \geq 2^k \cdot (1-\epsilon),$$

where

$$\epsilon = \begin{cases} \frac{1}{n-k+2} & \text{if } n-k \text{ is even} \\ \frac{1}{n-k+3} & \text{if } n-k \text{ is odd.} \end{cases}$$

7 On the Structure of Basis Matrices

In this section we analyze the structure of basis matrices S^0 and S^1 of (k,k)-threshold VCS. We say that a column of S^0 or S^1 is even (odd) if it has an even (odd) number of entries equal to 1.

Theorem 7.1 *Let S^0 and S^1 be two $n \times m$ boolean matrices such that the same column does not appear in both. Then, the matrices S^0 and S^1 are basis matrices of a (k,k)-threshold VCS with pixel expansion m and relative difference $\alpha(m) \leq h/2^{k-1}$ if and only if all the even columns appear in S^0 with multiplicity $h = m/2^{k-1}$ and all the odd columns appear in S^1 with the same multiplicity h. Consequently, $h \geq \alpha(m) \cdot m$, $\alpha(m) \leq 1/2^{k-1}$, and $m \geq 2^{k-1}$.*

Proof. We start by noticing that by Property 1 of Definition 2.2, the column with all zeroes has to belong to S^0 (e.g., see Lemma 5.11 of [1]). Assume that this all zeroes column appears with multiplicity h (by Lemma 5.11 of [1] it holds that $h \geq \alpha(m) \cdot m$).
Suppose that **c** and **d** are boolean columns of length n that differ only in one entry, say the i-th entry. Suppose that **c** appears with multiplicity h in S^j ($j = 0$ or 1). We have assumed that the same column does not appear in both basis matrices. Let $X_i = \{1, \ldots, k\} \backslash \{i\}$. Then, using the security condition $S^0[X_i] = S^1[X_i]$ up to a column permutation, we see that **d** appears with multiplicity h in S^{1-j}.
From the statements proved above, it follows that all the even columns appear in S^0 with multiplicity h and all the odd columns appear in S^1 with the same multiplicity h.
Conversely, if all the even columns appear in S^0 with multiplicity h and all the odd columns appear in S^1 with the same multiplicity h, then it is immediate to see that the matrices S^0 and S^1 are basis matrices of a (k,k)-threshold VCS with pixel expansion $m = h \cdot 2^{k-1}$ and with relative difference $\alpha(m) = 1/2^{k-1}$. Indeed, S^0 and S^1 can be thought of as the concatenation of h copies of the matrices T_k^0 and T_k^1, respectively, described at the beginning of Section 3. □

The "if" part of Theorem 7.1 was first shown by Naor and Shamir [12]. Also, Theorem 7.1 gives a more precise characterization of (k,k)-threshold VCS than the one provided by Theorem 10 and Corollary 11 of [8] which can be easily derived from our last result.

Lemma 5.3 of [1] states that if S^0 and S^1 are the two basis matrices of a (k,n)-threshold VCS and D is any $n \times p$ boolean matrix, then $S^0 \circ D$ and $S^1 \circ D$ are basis matrices of a (k,n)-threshold VCS. From this observation and Theorem 7.1 we obtain the following result.

Theorem 7.2 *Let S^0 and S^1 be two $n \times m$ boolean matrices. The matrices S^0 and S^1 are basis matrices of a weak (k,n)-threshold VCS with pixel expansion m if and only if for all* *subsets X consisting of k rows there exist a boolean matrix D_X and an integer h_X such that D_X is a sub-matrix of both $S^0[X]$ and $S^1[X]$, all the even columns appear in $S^0[X]\backslash D_X$ with multiplicity h_X, and all the odd columns appear in $S^1[X]\backslash D_X$ with multiplicity h_X.*

The next theorem provides a similar characterization for strong (k,n)-threshold VCS.

Theorem 7.3 *Let S^0 and S^1 be two $n \times m$ boolean matrices. The matrices S^0 and S^1 are basis matrices of a strong (k,n)-threshold VCS with pixel expansion m if and only if the conditions of Theorem 7.2 are satisfied, and in addition $S^0[X]$ contains more zero columns than $S^1[X]$ does, for all subsets X consisting of at least $k+1$ rows.*

Acknowledgements

D. R. Stinson would like to thank Alex Rosa for helpful comments. 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 National Council for Research (C.N.R.). Research of D. R. Stinson is supported by NSF grant CAR-9402141 and by the Center for Communication and Information Science at the University of Nebraska-Lincoln.

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Visual Cryptography for General Access Structures*, to appear in *Information and Computation*. (A preliminary version appeared as report TR96–012, Electronic Colloquium on Computational Complexity, available as `http://www.eccc.uni-trier.de/eccc/`.)

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Constructions and Bounds for Visual Cryptography*, in "23rd International Colloquium on Automata, Languages and Programming" (ICALP '96), F. M. auf der Heide and B. Monien Eds., Vol. 1099 of "Lecture Notes in Computer Science", Springer–Verlag, Berlin, pp. 416–428. 1996.

[3] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Extended Schemes for Visual Cryptography*, submitted to Discrete Applied Mathematics, 1996.

[4] Th. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Bibliographisches Institut, 1985.

[5] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, *A New Table of Constant Weight Codes*, IEEE Trans. on Inform. Theory, Vol. IT-36, no. 6, pp. 1334–1380, Jan. 1983.

[6] M. Caragiu, *On a Class of Constant Weight Codes*, Electronic Journal of Combinatorics **3** (1996), #R4, 13 pp.

[7] C. J. Colbourn and J. H. Dinitz, *CRC Handbook of Combinatorial Designs*, CRC Press, 1996.

[8] S. Droste, *New Results on Visual Cryptography*, in "Advances in Cryptology - CRYPTO '96", N. Koblitz Ed., Vol. 1109 of "Lecture Notes in Computer Science", Springer–Verlag, Berlin, pp. 401–415, 1996.

[9] J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, 1982.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[11] D. Naccache, *Colorful Cryptography – a purely physical secret-sharing scheme based on chromatic filters,* Coding and Information Integrity, French-Israeli workshop, December 1994.

[12] 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.

[13] M. Naor and A. Shamir, *Visual Cryptography II: Improving the Contrast via the Cover Base*, presented at Security in Communication Networks, Amalfi, Italy, September 16-17, 1996. Available as `http://www.unisa.it/SCN96/papers/NaSh.ps`.

[14] V. Rijmen and B. Preneel, *Efficient Colour Visual Encryption or "Shared Colors of Benetton"*, presented at EUROCRYPT '96 Rump Session. Available as `http://www.iacr.org/conferences/ec96/rump/preneel.ps`.

[15] E.R. Verheul and H.C.A. van Tilborg, *Constructions and Properties of k out of n visual secret sharing schemes,* submitted to Designs, Codes, and Cryptography.