Contrast Optimal Threshold Visual Cryptography Schemes

Carlo Blundo,[1,*] Paolo D'Arco,[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, paodar, ads}@dia.unisa.it

URL: http://www.dia.unisa.it/{~carblu/, ~paodar/, ~ads/}

[2] Department of Combinatorics and Optimization

University of Waterloo, Waterloo Ontario, N2L 3G1, Canada

E-mail: dstinson@uwaterloo.ca

URL: http://cacr.math.uwaterloo.ca/~stinson

November 16, 1999

Abstract

A (k, n)-threshold visual cryptography scheme ((k, n)-threshold VCS, for short) is a method to encode a secret image SI into n shadow images called shares such that any k or more shares enable the "visual" recovery of the secret image, but by inspecting less that k share one cannot gain any information on the secret image. The "visual" recovery consists of xeroxing the shares onto transparencies, and then stacking them. Any k shares will reveal the secret image without any cryptographic computation.

In this paper we analyze the contrast of the reconstructed image for (k, n)-threshold VCS. We define a canonical form for (k, n)-threshold VCS and we also provide a characterizazion of (k, n)-threshold VCS. We completely characterize contrast optimal $(n-1, n)$-threshold VCS in canonical form. Moreover, for $n \geq 4$, we provide, a contrast optimal $(3, n)$-threshold VCS in canonical form. We first describe a family of $(3, n)$-threshold VCS achieving various values of

*Research 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 partially supported by NSF grant CCR-9610138.

contrast and pixel expansion. Then, we prove an upper bound on the contrast of any $(3, n)$-threshold VCS and show that a scheme in the described family has optimal contrast. Finally, for $k = 4, 5$ we present two schemes with contrast asymptotically equal to $1/64$ and $1/256$, respectively.

1 Introduction

A (k, n)-threshold 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. Any (qualified) set of k or more participants can "visually" recover the secret image, but (forbidden) sets of participants of cardinality less that k 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. Visual cryptography schemes are characterized by two parameters: The *pixel expansion*, which is the number of subpixels each pixel of the original image is encoded into, and the *contrast* which measures the "difference" between a black and a white pixel in the reconstructed image.

This cryptographic paradigm was introduced by Naor and Shamir [12]. Further results on (k, n)-threshold visual cryptography schemes ((k, n)-threshold VCS, for short) can be found in [1, 3, 5, 7, 9, 16]. The model by Naor and Shamir has been extended in [1, 3] 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. Droste [7] gave an algorithm to construct (k, n)-threshold visual cryptography schemes. In [3] the authors provide the first construction for $(2, n)$-threshold VCS having the best possible contrast, for any $n \geq 2$. In [5], for any n, it is provided a complete characterization of $(2, n)$-threshold VCS having optimal contrast and minimum pixel expansion in terms of certain balanced incomplete block designs. In [9] the authors showed that by solving a suitable linear program one can compute the best contrast achievable in any (k, n)-threshold VCS. In [9], for the cases $k = 2$ with n even and $k = 3$ with n divisible by 4, it is described a (k, n)-threshold VCS achieving the best possible contrast.

For a simple and non-technical introduction to visual cryptography see [15].

In implementing visual cryptography schemes it would be useful to conceal the existence of the secret message, namely, the shares given to participants in the scheme should not look as a random bunch of pixels, but they should be innocent looking images (an house, a dog, a tree, ...). Naor and Shamir [12] first considered the problem of concealing the existence of the secret message for the case of 2 out of 2 threshold VCS. In [2] the authors gave a general technique to implement visual cryptography schemes with such an extended capability. Droste [7] also considered the problem of concealing the existence of the secret message and presented a technique to implement such schemes.

Alternative reconstruction methods for visual cryptography schemes based on "opaque" shares [13] and on polarized filters [4] have been recently proposed. Both models make assumptions different from ours on the way the shares combine. Visual cryptography schemes to encrypt coloured images are given in [10, 14, 16]. Recently, authentication and identification methods for human users based on visual cryptography have been considered [11]. In [6] the authors analyze the amount of randomness needed to visually share a secret image.

In this paper we analyze the contrast for (k, n)-threshold visual cryptography schemes. We are mainly interested in schemes achieving the maximum possible contrast for any fixed values of k and n. We refer to such schemes as *contrast optimal*. We define a canonical form for (k, n)-threshold VCS, and characterize (k, n)-threshold VCS (see Lemmas 3.9 and 3.10). We completely characterize contrast optimal $(n-1, n)$-threshold VCS in canonical form. Moreover, for $n \geq 4$, we present a contrast optimal $(3, n)$-threshold VCS in canonical form. We first describe a family of $(3, n)$-threshold VCS achieving various values of contrast and pixel expansion. Then, we prove an upper bound on the contrast of any $(3, n)$-threshold VCS and show that a scheme in the described family has optimal contrast. Finally, for $k = 4$ and 5 we present two schemes with contrast asymptotically equal to $1/64$ and $1/256$, respectively.

2 The Model

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 participants as black or as white according to some rule of contrast.

Definition 2.1 *Let k and n be two integers such that $k \leq n$ and let $\mathcal{P}$ be a set of n participants. Two collections (multisets) of $n \times m$ boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ constitute a* (k, n)-threshold visual cryptography scheme *with pixel expansion m if there exist the value α and the set $\{(X, t_X)\}_{X \subseteq \mathcal{P} : |X| = k}$ satisfying:*

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

2. Any (forbidden) set $X = \{i_1, i_2, \ldots, i_p\} \subseteq \mathcal{P}$, with $p < k$, 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 any k participants stack their transparencies they can correctly recover the image shared by the dealer. The value α is called *contrast* of the image and the set $\{(X, t_X)\}_{X \subseteq \mathcal{P}:|X|=k}$ is called the *set of thresholds*. (We use a slightly different terminology from [12] where the contrast is called relative difference and the quantity $\alpha \cdot m$ is referred to as the contrast of the scheme.) We want the product of the contrast times the pixels expansion to be as large as possible and at least one, that is, $\alpha \geq 1/m$. The second property is called *security*, since it implies that, even by inspecting all their shares, any set of less than k participants cannot gain any information in deciding whether the shared pixel was white or black.

Notice that if a set of participants X is a superset of a qualified set X', then they can recover the shared image by considering only the shares of the set X'. This does not in itself rule out the possibility that stacking all the transparencies of the participants in X does not reveal any information about the shared image. A *strong* (k, n)-threshold VCS is a (k, n)-threshold VCS in which Property 1 of Definition 2.1 is satisfied for any set X of cardinality at least k, that is, the image is visible if and only if k or *more* participants stack their transparencies.

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 of size k we associate a (possibly) different threshold t_X. Nevertheless, all the (k, n)-threshold VCS given in this paper have the property that for any $X, X' \subseteq \mathcal{P}$ with $|X| = |X'| \geq k$, it results that $t_X = t_{X'}$.

2.1 Basis Matrices

In this paper we consider only (k, n)-threshold 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, in Section 2.1 of [1] is has been shown how to obtain, from an arbitrary (k, n)-threshold VCS, a VCS having the same parameters m, α, and $\{(X, t_X)\}_{X \subseteq \mathcal{P}:|X|=k}$, with equally sized $\mathcal{C}_0$ and $\mathcal{C}_1$.

All 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 k and n be two integers such that $k \leq n$ and let $\mathcal{P}$ be a set of n participants. A (k,n)-threshold VCS with contrast α and set of thresholds $\{(X,t_X)\}_{X\subseteq\mathcal{P}:|X|=k}$ is realized using the two $n\times m$ basis matrices S^0 and S^1 if the following two conditions hold.*

1. *If $X=\{i_1,i_2,\ldots,i_k\}\subseteq\mathcal{P}$, (i.e., if X is a qualified set), then the "or" V of rows $i_1,i_2,\ldots,i_k$ of S^0 satisfies $w(V)\leq t_X-\alpha\cdot m$; whereas, for S^1 it results that $w(V)\geq t_X$.*

2. *If $X=\{i_1,i_2,\ldots,i_p\}\subseteq\mathcal{P}$ and $p<k$ (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 [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 Canonical (k,n)-threshold VCS

Most of the constructions found in literature for (k,n)-threshold VCS are realized by using basis matrices. Among these constructions there are a few having the property that all the columns of a given weight appear with the same multiplicity in the basis matrices (see, for instance, [12, 3, 1, 7, 5, 9, 16]). Because of the relevance of this property we review some of the constructions for (k,n)-threshold VCS having such a property.

- Naor and Shamir [12] proposed a (k,k)-threshold VCS which 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 k-vectors having an even number of '1's, and S^1 is the matrix whose columns are all the boolean k-vectors having an odd number of '1's. In [12] the basis matrices of $(2,n)$-threshold VCS are realized as follows: S^0 contains $n-1$ columns of weight 0 and one column of weight n; whereas, S^1 contains all the columns of weight 1. Naor and Shamir [12] also proposed a $(3,n)$-threshold VCS whose basis matrices are realized as follows: S^0 contains $n-2$ columns of weight zero and all the columns of weight $n-1$; whereas, S^1 contains all the columns of weight 1 and $n-2$ columns of weight n.

- In [3] the authors showed how to construct a $(2,n)$-threshold VCS which is optimal with respect to the contrast. The basis matrix S^1 of such scheme is realized by considering all the columns of weight $\lfloor n/2\rfloor$; whereas, the basis matrix S^0 contains $\binom{n-1}{\lfloor n/2 \rfloor}$ columns of weight zero and $\binom{n-1}{\lfloor n/2 \rfloor -1}$ columns of weight n.

- Droste [7] gave an algorithm to construct basis matrices of any (k,n)-threshold VCS. The basis matrices realized by such an algorithm are constructed by adding/deleting all the columns of particular weights to the basis matrices.

- Other (k,n)-threshold VCS in which all the columns of a given weight appear in the basis matrices can be found in [5]. For instance, when $k|n$, setting $\ell = n!/\left((n/k)!\right)^k$, we have that, for $j = 0, \ldots \lfloor k/2 \rfloor$, the basis matrix S^1 is realized by considering all the columns of weight $(2j+1)n/k$ each appearing with multiplicity ℓ and the basis matrix S^0 contains all the columns of weight $2jn/k$ each appearing with multiplicity ℓ.

- In [9] basis matrices containing all the columns of a given weight each occuring with the same frequency have been referred to as *totally symmetric* matrices. The authors analyzed (k,n)-threshold VCS having as basis matrices totally symmetric ones. They gave explicit constructions for $k = 2, 3, n$.

- In [16] the authors proposed two constructions for (k,n)-threshold VCS whose parameters are connected to notions in finite geometry and coding theory. The basis matrices derived from such constructions contain all the columns of a given weight.

In this section we consider basis matrices containing all the columns of a given weight each occuring with the same frequency with few additional properties (see Definition 3.1). We refer to such matrices as *canonical*. We show how to construct for any (k,n) threshold VCS a canonical scheme preserving the contrast. Since we are interested in optimizing the contrast, we focus our attention only on canonical form.

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 M be a matrix in the collection $\mathcal{C}_0 \cup \mathcal{C}_1$ of a (k,n)-threshold 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 $M[X] = M[X][\{1, \ldots, m\}]$ denotes the $|X| \times m$ matrix obtained from M by considering only the rows corresponding to participants in X. Let M be a matrix and let D be a sub-matrix of M having the same number of rows, with $M \backslash D$ we denote the matrix obtained from M by removing all the columns of the matrix D. For sets X and Y and for elements x and y, to avoid overburdening the notation, we will often write x for $\{x\}$, xy for $\{x, y\}$, xY for $\{x\} \cup Y$, and XY for $X \cup Y$. Let $\mathbf{c}$ be a boolean vector, with $\overline{\mathbf{c}}$ we denote the vector obtained from $\mathbf{c}$ by complementing all its entries; whereas, given a boolean matrix M with $\overline{M}$ we denote the matrix obtained from M by complementing all its entries. For $i = 0, 1$, with $f_{\mathbf{c},i}$ we denote the multiplicity of the column $\mathbf{c}$ in S^i, that is, $f_{\mathbf{c},i}$ is the number of times the column $\mathbf{c}$ appears in S^i.

By abusing of notation, we write $\mathbf{c} \in M$ to denote the fact that $\mathbf{c}$ is a column of the matrix M.

Definition 3.1 *Let (S^0, S^1) be the basis matrices of a (k,n)-threshold VCS. They are in* canonical *form if, for $i = 0, 1$, the following two properties are satisfied.*

1. *For any columns $\mathbf{c}$ and $\mathbf{c}'$ such that $w(\mathbf{c}) = w(\mathbf{c}')$, it results that $f_{\mathbf{c},i} = f_{\mathbf{c}',i}$.*

2. *For any column $\mathbf{c}$ it results that*

$$f_{\mathbf{c},i} = \begin{cases} f_{\overline{\mathbf{c}},i} & \text{if } k \text{ is even} \\ f_{\overline{\mathbf{c}},1-i} & \text{if } k \text{ is odd.} \end{cases}$$

A (k,n)-threshold VCS whose basis matrices are in canonical form is referred to as a *canonical (k,n)-threshold VCS.*

To prove some of our results we need the following theorem.

Theorem 3.2 ([5]) *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 (k,n)-threshold VCS with pixel expansion m and contrast α if and only if for all subsets X consisting of k rows there exist a boolean matrix $D[X]$ and an integer $z_X \geq \alpha \cdot m$ 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 z_X, and all the odd columns appear in $S^1[X] \backslash D[X]$ with multiplicity z_X.*

Theorem 3.2 follows directly from Theorem 7.1 of [5], and from Lemma 3.5 of [1]. More precisely, Theorem 7.1 of [5] establishes that a couple of basis matrices (T^0, T^1), such that the same column does not appear in both, realizes a (k,k) threshold VCS if and only if there is an integer h for which T^0 contains all the even columns with multiplicity h, and T^1 contains all the odd columns with the same multiplicity h. Since for any subset X of k rows, the restriction $(S^0[X], S^1[X])$ of (S^0, S^1) defines a couple of basis matrices realizing a (k,k)-VCS, then, from Lemma 3.5 of [1], $S^0[X]$ and $S^1[X]$ have the following structure: There is a matrix $D[X]$ and an integer z_X such that $D[X]$ is a submatrix of both $S^0[X]$ and $S^1[X]$, all the even columns appear in $S^0[X] \backslash D[X]$ with multiplicity z_X, and all the odd columns appear in $S^1[X] \backslash D[X]$ with the same multiplicity z_X.

Example 3.3 *Let*

$$S^0 = \left[\begin{array}{cccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right], \quad S^1 = \left[\begin{array}{cccccccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hline 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{array}\right]$$

be two basis matrices realizing a $(3,5)$ threshold VCS. If we consider the restrictions of these matrices to the first three rows, it is easy to see that $S^0[X]$ (resp. $S^1[X]$)

contains all the even (resp. odd) colums one time and the common matrix, up to a column permutation, is

$$D[X] = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

We will use the next lemma to prove that if there exists a (k,n)-threshold VCS with contrast α, then there exists a canonical (k,n)-threshold VCS having the same contrast α. A weaker version of the result stated by the next lemma was independently proved in [16, Theorem 5.7].

Lemma 3.4 *Let (S^0, S^1) be the basis matrices of a (k,n)-threshold VCS with pixel expansion m and contrast α. The matrices (B^0, B^1), defined as*

$$(B^0, B^1) = \begin{cases} (\overline{S^1}, \overline{S^0}) & \text{if } k \text{ is odd} \\ (\overline{S^0}, \overline{S^1}) & \text{if } k \text{ is even,} \end{cases}$$

are the basis matrices of a (k,n)-threshold VCS with pixel expansion m and contrast α.

Proof. Assume that k is odd and let $B^0 = \overline{S^1}$ and $B^1 = \overline{S^0}$. Since (S^0, S^1) are basis matrices of a (k,n)-threshold VCS, then, from Theorem 3.2, it results that for all subsets X consisting of k rows there exist a boolean matrix D^X and an integer $z_X \geq \alpha \cdot m$ 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 z_X, and all the odd columns appear in $S^1[X] \backslash D^X$ with multiplicity z_X. Hence, for all subsets X consisting of k rows there exist a boolean matrix $G^X = \overline{D^X}$ and an integer z_X such that G^X is a sub-matrix of both $B^0[X]$ and $B^1[X]$, all the even columns appear in $B^0[X] \backslash G^X$ with multiplicity z_X, and all the odd columns appear in $B^1[X] \backslash G^X$ with multiplicity z_X. Therefore, from Theorem 3.2, we get that (B^0, B^1) are basis matrices of a (k,n)-threshold VCS. It is immediate to see that the contrast of the (k,n)-threshold VCS having basis matrices (B^0, B^1) is the same as the contrast of the scheme we started with.
The proof for the case k even is analogous to the one for k odd. $\square$

In [5] it was shown that if there exists a (k,n)-threshold VCS Σ, realized using collections of $n \times m$ boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$, having contrast α, then there exists a (k,n)-threshold VCS realized by using basis matrices having the same contrast as Σ. We state this result as a lemma.

Lemma 3.5 *Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the collections of matrices of a (k,n)-threshold VCS with contrast α. Then, there exists a (k,n)-threshold VCS realized by using basis matrices having contrast α.*

Proof. Without loss of generality we can assume that $r = |\mathcal{C}_0| = |\mathcal{C}_1|$ (see Section 2.1 of [1]). Suppose that $\mathcal{C}_0 = \{M^{0,1}, \ldots, M^{0,r}\}$ and $\mathcal{C}_1 = \{M^{1,1}, \ldots, M^{1,r}\}$, where $\circ$ denotes the concatenation of two matrices. 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 contrast as Σ. $\square$

The next lemma holds.

Lemma 3.6 *Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the collections of matrices of a (k,n)-threshold VCS with contrast α. Then, there exists a canonical (k,n)-threshold VCS realized by basis matrices (S^0, S^1) having contrast α.*

Proof. Assume k odd. Let Σ be a (k,n)- threshold VCS with pixel expansion m and contrast α. Suppose that Σ is realized using collections of $n \times m$ boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$. By Lemma 3.5 there exists a (k,n)-threshold VCS realized by using basis matrices (S^0, S^1) having the same contrast α as Σ. For $i = 0, 1$, let $\mathcal{D}^i$ be the collection of boolean matrices obtained from S^i by permuting its rows. Now, construct a new pair of matrices D^0 and D^1 by concatenating all the matrices in $\mathcal{D}^0$ and $\mathcal{D}^1$, respectively. It is immediate to see that D^0 and D^1 constitute basis matrices of a (k,n)-threshold VCS having the same contrast as Σ. At this point, it results that if a column of weight w appeared in S^0 (S^1), then all the columns of weights w appears in D^0 (D^1). Finally, let $B^0 = \overline{D^1}$ and $B^1 = \overline{D^0}$. By Lemma 3.4, the pair (B^0, B^1) represents the basis matrices of a (k,n)-threshold VCS having contrast α. It is straightforward to check that $A^0 = B^0 \circ D^0$ and $A^1 = B^1 \circ D^1$ are the basis matrices of a canonical (k,n)-threshold VCS having contrast α.
The proof for the case k even is analogous to the one for k odd. $\square$

Notice that in [9] the authors considered totally symmetric matrices which satisfy only Property 1. of Definition 3.1 and they proved the analogous of Lemma 3.6.

In any canonical (k,n)-threshold VCS, by Property 1 of Definition 3.1, all the columns of a given weight appear with the same multiplicity. Therefore, we define the multiplicity of a column of weight j in S^i as $h_{j,i}$, i.e., $h_{j,i} = f_{\mathbf{c},i}$ if $w(\mathbf{c}) = j$. Hence, any canonical (k,n)-threshold VCS can be simply described by the pair of vectors $(h_{0,0}, \ldots, h_{n,0})$ and $(h_{0,1}, \ldots, h_{n,1})$. Clearly, the pixel expansion m of a canonical (k,n)-threshold VCS is equal to

$$m = \sum_{j=0}^{n} h_{j,0} \binom{n}{j} = \sum_{j=0}^{n} h_{j,1} \binom{n}{j}.$$

Moreover, it is easy to see that in a canonical (k,n)-threshold VCS, for any $X, X' \subseteq \mathcal{P}$, with $|X| = |X'| = k$, we have that $t_X = t_{X'}$ as in the original definition by Naor and Shamir [12]. This means also that the optimal contrast is the same in our definition as in the Naor Shamir's definition (however, the minimal pixel expansion need not be the same).

The next corollary is a consequence of Definition 3.1.

Corollary 3.7 *Let Σ be a (k,n)-threshold VCS in canonical form. If k is odd, then for $j = 0, \ldots, n$, it results that $h_{j,0} = h_{n-j,1}$; whereas, if k is even, for $j = 0, \ldots, n$, it results that $h_{j,0} = h_{n-j,0}$ and $h_{j,1} = h_{n-j,1}$.*

There is another equality relating the $h_{i,j}$'s which is based on the security of the (k,n)-threshold VCS. From Condition 2 of Definition 2.2 in [1], for $j = 0, \ldots, n$, it has to be that $w(S^0[j]) = w(S^1[j])$. From which one gets that

$$\sum_{i=1}^{n} h_{i,0}\binom{n-1}{i-1} = \sum_{i=1}^{n} h_{i,1}\binom{n-1}{i-1}.$$

Hence, in any canonical (k,n)-threshold VCS all the rows of the basis matrices have the same weight. The next corollary is an immediate consequence of previous observation and of Lemma 3.6.

Corollary 3.8 *The pixel expansion of any canonical (k,n)-threshold VCS is twice the weight of any row of a basis matrix.*

Proof. Suppose n is odd (n even) and let (S^0, S^1) be the basis matrices of a canonical (k,n)-threshold VCS. From Corollary 3.7 it results that $S^{1-i} = \overline{S^i}$ ($S^i = \overline{S^i}$), for $i = 0,1$. Hence, as in any canonical (k,n)-threshold VCS all the rows of the basis matrices have the same weight, we have that the weight of any row of a basis matrix is half of the pixel expansion of the scheme. □

Notice that if (A^0, A^1) and (B^0, B^1) are (k,n)-threshold VCS having contrast α, then $(A^0 \circ B^0, A^1 \circ B^1)$, where $\circ$ denotes the operator "concatenation" of two matrices, is a (k,n)-threshold VCS having contrast α. Hence, if $(h_{0,0}, \ldots, h_{n,0})$ and $(h_{0,1}, \ldots, h_{n,1})$ are a pair of vectors describing a canonical (k,n)-threshold VCS having contrast α, then, for any positive integer ℓ, the vectors $(\ell \cdot h_{0,0}, \ldots, \ell \cdot h_{n,0})$ and $(\ell \cdot h_{0,1}, \ldots, \ell \cdot h_{n,1})$ again describe a canonical (k,n)-threshold VCS having contrast α. Therefore, if we want to minimize the pixel expansion m for a given value of the contrast α, we consider values $h_{0,0}, \ldots, h_{n,0}, h_{0,1}, \ldots, h_{n,1}$ such that $\gcd(h_{0,0}, \ldots, h_{n,0}) = \gcd(h_{0,1}, \ldots, h_{n,1}) = 1$.

Suppose that $n \geq 2$ is an integer, and $2 \leq k \leq n$. For $i = 0,1$, let $h_i = (h_{0,i}, \ldots, h_{n,i})$ be an $(n+1)$-tuple of non-negative integers. For $i = 0,1$, define $S(h_i)$ to be the matrix in which every binary n-tuple of weight j occurs exactly $h_{j,i}$ times as a column ($0 \leq j \leq n$). In the following we provide a necessary and sufficient condition for the existence of (k,n)-threshold VCS realized by such matrices $S(h_0)$ and $S(h_1)$. The following lemma holds.

Lemma 3.9 *$S(h_0)$ and $S(h_1)$ are basis matrices of a (k,n)-threshold VCS with pixel expansion m and contrast α if and only if the following properties are satisfied:*

1. $\sum_{j=0}^{n} \binom{n}{j} h_{j,0} = \sum_{j=0}^{n} \binom{n}{j} h_{j,1} = m$.
2. $\sum_{j=p'}^{n-p+p'} \binom{n-p}{j-p'} h_{j,0} = \sum_{j=p'}^{n-p+p'} \binom{n-p}{j-p'} h_{j,1}$, *for* $1 \leq p \leq k-1$ *and* $0 \leq p' \leq p$,
3. $\sum_{j=0}^{n-k} \binom{n-k}{j} (h_{j,0} - h_{j,1}) = \alpha \cdot m$.

Proof. Suppose that $S(h_0)$ and $S(h_1)$ are basis matrices for a VCS with the stated parameters. The number of columns in $S(h_i)$ $(i = 0,1)$ is

$$\sum_{j=0}^{n} \binom{n}{j} h_{j,i}.$$

Therefore property 1 holds.

Next, let $\mathbf{c}$ be a binary column p-tuple, where $0 \leq p \leq k-1$. Suppose that the weight of $\mathbf{c}$ is p' (note that $p' \leq p$). Fix p rows of $S(h_0)$ and $S(h_1)$, say the first p rows. The number of occurrences of $\mathbf{c}$ as a column of $S(h_i)[\{1,\ldots,p\}]$ is

$$\sum_{j=p'}^{n-p+p'} \binom{n-p}{j-p'} h_{j,i},$$

for $i = 0, 1$. Therefore property 2. holds.

Finally, we look at the weight of the OR of k rows of $S(h_0)$ and $S(h_1)$, say the first k rows. If we let $X = \{1,\ldots,k\}$, then

$$w(S(h_1)_X) - w(S(h_0)_X) \geq \alpha \cdot m.$$

Let ϵ_i denote the number of occurrences of $(0,\ldots,0)^T$ as a column of $S(h_i)[X]$, for $i = 0, 1$. It is easy to see that

$$w(S(h_i)_X) = m - \epsilon_i,$$

for $i = 0, 1$. Hence,

$$w(S(h_i)_X) = m - \sum_{j=0}^{n-k} \binom{n-k}{j} h_{j,i},$$

for $i = 0, 1$. Therefore property 3. holds.

Conversely, if properties 1.–3. hold, it is easy to see that $S(h_0)$ and $S(h_1)$ are basis matrices for a VCS with the stated parameters. □

We can in fact simplify the statement of the above lemma, by observing that many of the conditions are redundant. More precisely, property 2 of Lemma 3.9 considers, for each $1 \leq p \leq k-1$, the restriction of the basis matrices to p rows, and requires that the same subcolumns appear with the same frequencies. However, we can simply check if the subcolumns of weight $1 \leq p' \leq k-1$ appears with the same frequencies in $S(h_0)$ and $S(h_1)$. Indeed, if this property is satisfied, the symmetric structure of the matrices, assures that any restriction of $S(h_0)$ and $S(h_1)$ to $1 \leq p \leq k-1$ rows contains the same subcolumns with the same frequencies.

From a mathematical point of view, by repeated application of Pascal's identity for binomial coefficients to property 2 of Lemma 3.9, we obtain the following equivalent formulation.

Lemma 3.10 *$S(h_0)$ and $S(h_1)$ are basis matrices of a (k,n)-threshold VCS with pixel expansion m and contrast α if and only if the following properties are satisfied:*

1. $\sum_{j=0}^{n} \binom{n}{j} h_{j,0} = \sum_{j=0}^{n} \binom{n}{j} h_{j,1} = m.$

2. *For* $1 \leq p' \leq k-1$, $\sum_{j=0}^{n-p'} \binom{n-p'}{j} h_{j,0} = \sum_{j=0}^{n-p'} \binom{n-p'}{j} h_{j,1}.$

3. $\sum_{j=0}^{n-k} \binom{n-k}{j} (h_{j,0} - h_{j,1}) = \alpha \cdot m.$

Example 3.11 Suppose $k = 2$ and $n = 4$. The following example is from [5]. Let $h_0 = (3, 0, 0, 0, 3)$ and let $h_1 = (0, 0, 1, 0, 0)$. This defines a $(2, 4)$ threshold VCS with $m = 6$ and contrast $\alpha = 1/3$:

$$\begin{aligned}
\sum_{j=0}^{4} \binom{4}{j} h_{j,0} &= \binom{4}{0} 3 + \binom{4}{4} 3 = 6 \\
\sum_{j=0}^{4} \binom{4}{j} h_{j,1} &= \binom{4}{2} 1 = 6 \\
\sum_{j=0}^{3} \binom{3}{j} h_{j,0} &= \binom{3}{0} 3 = 3 \\
\sum_{j=0}^{3} \binom{3}{j} h_{j,1} &= \binom{3}{2} 1 = 3 \\
\sum_{j=0}^{2} \binom{2}{j} (h_{j,0} - h_{j,1}) &= \binom{2}{0} 3 - \binom{2}{2} 1 = 2.
\end{aligned}$$

Example 3.12 Suppose $k = 3$ and $n = 7$. The following example is an application of a construction we give in Section 4.2. Let $h_0 = (9, 0, 0, 0, 0, 1, 0, 0)$ and let $h_1 = (0, 0, 1, 0, 0, 0, 0, 9)$. This defines a $(3, 7)$ threshold VCS with $m = 30$ and contrast $\alpha = 1/10$:

$$\begin{aligned}
\sum_{j=0}^{7} \binom{7}{j} h_{j,0} &= \binom{7}{0} 9 + \binom{7}{5} 1 = 30 \\
\sum_{j=0}^{7} \binom{7}{j} h_{j,1} &= \binom{7}{2} 1 + \binom{7}{7} 9 = 30 \\
\sum_{j=0}^{6} \binom{6}{j} h_{j,0} &= \binom{6}{0} 9 + \binom{6}{5} 1 = 15 \\
\sum_{j=0}^{6} \binom{6}{j} h_{j,1} &= \binom{6}{2} 1 = 15 \\
\sum_{j=0}^{5} \binom{5}{j} h_{j,0} &= \binom{5}{0} 9 + \binom{5}{5} 1 = 10 \\
\sum_{j=0}^{5} \binom{5}{j} h_{j,1} &= \binom{5}{2} 1 = 10 \\
\sum_{j=0}^{4} \binom{4}{j} (h_{j,0} - h_{j,1}) &= \binom{4}{0} 9 - \binom{4}{2} 1 = 3.
\end{aligned}$$

The characterization of (k, n)-threshold VCS provided by Lemma 3.10, because of Lemma 3.6, gives rise to a natural and simple formulation for computing their optimal contrast for any fixed n and k in terms of linear programming. We set $m = 1$ without loss of generality since α is unchanged if all the $h_{j,i}$'s are multiplied by a constant factor. The resulting LP has only $2n + 2$ variables.

Maximize:

$$\alpha = \sum_{j=0}^{n-k} \binom{n-k}{j} (h_{j,0} - h_{j,1})$$

Subject to:

$$\begin{array}{ll}
\displaystyle\sum_{j=0}^{n} \binom{n}{j} h_{j,0} = 1 & \\
\displaystyle\sum_{j=0}^{n} \binom{n}{j} h_{j,1} = 1 & \\
\displaystyle\sum_{j=0}^{n-p'} \binom{n-p'}{j} (h_{j,0} - h_{j,1}) = 0 & \text{for } p' = 1, \ldots, k-1 \\
h_{j,0} \geq 0 & \text{for } j = 0, \ldots, n \\
h_{j,1} \geq 0 & \text{for } j = 0, \ldots, n
\end{array}$$

It is worthwhile to notice that our linear program is equivalent to, but simpler than, the one given in [9]. In Appendix B are depicted tables whose entries have been filled in by solving the previous linear programming problem for $2 \leq k \leq n \leq 11$. Also in [9] are tabulated some values of the contrast.

We can further simplify the previous LP formulation taking into account Corollary 3.7. For odd values of k the LP formulation can be written as follows.

Maximize:

$$\alpha = \sum_{j=0}^{n-k} \binom{n-k}{j} (h_{j,0} - h_{n-j,0})$$

Subject to:

$$\begin{array}{ll}
\displaystyle\sum_{j=0}^{n} \binom{n}{j} h_{j,0} = 1 & \\
\displaystyle\sum_{j=0}^{n-p'} \binom{n-p'}{j} (h_{j,0} - h_{n-j,0}) = 0 & \text{for } p' = 1, \ldots, k-1 \\
h_{j,0} \geq 0 & \text{for } j = 0, \ldots, n
\end{array}$$

For even values of k the LP formulation can be obtained similarly. This new LP formulation is clearly simpler than the previous one as it uses only half of the variables and it reduces the number of constraints.

In view of Lemma 3.6, if we are interested in getting schemes with a given contrast or bound on the contrast itself, then we can restrict our attention to canonical (k,n)-threshold VCS. Therefore, henceforth, unless otherwise specified, all (k,n)-threshold VCS we consider/analyze are canonical (k,n)-threshold VCS.

4 Contrast Optimal (k,n)-threshold VCS

We recall that, for fixed values of k and n, a contrast optimal scheme is a scheme achieving the maximum possible contrast over all (k,n) threshold VCSs. Contrast optimal (k,n)-threshold VCSs for $k=2$ and $k=n$, have already extensively studied (see [5, 12]). It is interesting to point out that the basis matrices realizing the (k,k)-threshold VCSs described in [12], and the basis matrices of the first construction proposed in [5] for $(2,n)$-threshold VCSs are both in canonical form.

Notice that the same column cannot appear in both basis matrices of a contrast optimal (k,n)-threshold VCS. This property is easy to verify. Indeed, if the same column appears in both basis matrices, then by removing it we obtain a new scheme having a better contrast than the one we started with. This property implies the following fact.

Fact 4.1 *In any contrast optimal (k,n)-threshold VCS whose basis matrices are in canonical form, for $j=0,\ldots,n$ and $i=0,1$, it holds that,*

1. *If $h_{j,1-i}>0$, then $h_{j,i}=0$.*
2. *If k is even, then $h_{j,i}=h_{n-j,i}$.*
3. *If k is odd, then $h_{j,i}=h_{n-j,1-i}$.*

As a consequence of above fact and because of Corollary 3.7, we have that if n is even and k is odd then $h_{n/2,0}=h_{n/2,1}=0$.

4.1 Contrast Optimal $(n-1,n)$-threshold VCS

In this section we characterize contrast optimal $(n-1,n)$-threshold VCS whose basis matrices are in canonical form.

The next lemma holds.

Lemma 4.2 *Let $n\geq 3$. In any contrast optimal $(n-1,n)$-threshold VCS whose basis matrices are in canonical form, the $h_{j,i}$'s satisfy:*

1. *$h_{j,0}>0$ if and only if either $j<n/2$ and j is even or $j>n/2$ and j is odd.*
2. *$h_{j,1}>0$ if and only if either $j<n/2$ and j is odd or $j>n/2$ and j is even.*

Proof. Let (S^0,S^1) be the basis matrices of a canonical $(n-1,n)$-threshold VCS which is contrast optimal. It holds that:

$$\begin{array}{c}\text{If } j \text{ is odd and } h_{j,1}=0, \text{ then } h_{j+1,1}>0;\\ \text{whereas, if } j \text{ is even and } h_{j,0}=0, \text{ then } h_{j+1,0}>0.\end{array}\tag{1}$$

Would it be otherwise we have $h_{j,1}=h_{j+1,1}=0$ which is impossible as, by Theorem 3.2, all the columns of weight j have to appear among the columns of $S^1[X]$, where X is a subset of $\{1,\ldots,n\}$ of cardinality $n-1$. Similarly, we can prove that if

j is even and $h_{j,0} = 0$, then it holds that $h_{j+1,0} > 0$.
We will prove that for any integer $j < n/2$ it holds that:

$$\textit{If } j \textit{ is even, then } h_{j,0} > 0\textit{; whereas, if } j \textit{ is odd, then } h_{j,1} > 0. \qquad (2)$$

Therefore, applying Corollary 3.7, the lemma holds.
Now assume that n is even and $j < n/2$. Suppose by contradiction that $h_{j,0} = 0$. From (1) and by Fact 4.1 we have $h_{j+1,0} > 0$ and $h_{j+1,1} = 0$. Applying again (1) and Fact 4.1 we get $h_{j+2,1} > 0$ and $h_{j+2,0} = 0$. Iterating the previous argument we get that either $h_{n/2,0} > 0$ or $h_{n/2,1} > 0$ depending on whether $n/2$ is even or odd which is a contradiction (recall that $h_{n/2,0} = h_{n/2,1} = 0$). If j is odd, then we repeat the proof for the case j even, *mutatis mutandis.*
If n is odd, then by Corollary 3.7 we have that $h_{(n-1)/2,i} = h_{(n+1)/2,i}$, where $i = 0, 1$. At this point we repeat the proof for the case n even, *mutatis mutandis.* We get that either $h_{(n-1)/2,0} = 0$ and $h_{(n+1)/2,0} > 0$ or $h_{(n-1)/2,1} = 0$ and $h_{(n+1)/2,1} > 0$ which is a contradiction. Thus, the lemma holds. $\square$

The next lemma states the exact value of the $h_{j,i}$ of any contrast optimal $(n-1, n)$-threshold VCS whose basis matrices are in canonical form.

Lemma 4.3 *Let $n \geq 3$. In any contrast optimal $(n-1, n)$-threshold VCS whose basis matrices are in canonical form, the $h_{j,i}$'s satisfy:*

- *If n is even, then for $j = 0, \ldots, \lfloor (n-2)/4 \rfloor$, we have $h_{2j,0} = h_{n-2j,1} = \frac{n}{2} - 2j$; whereas, for $j = 0, \ldots, \lfloor (n-4)/4 \rfloor$, we have $h_{2j+1,1} = h_{n-(2j+1),0} = \frac{n}{2} - (2j+1)$.*
- *If n is odd, then for $j = 0, \ldots, \lfloor n/4 \rfloor$, we have $h_{2j,0} = h_{n-2j,0} = n - 4j$; whereas, for $j = 0, \ldots, \lceil (n-5)/4 \rceil$, we have $h_{2j+1,1} = h_{n-(2j+1),1} = n - (4j+2)$.*

Proof. Let Σ be a contrast optimal $(n-1, n)$-threshold VCS. Let (S^0, S^1) be the $n \times m$ basis matrices of Σ and let α be its contrast. Let X be a subset of $\{1, \ldots, n\}$ of cardinality $n-1$ and let $\mathbf{c}$ be a column of weight j, where $n/2 \leq j < n$. Suppose j is even. According to Theorem 3.2, the column $\mathbf{c}$ has to appear at least $\alpha \cdot m$ times more in $S^0[X]$ than in $S^1[X]$. Therefore, since Σ is contrast optimal, by Lemma 4.2 we have that $h_{j+1,0} - h_{j,1} = \alpha \cdot m$. A similar argument applies when j is odd. In this case we obtain $h_{j+1,1} - h_{j,0} = \alpha \cdot m$. For n even, recalling Lemma 4.2 and setting, w.l.o.g., $\alpha \cdot m = 1$, we get the following $n/2$ linear equations in n unknowns

$$\begin{array}{rcll} h_{n-2j,1} - h_{n-(2j+1),0} & = & 1 & \text{for } j = 0, \ldots, \lfloor (n-2)/4 \rfloor \\ h_{n-(2j+1),0} - h_{n-(2j+2),1} & = & 1 & \text{for } j = 0, \ldots, \lfloor (n-4)/4 \rfloor \end{array} \qquad (3)$$

Summing up equations (3) and recalling that $h_{n/2,0} = h_{n/2,1} = 0$, we get that $h_n = n/2$ from which we can compute the value of the other unknowns. Therefore, we obtain that if n is even, then for $j = 0, \ldots, \lfloor (n-2)/4 \rfloor$, we have $h_{2j,0} = h_{n-2j,1} = \frac{n}{2} - 2j$; whereas, for $j = 0, \ldots, \lfloor (n-4)/4 \rfloor$, we have $h_{2j+1,1} = h_{n-(2j+1),0} = \frac{n}{2} - (2j+1)$.
If n is odd, then we set $\alpha \cdot m = 2$ and we repeat the proof for the case n even, *mutatis mutandis.* $\square$

The results of the above lemma can be summarized as follows: If n is even, then, for $j = 0, \ldots, n$,

$$h_{j,0} = h_{n-j,1} = \begin{cases} \frac{n}{2} - j & \text{if } j \text{ is even and } j < n/2 \\ j - \frac{n}{2} & \text{if } j \text{ is odd and } j > n/2 \\ 0 & \text{otherwise.} \end{cases}$$

If n is odd, then, for $j = 0, \ldots, \lfloor n/2 \rfloor$,

$$h_{j,0} = h_{n-j,0} = \begin{cases} n - 2j & \text{if } j \text{ is even and } j < n/2 \\ 0 & \text{otherwise.} \end{cases}$$

and

$$h_{j,1} = h_{n-j,1} = \begin{cases} n - 2j & \text{if } j \text{ is odd and } j < n/2 \\ 0 & \text{otherwise.} \end{cases}$$

The next lemma holds.

Lemma 4.4 *For any $n \geq 3$ and for any contrast optimal canonical $(n-1, n)$-threshold VCS the pixel expansion m is given by*

$$m = \begin{cases} \frac{n}{4}\binom{n}{n/2} & \text{if } n \text{ is even} \\ n\binom{n-1}{(n-1)/2} & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Assume n is even. We have that,

$$\begin{aligned} m &= \sum_{j=0}^{n} h_{j,0}\binom{n}{j} \\ &= \sum_{j=0}^{\lfloor (n-2)/4 \rfloor} \left(\frac{n}{2} - 2j\right)\binom{n}{2j} + \sum_{j=0}^{\lfloor (n-4)/4 \rfloor} \left(\frac{n}{2} - (2j+1)\right)\binom{n}{2j+1} \\ &= \sum_{j=0}^{n/2-1} \left(\frac{n}{2} - j\right)\binom{n}{j} \end{aligned}$$

Since for any even integer r and any integer g it holds that, see [8, pag. 166],

$$\sum_{j=0}^{g} \left(\frac{r}{2} - j\right)\binom{r}{j} = \frac{g+1}{2}\binom{r}{g+1}.$$

then,

$$m = \frac{n}{4}\binom{n}{n/2}.$$

On the other hand, if n is odd, then

$$m = \sum_{j=0}^{n} h_{j,0}\binom{n}{j} = 2\sum_{j=0}^{\lfloor n/4 \rfloor} (n - 4j)\binom{n}{2j}.$$

We begin by simplifying the sum as follows:

$$\begin{aligned}
\sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}(n-4j)\binom{n}{2j} &= \sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\left((n-2j)\binom{n}{n-2j} - 2j\binom{n}{2j}\right) \\
&= \sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\left(n\binom{n-1}{n-2j-1} - n\binom{n-1}{2j-1}\right) \\
&= n\left(\sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2j} - \sum_{j=1}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2j-1}\right).
\end{aligned}$$

Recall that

$$\sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor}\binom{n-1}{2j} = \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor}\binom{n-1}{2j-1} = 2^{n-2}$$

for any positive integer n. Suppose $n \equiv 1 \bmod 4$. Then we have the following:

$$\begin{aligned}
\sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor}\binom{n-1}{2j} &= \sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2j} + \sum_{j=\lfloor \frac{n}{4} \rfloor}^{\lfloor \frac{n-1}{2} \rfloor}\binom{n-1}{2j} - \binom{n-1}{\frac{n-1}{2}} \\
&= \sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2j} + \sum_{i=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2\left(\lfloor \frac{n}{4} \rfloor + i\right)} - \binom{n-1}{\frac{n-1}{2}} \\
&= \sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2j} + \sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{n-1-2j} - \binom{n-1}{\frac{n-1}{2}} \\
&= 2\sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2j} - \binom{n-1}{\frac{n-1}{2}}
\end{aligned}$$

Suppose $n \equiv 3 \bmod 4$. Then we have the following:

$$\begin{aligned}
\sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor}\binom{n-1}{2j} &= \sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2j} + \sum_{j=\lfloor \frac{n}{4} \rfloor+1}^{\lfloor \frac{n-1}{2} \rfloor}\binom{n-1}{2j} \\
&= \sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2j} + \sum_{i=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2\left(\lfloor \frac{n}{4} \rfloor + 1 + i\right)} \\
&= \sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2j} + \sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{n-2j} \\
&= 2\sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2j}
\end{aligned}$$

Therefore, for n odd we have

$$\sum_{j=0}^{\lfloor \frac{n}{4} \rfloor}\binom{n-1}{2j} = \begin{cases} \frac{1}{2}\left(2^{n-2} + \binom{n-1}{\frac{n-1}{2}}\right) & \text{if } n \equiv 1 \bmod 4 \\ \frac{1}{2}\left(2^{n-2}\right) & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

Similarly,

$$\sum_{j=1}^{\lfloor\frac{n}{4}\rfloor}\binom{n-1}{2j-1} = \begin{cases} \frac{1}{2}\left(2^{n-2}\right) & \text{if } n \equiv 1 \bmod 4 \\ \frac{1}{2}\left(2^{n-2} - \binom{n-1}{\frac{n-1}{2}}\right) & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

Hence, for n odd,

$$\sum_{j=0}^{\lfloor\frac{n}{4}\rfloor}(n-4j)\binom{n}{2j} \quad = \quad \frac{n}{2}\binom{n-1}{\frac{n-1}{2}}.$$

Thus, the theorem holds. $\square$

Theorem 4.5 *For any $n \geq 3$ and for any canonical $(n-1,n)$-threshold VCS the maximum contrast α is given by*

$$\alpha = \begin{cases} \left[\frac{n}{4}\binom{n}{n/2}\right]^{-1} & \textit{if } n \textit{ is even} \\ \left[\frac{n}{2}\binom{n-1}{(n-1)/2}\right]^{-1} & \textit{if } n \textit{ is odd.} \end{cases}$$

Proof. In the proof of Lemma 4.3, to compute the value of the $h_{j,i}$'s of any contrast optimal $(n-1,n)$-threshold VCS, for n even, we set $\alpha \cdot m = 1$; whereas for n odd, we set $\alpha \cdot m = 2$. Therefore, applying Lemma 4.4 the theorem holds. $\square$

It is worthwhile to notice that according to the previous lemma one has that in any contrast optimal $(n-1,n)$-threshold VCS $\alpha = \Theta(2^{-n}n^{-1/2})$. This is a lower contrast than an (n,n)-threshold VCS.

4.2 Contrast Optimal $(3,n)$-threshold VCS

In this section we provide, for $n \geq 4$, a contrast optimal $(3,n)$-threshold VCS which is also strong and has its basis matrices in canonical form. We first describe a family of $(3,n)$-threshold VCS achieving various values of contrast and pixel expansion. Then, for any fixed $n \geq 4$, we determine the scheme in this family having the best contrast. Finally, we prove that the scheme has optimal contrast among all $(3,n)$-threshold VCS by proving an upper bound on the contrast of any $(3,n)$-threshold VCS.

For any $n \geq 4$ and any integer $1 \leq g < n/2$, consider the visual cryptography scheme whose basis matrices are in canonical form, denoted by $\mathcal{S}(3,n,g)$, described by the following $h_{j,i}$'s.

$$h_{0,0} = h_{n,1} = \binom{n-1}{g} - \binom{n-1}{g-1} \quad \text{and} \quad h_{n-g,0} = h_{g,1} = 1 \tag{4}$$

whereas all the remaining $h_{j,i}$'s are equal to zero. This is a strong $(3,n)$-threshold VCS as shown by the Theorem 4.7.

Example 4.6 *If $n = 5$, then g can be either 1 or 2. Let $g = 1$. Then, $h_{0,0} = h_{5,1} = \binom{5-1}{1} - \binom{5-1}{1-1} = 3$, and $h_{4,0} = h_{1,1} = 1$. The corresponding basis matrices are,*

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

Let $g = 2$. Then, $h_{0,0} = h_{5,1} = \binom{5-1}{2} - \binom{5-1}{2-1} = 2$, and $h_{3,0} = h_{2,1} = 1$. The corresponding basis matrices are,

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

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

Theorem 4.7 *For any $n \geq 4$ and any integer $1 \leq g < n/2$, the scheme $\mathcal{S}(3, n, g)$ described by (4) is a strong $(3, n)$-threshold VCS having pixel expansion and contrast equal to*

$$m = 2\binom{n-1}{g} \quad \text{and} \quad \alpha = \frac{g(n-2g)}{2(n-1)(n-2)},$$

respectively.

Proof. Let $h_i = (h_{0,i}, \ldots, h_{n,i})$, for $i = 0, 1$, where the $h_{j,i}$'s are given by (4) and let $S_g(h_0)$ and $S_g(h_1)$ be binary matrices in which, for $i = 0, 1$, every binary n-tuple of weight j occurs exactly $h_{j,i}$ times as a column of $S_g(h_i)$. Then, $S_g(h_0)$ and $S_g(h_1)$ satisfy the conditions of Lemma 3.10, where

$$\alpha = \frac{\binom{n-3}{g-1} - \binom{n-3}{g-2}}{2\binom{n-1}{g}} = \frac{g(n-2g)}{2(n-1)(n-2)} \quad \text{and} \quad m = 2\binom{n-1}{g}. \tag{5}$$

Indeed, it is immediate to verify that

$$\sum_{j=0}^{n} \binom{n}{j} h_{j,0} = \binom{n-1}{g} - \binom{n-1}{g-1} + \binom{n}{n-g} = 2\binom{n-1}{g}$$

and

$$\sum_{j=0}^{n} \binom{n}{j} h_{j,1} = \binom{n}{g} + \binom{n-1}{g} - \binom{n-1}{g-1} = 2\binom{n-1}{g}.$$

Hence, Condition 1 of Lemma 3.10 is satisfied. Condition 2 is also satisfied because of

$$\sum_{j=0}^{n-1} \binom{n-1}{j} h_{j,0} = \binom{n-1}{g} - \binom{n-1}{g-1} + \binom{n-1}{n-g} = \binom{n-1}{g} = \sum_{j=0}^{n-1} \binom{n-1}{j} h_{j,1};$$

and

$$\begin{aligned}\sum_{j=0}^{n-2} \binom{n-2}{j} h_{j,0} = \binom{n-1}{g} - \binom{n-1}{g-1} + \binom{n-2}{n-g} &= \binom{n-1}{g} - \binom{n-2}{g-1} \\ &= \binom{n-2}{g} = \sum_{j=0}^{n-2} \binom{n-2}{j} h_{j,1}.\end{aligned}$$

Now, we prove that Condition 3 of Lemma 3.10 is satisfied, where α and m are as given by (5). We have that

$$\begin{aligned}\sum_{j=0}^{n-3} \binom{n-3}{j} (h_{j,0} - h_{j,1}) &= \binom{n-1}{g} - \binom{n-1}{g-1} - \binom{n-3}{g} + \binom{n-3}{n-g} \\ &= \binom{n-2}{g} + \binom{n-2}{g-1} - \binom{n-1}{g-1} - \binom{n-3}{g} + \binom{n-3}{g-3} \\ &= \binom{n-3}{g-1} - \binom{n-2}{g-2} + \binom{n-3}{g-3} \\ &= \binom{n-3}{g-1} - \binom{n-3}{g-2} = \alpha \cdot m.\end{aligned}$$

This proves that Condition 3 of Lemma 3.10 holds.
Finally, we prove that the scheme $\mathcal{S}(3, n, g)$ is strong. For any $3 \leq \ell \leq n$ and for any $Y \subseteq \{1, \ldots, n\}$ such that $|Y| = \ell$, the number of zero columns in $S_g(h_0)[Y]$ ($S_g(h_1)[Y]$) does not depend on the particular set Y, but only on its size ℓ since the basis matrices are in canonical form. Hence, we refer to such a quantity as χ_ℓ^0 (χ_ℓ^1). We have that

$$\chi_\ell^0 = \binom{n-1}{g} - \binom{n-1}{g-1} + \binom{n-\ell}{n-g} \quad \text{and} \quad \chi_\ell^1 = \binom{n-\ell}{g}.$$

Notice that when $\ell > g$, then $\binom{n-\ell}{n-g} = 0$; whereas, $\binom{n-\ell}{g} = 0$ when $g > n - \ell$. We define the function $\beta(\ell)$, for $3 \leq \ell \leq n$, as $\beta(\ell) \triangleq \chi_\ell^0 - \chi_\ell^1$, that is,

$$\beta(\ell) = \binom{n-1}{g} - \binom{n-1}{g-1} + \binom{n-\ell}{n-g} - \binom{n-\ell}{g}.$$

To prove that the scheme is strong it is enough to show that $\beta(\ell) \geq \alpha \cdot m$, for $3 \leq \ell \leq n$. We next show that the function $\beta(\ell)$ is non decreasing, by proving that

$\beta(\ell+1)-\beta(\ell) \geq 0$. Indeed, this difference can be written as

$$\begin{aligned}
\beta(\ell+1)-\beta(\ell) &= \binom{n-\ell-1}{n-g} - \binom{n-\ell}{n-g} + \binom{n-\ell}{g} - \binom{n-\ell-1}{g} \\
&= \binom{n-\ell-1}{g-1} - \binom{n-\ell-1}{n-g-1} \\
&= \binom{n-\ell-1}{g-1} - \binom{n-\ell-1}{g-\ell}.
\end{aligned}$$

Notice that if $\ell > g$, then $\binom{n-\ell-1}{g-\ell} = 0$ and $\beta(\ell+1)-\beta(\ell) \geq 0$. Assume $\ell = g$. Then $\beta(\ell+1)-\beta(\ell) = \binom{n-\ell-1}{g-1} - 1$. Since $g < n/2$ and $\ell = g$, then $g-1 \leq n-\ell-1$. Thus, $\beta(\ell+1)-\beta(\ell) \geq 0$. Finally, assume $\ell < g$. Then

$$\begin{aligned}
\beta(\ell+1)-\beta(\ell) &= \frac{(n-\ell-1)!}{(g-1)!\cdot(n-\ell-g)!} - \frac{(n-\ell-1)!}{(g-\ell)!\cdot(n-g-1)!} \\
&= \frac{(n-\ell-1)!}{(g-\ell)!\cdot(n-\ell-g)!} \cdot \frac{\Pi_{j=1}^{\ell-1}(n-g-j) - \Pi_{j=1}^{\ell-1}(g-j)}{\Pi_{j=1}^{\ell-1}(n-g-j)\cdot(g-j)}.
\end{aligned}$$

The above quantity is non-negative, as $n-g-j \geq g-j$ for $g \leq n/2$. Therefore, the function $\beta(\ell)$ is a non decreasing function. Hence, since $\beta(3) \geq \alpha \cdot m$, the scheme $\mathcal{S}(3,n,g)$ is strong. □

From the arguments used in the proof of the above theorem one can see that by stacking together more than three transparencies from the scheme $\mathcal{S}(3,n,g)$, the image we recover becomes more visible (i.e., the difference between a white and a black pixel is larger when we stack together more than three transparencies). When we stack $n-g < \ell \leq n$ transparencies we have that $\beta(\ell) = \binom{n-1}{g} - \binom{n-1}{g-1}$. Since $m = 2\binom{n-1}{g}$, we get that the "contrast" in this case is equal to

$$\frac{\beta(\ell)}{m} = \frac{\binom{n-1}{g} - \binom{n-1}{g-1}}{2\binom{n-1}{g}} = \frac{n-2g}{2(n-g)}.$$

Notice that, for fixed n, the contrast of the scheme given by Theorem 4.7 depends only on the parameter g. Hence, the scheme achieving the best contrast among the schemes $\mathcal{S}(3,n,g)$ is obtained by choosing the integer g in the interval $[1, n/2[$, in such a way that the quantity $(n-2g)g$ is maximized. For real g the function $(n-2g)g$ is convex $\cap$ and reaches its maximum at $g = n/4$. Since g has to be an integer, a simple algebra shows that the quantity $(n-2g)g$ reaches its maximum at $g = \lfloor (n+1)/4 \rfloor$. Thus, for any $n \geq 4$, the following $h_{j,i}$'s describe a strong $(3,n)$-threshold VCS achieving the best contrast among the family of schemes $\mathcal{S}(3,n,g)$.

$$h_{0,0} = h_{n,1} = \binom{n-1}{\lfloor \frac{n+1}{4} \rfloor} - \binom{n-1}{\lfloor \frac{n+1}{4} \rfloor - 1} \qquad \text{and} \qquad h_{n-\lfloor \frac{n+1}{4} \rfloor,0} = h_{\lfloor \frac{n+1}{4} \rfloor,1} = 1, \quad (6)$$

whereas all the remaining $h_{j,i}$'s are equal to zero. The contrast of the scheme described by the above $h_{j,i}$'s is equal to

$$\frac{\left(n - 2\lfloor\frac{n+1}{4}\rfloor\right)\lfloor\frac{n+1}{4}\rfloor}{2(n-1)(n-2)}. \tag{7}$$

We now show that the schemes described by (6) is indeed a contrast optimal $(3, n)$-threshold VCS.

Theorem 4.8 *Let $n \geq 4$. In any $(3, n)$-threshold visual cryptography scheme it holds that*

$$\alpha \leq \frac{\left(n - 2\lfloor\frac{n+1}{4}\rfloor\right)\lfloor\frac{n+1}{4}\rfloor}{2(n-1)(n-2)}.$$

Proof. Let S^0 and S^1 be the $n \times m$ basis matrices in canonical form of a $(3, n)$-threshold VCS with contrast α. Since our aim is to prove an upper bound on the contrast we do not loose of generality in considering basis matrices in such a form (see Lemma 3.6). Let $T = \{2, \ldots, n\}$ and $Z_i = \{j : S^i[1][j] = 0\}$, that is, Z_i denotes the set of indices of columns of S^i having a zero as first entry. Finally, let $A^0 = S^0[T][Z_0]$ and $A^1 = S^1[T][Z_1]$. In other words, the pair of matrices $A = (A^0, A^1)$ is constituted by the sub-matrices of S^0 and S^1 obtained by removing all the columns having a one as first entry and removing the first row. Hence, up to a column permutation, the basis matrices S^0 and S^1 are of the following form:

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

where B^0 and B^1 are boolean matrices. It is known (see Theorem 6.1 and Corollary 6.2 of [5]) that A^0 and A^1 are basis matrices of a $(2, n-1)$-threshold VCS. Now, denote by $\alpha(A)$ the contrast of the $(2, n-1)$-threshold VCS with basis matrices (A^0, A^1). Since by Corollary 3.8 $m = 2w(S^0[1])$, then it is easy to see that the contrast α of the scheme represented by (S^0, S^1) is equal to

$$\alpha = \frac{\alpha(A)}{2}, \tag{8}$$

while the pixel expansion is equal to $m = 2m'$, where m' is the pixel expansion of the scheme having basis matrices (A^0, A^1), that is, $m' = \sum_{j \in J} h_{j,1}\binom{n-1}{j}$, where J is the set of indices j for which $h_{j,1} > 0$ and $j < n$ in A^1. Let X be a set of two rows, we have that

$$\alpha(A) \leq \frac{w(A^1_X) - w(A^0_X)}{m'},$$

Since $w(A^1[i]) = w(A^0[i])$, for $i = 1, \ldots, n-1$, we have that $w(A^1_X) - w(A^0_X)$ is equal to the number of columns $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ in $A^1[X]$ minus the number of columns $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ in $A^0[X]$.

Therefore, we get that

$$\begin{aligned} w(A^1_X) - w(A^0_X) &= \sum_{j\in J}\left[h_{j,1}\binom{n-3}{j-1} - h_{n-j,0}\binom{n-3}{n-j-1}\right] \\ &= \sum_{j\in J} h_{j,1}\left[\binom{n-3}{j-1} - \binom{n-3}{j-2}\right]. \end{aligned}$$

Hence,

$$\alpha(A) \le \frac{\sum_{j\in J} h_{j,1}\left[\binom{n-3}{j-1} - \binom{n-3}{j-2}\right]}{\sum_{j\in J} h_{j,1}\binom{n-1}{j}}. \tag{9}$$

Notice that for any function $g(x)$, for any positive function $f(x)$, and for any non empty set D which is a subset of both functions' domain, it holds that

$$\frac{\sum_{x\in D} g(x)}{\sum_{x\in D} f(x)} \le \max_{x\in D}\frac{g(x)}{f(x)}.$$

Therefore, since $J \subseteq \{0,\ldots,n-1\}$, we have that

$$\frac{\sum_{j\in J} h_{j,1}\left[\binom{n-3}{j-1} - \binom{n-3}{j-2}\right]}{\sum_{j\in J} h_{j,1}\binom{n-1}{j}} \le \max_{j\in J}\frac{\binom{n-3}{j-1} - \binom{n-3}{j-2}}{\binom{n-1}{j}} = \max_{j\in J}\frac{(n-2j)j}{(n-1)(n-2)}.$$

We have already seen earlier in this section that the function $(n-2j)j$ reaches its maximum over the integers $j \in \{0,\ldots,n-1\}$ at $j = \lfloor (n+1)/4 \rfloor$. Therefore,

$$\alpha(A) \le \frac{\left(n - 2\lfloor \frac{n+1}{4} \rfloor\right)\lfloor \frac{n+1}{4} \rfloor}{(n-1)(n-2)}.$$

The theorem then follows by (8). $\square$

Let $\alpha_3(n)$ be the expression (7). It is easy to see that $\lim_{n\to\infty} \alpha_3(n) = 1/16$. Therefore, the construction for $(3,n)$-threshold VCS given at the end of Section 5 in [5] has nearly optimal contrast asymptotically, as well as a small pixel expansion.

5 A Canonical $(4, n)$-threshold VCS

In this section we provide, for $n \ge 4$, a class of strong $(4,n)$-threshold VCS whose basis matrices are in canonical form. We first describe a family of $(4,n)$-threshold VCS achieving various values of contrast and pixel expansion. Then, for any fixed $n \ge 4$, we determine the scheme in this family having the best contrast.

For any even $n \geq 4$ and any integer $1 \leq g < n/2$, consider the visual cryptography scheme whose basis matrices are in canonical form, denoted by $\mathcal{S}(4, n, g)$, described by the following $h_{j,i}$'s

$$\begin{array}{c} h_{0,0} = h_{n,0} = \binom{n-3}{n/2-1} \frac{t_{n,g}(n-1)(n-2g)^2}{ng(n-g)}, \\ h_{n/2,0} = t_{n,g}, \quad \text{and} \quad h_{g,1} = h_{n-g,1} = \frac{\binom{n-3}{n/2-1}}{\binom{n-2}{g-1}} \cdot t_{n,g} \end{array} \tag{10}$$

where $t_{n,g} = \binom{n-2}{g-1} / \gcd\left\{\binom{n-2}{g-1}, \binom{n-3}{n/2-1}\right\}$ and all the remaining $h_{j,i}$'s are equal to zero. This is a strong $(4, n)$-threshold VCS as shown by the following theorem.

Theorem 5.1 *For any even integer $n \geq 4$ and any integer $1 \leq g < n/2$, the scheme $\mathcal{S}(4, n, g)$ is a strong $(4, n)$-threshold VCS having pixel expansion and contrast equal to*

$$m = \frac{2nt_{n,g}(n-1)}{g(n-g)} \binom{n-3}{n/2-1} \quad \text{and} \quad \alpha = \frac{g(n-g)(n-2g)^2}{4n(n-1)(n-2)(n-3)},$$

respectively.

Proof. Let $h_i = (h_{0,i}, \ldots, h_{n,i})$, for $i = 0, 1$, where the $h_{j,i}$'s are given by (10) and let $S_g(h_0)$ and $S_g(h_1)$ be binary matrices in which, for $i = 0, 1$, every binary n-tuple of weight j occurs exactly $h_{j,i}$ times as a column of $S_g(h_i)$. Then, $S_g(h_0)$ and $S_g(h_1)$ satisfy the conditions of Lemma 3.10. Indeed, it is immediate to verify that

$$\begin{aligned} \sum_{j=0}^{n} \binom{n}{j} h_{j,0} &= \left[2\binom{n-3}{n/2-1} \frac{(n-1)(n-2g)^2}{ng(n-g)} + \binom{n}{n/2}\right] t_{n,g} \\ &= \binom{n-3}{n/2-1} \left[\frac{2(n-1)(n-2g)^2}{ng(n-g)} + \frac{8n(n-1)(n-2)}{n^2(n-2)}\right] t_{n,g} \\ &= \frac{2nt_{n,g}(n-1)}{g(n-g)} \binom{n-3}{n/2-1} \end{aligned}$$

and

$$\sum_{j=0}^{n} \binom{n}{j} h_{j,1} = \frac{\binom{n-3}{n/2-1}}{\binom{n-2}{g-1}} \binom{n}{g} t_{n,g} + \frac{\binom{n-3}{n/2-1}}{\binom{n-2}{g-1}} \binom{n}{n-g} t_{n,g} = \frac{2nt_{n,g}(n-1)}{g(n-g)} \binom{n-3}{n/2-1}.$$

Hence, Condition 1 of Lemma 3.10 is satisfied. To prove that Condition 2 of Lemma 3.10 is satisfied we have to show that, for $\ell = 1, 2, 3$, the following identity holds

$$\sum_{j=0}^{n-\ell} \binom{n-\ell}{j} h_{j,0} = \sum_{j=0}^{n-\ell} \binom{n-\ell}{j} h_{j,1}. \tag{11}$$

Notice that, for $\ell = 1$, we have

$$\sum_{j=0}^{n-\ell} \binom{n-\ell}{j} h_{j,0} = t_{n,g} \binom{n-3}{n/2-1} \frac{(n-1)(n-2g)^2}{ng(n-g)} + t_{n,g} \binom{n-1}{n/2}$$

$$
\begin{aligned}
&= t_{n,g}\binom{n-3}{n/2-1}\left[\frac{(n-1)(n-2g)^2}{ng(n-g)}+\frac{4(n-1)}{n}\right]\\
&= t_{n,g}\binom{n-3}{n/2-1}\frac{n(n-1)}{g(n-g)}
\end{aligned}
$$

and

$$
\begin{aligned}
\sum_{j=0}^{n-\ell}\binom{n-\ell}{j}h_{j,1} &= \frac{t_{n,g}\binom{n-3}{n/2-1}}{\binom{n-2}{g-1}}\left[\binom{n-1}{g}+\binom{n-1}{g-1}\right]\\
&= \frac{t_{n,g}\binom{n-3}{n/2-1}\binom{n}{g}}{\binom{n-2}{g-1}}\\
&= t_{n,g}\binom{n-3}{n/2-1}\frac{n(n-1)}{g(n-g)}.
\end{aligned}
$$

Therefore, for $\ell = 1$, we have that the identity (11) holds. (The cases $\ell = 2$ and $\ell = 3$ are considered in Appendix A.) Now, we prove that Condition 3 of Lemma 3.10, where α and m are as given by (5), that is,

$$
\sum_{j=0}^{n-4}\binom{n-4}{j}(h_{j,0}-h_{j,1}) = \frac{t_{n,g}(n-2g)^2}{2(n-2)(n-3)}\binom{n-3}{n/2-1} \tag{12}
$$

is satisfied. We have that

$$
\begin{aligned}
&\sum_{j=0}^{n-4}\binom{n-4}{j}(h_{j,0}-h_{j,1}) =\\
&\quad t_{n,g}\binom{n-3}{n/2-1}\left[\frac{(n-1)(n-2g)^2}{ng(n-g)}+\frac{\binom{n-4}{n/2}}{\binom{n-3}{n/2-1}}-\frac{\binom{n-4}{g}+\binom{n-4}{n-g}}{\binom{n-2}{g-1}}\right]\\
&= t_{n,g}\binom{n-3}{n/2-1}\left[\frac{(n-1)(n-2)^2}{ng(n-g)}+\frac{(n-4)(n-6)}{2n(n-3)}\right.\\
&\qquad\left.-\frac{(n-g-1)(n-g-2)(n-g-3)}{g(n-2)(n-3)}-\frac{(g-1)(g-2)(g-3)}{(n-g)(n-2)(n-3)}\right]\\
&= \frac{t_{n,g}(n-2g)^2}{2(n-2)(n-3)}\binom{n-3}{n/2-1}.
\end{aligned}
$$

This proves that Condition 3 of Lemma 3.10 holds.

Finally, we prove that the scheme $\mathcal{S}(4, n, g)$ is strong. For any $4 \le \ell \le n$ and for any $Y \subseteq \{1, \ldots, n\}$ such that $|Y| = \ell$, the number of zero columns in $S_g(h_0)[Y]$ ($S_g(h_1)[Y]$) does not depend on the particular set Y, but only on its size ℓ since the basis matrices are in canonical form. Hence, we refer to such a quantity as χ^0_ℓ (χ^1_ℓ). We have that

$$
\chi^0_\ell = \frac{t_{n,g}(n-1)(n-2g)^2}{ng(n-g)}\binom{n-3}{n/2-1} + t_{n,g}\binom{n-\ell}{n/2}
$$

and

$$\chi_\ell^1 = t_{n,g} \frac{\binom{n-3}{n/2-1}}{\binom{n-2}{g-1}} \left[\binom{n-\ell}{g} + \binom{n-\ell}{n-g} \right].$$

Notice that when $\ell > g$, then $\binom{n-\ell}{n-g} = 0$; whereas, $\binom{n-\ell}{g} = 0$ when $g > n-\ell$. We define the function $\beta(\ell)$, for $4 \leq \ell \leq n$, as $\beta(\ell) \triangleq \chi_\ell^0 - \chi_\ell^1$, that is,

$$\beta(\ell) = \frac{t_{n,g}(n-1)(n-2g)^2}{ng(n-g)} \binom{n-3}{n/2-1} + t_{n,g} \binom{n-\ell}{n/2} - t_{n,g} \frac{\binom{n-3}{n/2-1}}{\binom{n-2}{g-1}} \left[\binom{n-\ell}{g} + \binom{n-\ell}{n-g} \right].$$

To prove that the scheme is strong it is enough to show that $\beta(\ell) \geq \alpha \cdot m$, for $4 \leq \ell \leq n$. Next we show that the function $\beta(\ell)$ is non decreasing, by proving that $\beta(\ell+1) - \beta(\ell) \geq 0$. Indeed, this difference can be written as

$$\beta(\ell+1) - \beta(\ell) = \left[\binom{n-\ell-1}{g-1} + \binom{n-\ell-1}{n-g-1} \right] \frac{\binom{n-3}{n/2-1}}{\binom{n-2}{g-1}} t_{n,g} - \binom{n-\ell-1}{\frac{n}{2}-1} t_{n,g}.$$

Assume $\ell \leq g$. Then, after some algebra, to prove $\beta(\ell+1) - \beta(\ell) \geq 0$ is equivalent to prove that

$$\frac{\prod_{j=1}^{\ell-1}(n-g-j) + \prod_{j=1}^{\ell-1}(g-j) - 2\prod_{j=1}^{\ell-1}\left(\frac{n}{2}-j\right)}{2\prod_{j=1}^{\ell-1}\left(\frac{n}{2}-j\right)} \geq 0.$$

Since $j < \ell \leq g < n/2$, we have that the denominator is positive. Therefore, we have to show that the numerator is non negative. To this aim we need some definitions and properties of combinatorial quantities (see [8, pag. 47–48]). For any integer $s \geq 0$ and real x, the *rising factorial power* $x^{\overline{s}}$ is defined as $x^{\overline{s}} = x(x+1)\cdots(x+s-1)$. The rising factorial power is strictly related to the *Stirling numbers of first kind.* For any integers n and k such that $n \geq k \geq 0$ and $n > 0$, the Stirling numbers of first kind, denoted by $\left[\begin{matrix} n \\ k \end{matrix} \right]$, count the number of ways to arrange n objects into k cycles and they are defined as

$$\left[\begin{matrix} n \\ k \end{matrix} \right] = (n-1)\left[\begin{matrix} n-1 \\ k \end{matrix} \right] + \left[\begin{matrix} n-1 \\ k-1 \end{matrix} \right] \qquad \text{with} \qquad \left[\begin{matrix} 0 \\ 0 \end{matrix} \right] = 1 \text{ and } \left[\begin{matrix} n \\ 0 \end{matrix} \right] = 0.$$

The Stirling numbers of first kind and the rising factorial powers are related by

$$x^{\overline{n}} = \sum_{k=0}^{n} \left[\begin{matrix} n \\ k \end{matrix} \right] x^k.$$

Using the rising factorial powers and the above identity, we have that

$$\prod_{j=1}^{\ell-1}(n-g-j)+\prod_{j=1}^{\ell-1}(g-j)-2\prod_{j=1}^{\ell-1}\left(\frac{n}{2}-j\right)$$

$$\begin{aligned}
&= (n-g-\ell+1)^{\overline{\ell-1}}-2\left(\frac{n}{2}-\ell+1\right)^{\overline{\ell-1}}+(g-\ell+1)^{\overline{\ell-1}}\\
&= \sum_{p=1}^{\ell-1}\left[\begin{array}{c}\ell-1\\ p\end{array}\right](n-g-\ell+1)^p-2\sum_{p=1}^{\ell-1}\left[\begin{array}{c}\ell-1\\ p\end{array}\right]\left(\frac{n}{2}-\ell+1\right)^p+\\
&\qquad\qquad \sum_{p=1}^{\ell-1}\left[\begin{array}{c}\ell-1\\ p\end{array}\right](g-\ell+1)^p\\
&= \sum_{p=1}^{\ell-1}\left[\begin{array}{c}\ell-1\\ p\end{array}\right]\left((n-g-\ell+1)^p-2\left(\frac{n}{2}-\ell+1\right)^p+(g-\ell+1)^p\right)
\end{aligned}$$

By induction on p, it is immediate to see that $(n-g-\ell+1)^p-2(n/2-\ell+1)^p+(g-\ell+1)^p\geq 0$. Indeed, setting $a=n/2-\ell+1$ and $d=n/2-g$, we have to prove that $(a+d)^p-2a^p+(a-d)^p\geq 0$. (Notice that $a>d>0$.) For $p=1$, the basis of the induction is true. By inductive hypothesis, assume that $(a+d)^p-2a^p+(a-d)^p\geq 0$, for some $p\geq 1$. We have that

$$\begin{aligned}
(a+d)^{p+1}+(a-d)^{p+1} &= a[(a+d)^p+(a-d)^p]+d[(a+d)^p-(a-d)^p]\\
&\geq a[(a+d)^p+(a-d)^p]\\
&\geq 2a^{p+1}.\ \text{(by the inductive hypothesis)}
\end{aligned}$$

Hence, for $\ell\leq g$, we have that $\beta(\ell+1)-\beta(\ell)\geq 0$.
Assume now $g<\ell\leq n/2$. Then, to prove that $\beta(\ell+1)-\beta(\ell)\geq 0$ is equivalent to prove that

$$\frac{\displaystyle\prod_{j=1}^{\ell-1}(n-g-j)-2\prod_{j=1}^{\ell-1}\left(\frac{n}{2}-j\right)}{\displaystyle 2\prod_{j=1}^{\ell-1}\left(\frac{n}{2}-j\right)}\geq 0.$$

Since $j<\ell\leq n/2$, we have that the denominator of the above expression is a positive quantity; while, the numerator can be written as

$(n-g-\ell+1)^{\overline{\ell-1}}-2(n/2-\ell+1)^{\overline{\ell-1}}$

$$\begin{aligned}
&= \sum_{p=1}^{\ell-1}\left[\begin{array}{c}\ell-1\\ p\end{array}\right](n-g-\ell+1)^p-2\sum_{p=1}^{\ell-1}\left[\begin{array}{c}\ell-1\\ p\end{array}\right]\left(\frac{n}{2}-\ell+1\right)^p\\
&= \sum_{p=1}^{\ell-1}\left[\begin{array}{c}\ell-1\\ p\end{array}\right]\left((n-g-\ell+1)^p-2\left(\frac{n}{2}-\ell+1\right)^p\right).
\end{aligned}$$

By induction on p, one can see that $(n-g-\ell+1)^p-2(n/2-\ell+1)^p\geq 0$. Therefore, for $g<\ell\leq n/2$ we have that $\beta(\ell+1)-\beta(\ell)\geq 0$.

Finally, assume that $\ell > n/2$. Then,

$$\beta(\ell+1) - \beta(\ell) = \frac{t_{n,g} \cdot \binom{n-\ell-1}{g-1}\binom{n-3}{n/2-1}}{\binom{n-2}{g-1}} \geq 0.$$

Therefore, the function $\beta(\ell)$ is non decreasing. Hence, since $\beta(4) \geq \alpha \cdot m$, the scheme $\mathcal{S}(4,n,g)$ is strong. □

Notice that, for fixed n, the contrast of the scheme given by Theorem 5.1 depends only on the parameter g. Hence, for fixed n, the scheme achieving the best contrast among the schemes $\mathcal{S}(4,n,g)$ is obtained by choosing the integer g in the interval $[1, n/2[$, in such a way that the quantity

$$\alpha_4(g,n) = \frac{g(n-g)(n-2g)^2}{4n(n-1)(n-2)(n-3)}$$

is maximized. For real g and for fixed n, a simple algebra shows that the function $g(n-g)(n-2g)^2$, with $g \in [1, n/2[$, is convex $\cap$ and reaches its maximum at $g = (2-\sqrt{2})n/4$. Since g has to be an integer, we have that g can be either equal to $\lfloor (2-\sqrt{2})n/4 \rfloor$ or equal to $\lceil (2-\sqrt{2})n/4 \rceil$. For any fixed $n \geq 4$, let $g_n \in \left\{ \lfloor (2-\sqrt{2})n/4 \rfloor, \lceil (2-\sqrt{2})n/4 \rceil \right\}$ be the integer which maximizes $\alpha_4(g,n)$. One can easily see that $\lim_{n\to\infty} \alpha_4(g_n,n) = 1/64$.

Remark 5.2 Theorem 5.1 holds only when n is even. If n is odd, then, by applying the technique given in Theorem 5.1, we construct a $(4, n+1)$-threshold VCS, and then we consider only the first n rows of the basis matrices of such scheme. Therefore, for any odd $n \geq 4$ and any integer $1 \leq g < n/2$, there exists a strong $(4,n)$-threshold VCS having pixel expansion and contrast equal to

$$m = \frac{2nt_{n,g}(n+1)}{g(n+1-g)}\binom{n+1-3}{(n+1)/2-1} \quad \text{and} \quad \alpha = \frac{g(n+1-g)(n+1-2g)^2}{4n(n+1)(n-1)(n-2)},$$

respectively.

6 A Canonical $(5,n)$-threshold VCS

In this section we provide, for $n \geq 5$, a class of $(5,n)$-threshold VCS whose basis matrices are in canonical form. Similarly to the previous cases, we first describe a family of $(5,n)$-threshold VCS achieving various values of contrast and pixel expansion. Then, for any fixed $n \geq 5$ we determine the scheme in this family having the best contrast.

For any two integers ℓ and g such that $1 \leq \ell < g < n/2$, the $(5,n)$-threshold VCS whose basis matrices are in canonical form, denoted by $\mathcal{S}(5,n,\ell,g)$, is described by the following $h_{j,i}$'s:

$$h_{g,0} = h_{n-g,1} = t_{(n,\ell,g)}, \qquad h_{n-\ell,0} = h_{\ell,1} = s_{(n,\ell,g)}, \qquad \text{and} \qquad h_{0,0} = h_{n,1} = r_{(n,\ell,g)}, \tag{13}$$

where

$$t_{(n,\ell,g)} = \frac{\binom{n-4}{\ell-1} - \binom{n-4}{\ell-3}}{\gcd\left\{\binom{n-4}{\ell-1} - \binom{n-4}{\ell-3}, \binom{n-4}{g-1} - \binom{n-4}{g-3}\right\}}, \quad s_{(n,\ell,g)} = t_{(n,\ell,g)} \frac{\left[\binom{n-4}{g-1} - \binom{n-4}{g-3}\right]}{\left[\binom{n-4}{\ell-1} - \binom{n-4}{\ell-3}\right]},$$

$$r_{(n,\ell,g)} = s_{(n,\ell,g)} \left[\binom{n-4}{\ell} - \binom{n-4}{\ell-4}\right] - t_{(n,\ell,g)} \left[\binom{n-4}{g} - \binom{n-4}{g-4}\right],$$

and all the remaining $h_{j,i}$'s are equal to zero.

Theorem 6.1 *For any two integers ℓ and g such that $1 \le \ell < g < n/2$, the scheme $\mathcal{S}(5,n,\ell,g)$ is a canonical $(5,n)$-threshold VCS having pixel expansion and contrast equal to*

$$m = s_{(n,\ell,g)} \left[\binom{n}{\ell} + \binom{n-4}{\ell} - \binom{n-4}{\ell-4}\right] + t_{(n,\ell,g)} \left[\binom{n}{g} + \binom{n-4}{g-4} - \binom{n-4}{g}\right]$$

and

$$\alpha = \frac{\ell(g-\ell)(n-g)(n-2g)(n-2\ell)}{2(n+2\ell-2g)(n-1)(n-2)(n-3)(n-4)},$$

respectively.

Proof. It is easy to see that Condition 1 of Lemma 3.10 is satisfied as the basis matrices of the scheme $\mathcal{S}(5,n,\ell,g)$ are one the complement of the other. To prove that Condition 2 of Lemma 3.10 is satisfied we have to show that, for $1 \le q \le 4$, the following equality holds

$$\sum_{j=0}^{n-q} \binom{n-q}{j} h_{j,1} = \sum_{j=0}^{n-q} \binom{n-q}{j} h_{j,0}. \tag{14}$$

We have that

$$\sum_{j=0}^{n-q} \binom{n-q}{j} h_{j,1} \;=\; t_{(n,\ell,g)} \binom{n-q}{\ell} \frac{\binom{n-4}{g-1} - \binom{n-4}{g-3}}{\binom{n-4}{\ell-1} - \binom{n-4}{\ell-3}} + t_{(n,\ell,g)} \binom{n-q}{n-g}$$

and

$$\begin{aligned}\sum_{j=0}^{n-q} \binom{n-q}{j} h_{j,0} \;=\; & t_{(n,\ell,g)} \frac{\binom{n-4}{g-1} - \binom{n-4}{g-3}}{\binom{n-4}{\ell-1} - \binom{n-4}{\ell-3}} \left[\binom{n-4}{\ell} - \binom{n-4}{\ell-4} + \binom{n-q}{n-\ell}\right] - \\ & t_{(n,\ell,g)} \left[\binom{n-4}{g} - \binom{n-4}{g-4}\right] + t_{(n,\ell,g)} \binom{n-q}{g}.\end{aligned}$$

Therefore, equality (14) is satisfied if and only if the quantity

$$A(n,\ell,g) \triangleq \frac{\binom{n-4}{g-1} - \binom{n-4}{g-3}}{\binom{n-4}{\ell-1} - \binom{n-4}{\ell-3}} \left[\binom{n-4}{\ell} - \binom{n-4}{\ell-4}\right] - \left[\binom{n-4}{g} - \binom{n-4}{g-4}\right] \tag{15}$$

is equal to

$$B(n,\ell,g,q) \triangleq \frac{\binom{n-4}{g-1}-\binom{n-4}{g-3}}{\binom{n-4}{\ell-1}-\binom{n-4}{\ell-3}}\left[\binom{n-q}{\ell}-\binom{n-q}{n-\ell}\right]-\left[\binom{n-q}{g}-\binom{n-q}{n-g}\right]. \quad (16)$$

If we substitute q for 4 in (16) we get expression (15). Therefore, (14) is satisfied for $q=4$. We will prove that equality (14) holds when $q=1$ and $4 \le \ell < g$. (The remaining cases are analyzed in Appendix A.)
Note that $A(n,\ell,g)$ can be written as

$$\frac{\binom{n-4}{g-3}\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]}{\binom{n-4}{\ell-3}\left[\frac{(n-\ell-1)(n-\ell-2)}{(\ell-1)(\ell-2)}-1\right]}\binom{n-4}{\ell-3}\left[\frac{(n-\ell-1)(n-\ell-2)(n-\ell-3)}{\ell(\ell-1)(\ell-2)}-\frac{\ell-3}{n-\ell}\right]$$
$$-\binom{n-4}{g-3}\left[\frac{(n-g-1)(n-g-2)(n-g-3)}{g(g-1)(g-2)}-\frac{g-3}{n-g}\right]$$

which is equal to

$$\binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]\left[\frac{(n-\ell-1)(n-\ell-2)(n-\ell-3)}{\ell(\ell-1)(\ell-2)}-\frac{\ell-3}{n-\ell}\right]}{\left[\frac{(n-\ell-1)(n-\ell-2)}{(\ell-1)(\ell-2)}-1\right]}\right.$$
$$\left.-\frac{(n-g-1)(n-g-2)(n-g-3)}{g(g-1)(g-2)}+\frac{g-3}{n-g}\right\}.$$

After some algebra, we get that the above expression is reduced to

$$\binom{n-4}{g-3}\frac{(n-1)(n-2)(n-3)(n-2g)(g-\ell)(n-\ell-g)}{g\ell(g-1)(g-2)(n-\ell)(n-g)}. \quad (17)$$

We can rewrite $B(n,\ell,g,1)$ as:

$$\frac{\binom{n-4}{g-3}\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]}{\binom{n-4}{\ell-3}\left[\frac{(n-\ell-1)(n-\ell-2)}{(\ell-1)(\ell-2)}-1\right]}\binom{n-4}{\ell-3}\left[\frac{(n-1)(n-2)(n-3)}{\ell(\ell-1)(\ell-2)}-\frac{(n-1)(n-2)(n-3)}{(\ell-1)(\ell-2)(n-\ell)}\right]$$
$$-\binom{n-4}{g-3}\left[\frac{(n-1)(n-2)(n-3)}{g(g-1)(g-2)}-\frac{(n-1)(n-2)(n-3)}{(g-1)(g-2)(n-g)}\right]$$

which is equal to

$$\binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]\left[\frac{(n-1)(n-2)(n-3)}{\ell(\ell-1)(\ell-2)}-\frac{(n-1)(n-2)(n-3)}{(\ell-1)(\ell-2)(n-\ell)}\right]}{\left[\frac{(n-\ell-1)(n-\ell-2)}{(\ell-1)(\ell-2)}-1\right]}\right.$$
$$\left.-\left[\frac{(n-1)(n-2)(n-3)}{g(g-1)(g-2)}-\frac{(n-1)(n-2)(n-3)}{(g-1)(g-2)(n-g)}\right]\right\}.$$

A simple algebra shows that the above expression reduces to (17). Therefore, when $q = 1$ and $4 \leq \ell < g$ equality (14) is satisfied.
To prove that Condition 3 of Lemma 3.10 is satisfied we have to show that

$$\sum_{j=0}^{n-5} \binom{n-5}{j} (h_{j,0} - h_{j,1}) = \alpha \cdot m. \tag{18}$$

We show that (18) holds for $4 \leq \ell < g$. (The cases $1 \leq \ell < g \leq 3$ and $1 \leq \ell \leq 3$ with $g \geq 4$ are considered in Appendix A.) It is immediate to see that equation (18) is satisfied if and only if:

$$\frac{\sum_{j=0}^{n-5} \binom{n-5}{j} (h_{j,0} - h_{j,1})}{m} = \frac{\ell(g-\ell)(n-g)(n-2g)(n-2\ell)}{2(n+2\ell-2g)(n-1)(n-2)(n-3)(n-4)}. \tag{19}$$

We have that

$$\begin{aligned}
&\frac{\sum_{j=0}^{n-5} \binom{n-5}{j} (h_{j,0} - h_{j,1})}{m} \\
&= \frac{s_{(n,\ell,g)} \left[\binom{n-4}{\ell} - \binom{n-4}{n-\ell} + \binom{n-5}{n-\ell} - \binom{n-5}{\ell}\right] - t_{(n,\ell,g)} \left[\binom{n-4}{g} - \binom{n-4}{n-g} + \binom{n-5}{g} - \binom{n-5}{n-g}\right]}{s_{(n,\ell,g)} \left[\binom{n}{\ell} + \binom{n-4}{\ell} - \binom{n-4}{\ell-4}\right] + t_{(n,\ell,g)} \left[\binom{n}{g} + \binom{n-4}{g-4} - \binom{n-4}{g}\right]} \\
&= \frac{s_{(n,\ell,g)} \left[\binom{n-5}{\ell-1} - \binom{n-5}{\ell-4}\right] - t_{(n,\ell,g)} \left[\binom{n-5}{g-1} - \binom{n-5}{g-4}\right]}{s_{(n,\ell,g)} \left[\binom{n}{\ell} + \binom{n-4}{\ell} - \binom{n-4}{\ell-4}\right] + t_{(n,\ell,g)} \left[\binom{n}{g} + \binom{n-4}{g-4} - \binom{n-4}{g}\right]}.
\end{aligned} \tag{20}$$

Let

$$a \triangleq s_{(n,\ell,g)} \left[\binom{n-5}{\ell-1} - \binom{n-5}{\ell-4}\right] \qquad b \triangleq t_{(n,\ell,g)} \left[\binom{n-5}{g-1} - \binom{n-5}{g-4}\right]$$

$$c \triangleq s_{(n,\ell,g)} \left[\binom{n}{\ell} + \binom{n-4}{\ell} - \binom{n-4}{\ell-4}\right] \qquad d \triangleq t_{(n,\ell,g)} \left[\binom{n}{g} + \binom{n-4}{g-4} - \binom{n-4}{g}\right].$$

It is easy to check that the following three equalities hold.

$$\begin{aligned}
\frac{a}{c} &= \frac{\ell(n-2\ell)(n^2 - n\ell - 6n + \ell^2 + 11)}{2(n-3)(n-4)(n^2 - n\ell - 3n + 2\ell^2 + 2)}. \\
\frac{b}{a} &= \frac{(n^2 - ng - 6n + g^2 + 11)}{(n^2 - n\ell - 6n + \ell^2 + 11)}. \\
\frac{d}{c} &= \frac{\ell(n-2\ell)(2n^2 - 3ng - 3n + 2g^2 + 2)}{(n-2g)(n-g)(n^2 - n\ell - 3n + 2\ell^2 + 2)}.
\end{aligned}$$

Since $(a-b)/(c+d)=\frac{a(1-b/a)}{c(1+d/c)}$ we have that

$$\frac{s_{(n,\ell,g)}\left[\binom{n-5}{\ell-1}-\binom{n-5}{\ell-4}\right]-t_{(n,\ell,g)}\left[\binom{n-5}{g-1}-\binom{n-5}{g-4}\right]}{s_{(n,\ell,g)}\left[\binom{n}{\ell}+\binom{n-4}{\ell}-\binom{n-4}{\ell-4}\right]+t_{(n,\ell,g)}\left[\binom{n}{g}+\binom{n-4}{g-4}-\binom{n-4}{g}\right]}$$

can be rewritten as

$$\frac{\ell(n-2\ell)(n^2-n\ell-6n+\ell^2+11)}{2(n-3)(n-4)(n^2-n\ell-3n+2\ell^2+2)}\cdot\left[\frac{1\quad-\quad\frac{(n^2-ng-6n+g^2+11)}{(n^2-n\ell-6n+\ell^2+11)}}{1\quad+\quad\frac{\ell(n-2\ell)(2n^2-3ng-3n+2g^2+2)}{(n-2g)(n-g)(n^2-n\ell-3n+2\ell^2+2)}}\right].$$

It is simple, but tedious to check, to see that the previous expression reduces to

$$\frac{\ell(g-\ell)(n-g)(n-2g)(n-2\ell)}{2(n+2\ell-2g)(n-1)(n-2)(n-3)(n-4)}.$$

Therefore, Equation (18) is satisfied and the theorem holds. $\square$

Notice that, for fixed n, the contrast of the scheme given in the above theorem depends only on the parameters ℓ and g. Therefore, if we want to get from the construction given by Theorem 6.1 the scheme achieving the best contrast we have to choose, for a fixed n, the integers ℓ and g, where $1\le\ell<g<n/2$, in such a way that the quantity

$$\alpha_5(\ell,g,n)=\frac{\ell(g-\ell)(n-g)(n-2g)(n-2\ell)}{2(n+2\ell-2g)(n-1)(n-2)(n-3)(n-4)}$$

is maximized. Choosing ℓ and g proportional to n, setting $\ell=\gamma\cdot n$ and $g=\delta\cdot n$, where γ and δ are constant to be determined later such that $0<\gamma<\delta<1$, we have that

$$\alpha_5(\gamma\cdot n,\delta\cdot n,n)=\frac{\gamma(\delta-\gamma)(1-\delta)(1-2\delta)(1-2\gamma)n^5}{2(1+2\gamma-2\delta)n(n-1)(n-2)(n-3)(n-4)}.$$

One can easily see that

$$\lim_{n\to\infty}\alpha_5(\gamma\cdot n,\delta\cdot n,n)=\frac{\gamma(\delta-\gamma)(1-\delta)(1-2\delta)(1-2\gamma)}{2(1+2\gamma-2\delta)}.$$

For real γ and δ, with $0<\gamma<\delta<1$, by using the system `Mathematica`™, we have seen that, for fixed n, the function $\gamma(\delta-\gamma)(1-\delta)(1-2\delta)(1-2\gamma)/2(1+2\gamma-2\delta)$ reaches it maximum at $(\overline{\gamma},\overline{\delta})=(0.0954913,0.345492)$ and the above limit is equal to

$$\lim_{n\to\infty}\alpha_5(\overline{\gamma}\cdot n,\overline{\delta}\cdot n,n)=\frac{1}{256}.$$

Therefore, there are $(5,n)$-threshold VCS that, for large n, have contrast almost $1/256$.

7 Conclusion

In this paper we have analyzed the contrast of the reconstructed image for (k, n)-threshold VCS. We have defined a canonical form for such VCS and we have also provided a characterizazion of (k, n)-threshold VCS. Several open problems arise. For instance, we conjecture that the (k, n)-threshold VCS, for $k = 4$ and 5, have an optimal contrast. Moreover, further research could be done in finding a closed formula for the optimal contrast for general (k, n)-threshold VCS.

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Visual Cryptography for General Access Structures*, in *Information and Computation*, Vol. 129, No. 2, pp. 86–106, 1996.

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Extended Schemes for Visual Cryptography*, submitted for publication, 1996. Available as `http://www.unisa.it/VISUAL/papers/evcs.ps`.

[3] 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.

[4] E. Biham and A. Itzkovitz, *Visual Cryptography with Polarization*, talk given by Biham at the "Weizmann Workshop on Cryptography", Weizmann Institute, Rehovot, Israel, June 8–9, 1997.

[5] C. Blundo, A. De Santis, and D. R. Stinson, *On the Contrast in Visual Cryptography Schemes*, in *Journal of Cryptology*, Vol. 12, pp. 261-289, 1999.

[6] A. De Bonis and A. De Santis, *Randomness in Visual Cryptography*, in in "Proc. of STACS 2000", 17th International Symposium on Theoretical Aspects of Computer Science, 2000.

[7] 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.

[8] R. L. Graham, D. E. Knuth, and O. Patashnik, Concrete Mathematics. A foundation for Computer Science. Addison Wesley, 1988.

[9] T. Hofmeister, M. Krause, and H. U. Simon, *Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography*, in "COCOON '97", T. Jiang and D. T. Lee, Eds., Vol. 1276 of "Lecture Notes in Computer Science", Springer–Verlag, Berlin, pp. 176–185, 1997.

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

[11] M. Naor and B. Pinkas, *Visual Authentication and Identification*, in "Advances in Cryptology - CRYPTO '97", B. S. Kaliski Jr. Ed., Vol. 1294 of "Lecture Notes in Computer Science", Springer–Verlag, Berlin, pp. 322–336, 1997. Available at *Theory of Cryptography Library* as `ftp://theory.lcs.mit.edu/pub/tcryptol/97-13.ps`.

[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*. Available at *Theory of Cryptography Library* as `ftp://theory.lcs.mit.edu/pub/tcryptol/96-07.ps`.
A preliminary version appears in "Security Protocols", M. Lomas Ed., Vol. 1189 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp. 197–202, 1997.

[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] D. R. Stinson, *An Introduction to Visual Cryptography*, presented at Public Key Solutions '97, Toronto, April 28-30, 1997. Available as
`http://bibd.unl.edu/ stinson/VKS-PKS.ps`.

[16] E. R. Verheul and H. C. A. van Tilborg, *Constructions and Properties of k out of n visual secret sharing schemes, Designs, Codes, and Cryptography*, Vol. 11, No. 2, pp. 179–196, 1997.

A Appendix A

In the following we show the computation omitted from the proof of Theorem 5.1.

- Proof that the equality (11) in Theorem 5.1 is satisfied for the case $\ell = 2$. We have that

$$\begin{aligned}\sum_{j=0}^{n-\ell}\binom{n-\ell}{j}h_{j,0} &= t_{n,g}\left[\binom{n-3}{n/2-1}\frac{(n-1)(n-2g)^2}{ng(n-g)}+\binom{n-2}{n/2}\right]\\ &= t_{n,g}\binom{n-3}{n/2-1}\left[\frac{(n-1)(n-2g)^2}{ng(n-g)}+\frac{2(n-2)}{n}\right]\\ &= t_{n,g}\binom{n-3}{n/2-1}\frac{n^2-2ng-n+2g^2}{g(n-g)}\end{aligned}$$

and

$$\begin{aligned}\sum_{j=0}^{n-\ell}\binom{n-\ell}{j}h_{j,1} &= t_{n,g}\binom{n-3}{n/2-1}\frac{\binom{n-2}{g}+\binom{n-2}{n-g}}{\binom{n-2}{g-1}}\\ &= t_{n,g}\binom{n-3}{n/2-1}\left[\frac{(n-g-1)}{g}+\frac{g-1}{n-g}.\right]\\ &= t_{n,g}\binom{n-3}{n/2-1}\frac{n^2-2ng-n+2g^2}{g(n-g)}.\end{aligned}$$

Therefore, for $\ell = 2$, we have that the identity (11 in Theorem 5.1 holds.

- Proof that the equality (11) in Theorem 5.1 is satisfied for the case $\ell = 3$. We have that

$$\begin{aligned}\sum_{j=0}^{n-\ell}\binom{n-\ell}{j}h_{j,0} &= t_{n,g}\left[\binom{n-3}{n/2-1}\frac{(n-1)(n-2g)^2}{ng(n-g)}+\binom{n-3}{n/2}\right]\\ &= t_{n,g}\binom{n-3}{n/2-1}\left[\frac{(n-1)(n-2g)^2}{ng(n-g)}+\frac{n-4}{n}\right]\end{aligned}$$

and

$$\sum_{j=0}^{n-\ell}\binom{n-\ell}{j}h_{j,1} =$$

$$\binom{n-3}{n/2-1}\frac{(n-1)(n-2g)^2}{ng(n-g)}+\binom{n-3}{n/2} = \binom{n-3}{g}\frac{\binom{n-3}{n/2-1}}{\binom{n-2}{g-1}}+\binom{n-3}{n-g}\frac{\binom{n-3}{n/2-1}}{\binom{n-2}{g-1}}$$

that is,

$$\frac{(n-1)(n-2g)^2}{ng(n-g)}+\frac{n/2-2}{n/2} = \frac{\binom{n-3}{g}+\binom{n-3}{n-g}}{\binom{n-2}{g-1}}$$

which turns out to be equivalent to

$$\frac{(n-1)(n-2g)^2}{ng(n-g)} + \frac{n-4}{n} = \frac{(n-g-1)(n-g-2)}{g(n-2)} + \frac{(g-1)(g-2)}{(n-g)(n-2)}.$$

A simple algebra shows that the above equality holds.

In the following we show the computations omitted from the proof of Theorem 6.1. Recall that equality (14) holds if and only if the expression (15) is equal to the expression (16). Now, we show that equality (14) is always satisfied.

- For $q = 2$ and $4 \leq \ell < g$, we must show that

$$A(n, \ell, g) = B(n, \ell, g, 2)$$

In Theorem 6.1 we proved that $A(n, \ell, g)$ is equal to (17). Notice that $B(n, \ell, g, 2)$ can be written as

$$\frac{\binom{n-4}{g-3}\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)} - 1\right]}{\binom{n-4}{\ell-3}\left[\frac{(n-\ell-1)(n-\ell-2)}{(\ell-1)(\ell-2)} - 1\right]} \binom{n-4}{\ell-3}\left[\frac{(n-\ell-1)(n-2)(n-3)}{\ell(\ell-1)(\ell-2)} - \frac{(n-2)(n-3)}{(\ell-2)(n-\ell)}\right]$$
$$-\binom{n-4}{g-3}\left[\frac{(n-g-1)(n-2)(n-3)}{g(g-1)(g-2)} - \frac{(n-2)(n-3)}{(g-2)(n-g)}\right]$$

which is equal to

$$\binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)} - 1\right]\left[\frac{(n-\ell-1)(n-2)(n-3)}{\ell(\ell-1)(\ell-2)} - \frac{(n-2)(n-3)}{(\ell-2)(n-\ell)}\right]}{\left[\frac{(n-\ell-1)(n-\ell-2)}{(\ell-1)(\ell-2)} - 1\right]}\right.$$
$$\left. - \left[\frac{(n-g-1)(n-2)(n-3)}{g(g-1)(g-2)} - \frac{(n-2)(n-3)}{(g-2)(n-g)}\right]\right\}.$$

A simple algebra shows that the above expression can be reduced to (17). Therefore, equality (14) is satisfied when $q = 2$ and $4 \leq \ell < g$.

- For $q = 3$ and $4 \leq \ell < g$, we must show that

$$A(n, \ell, g) = B(n, \ell, g, 3)$$

In Theorem 6.1 we proved that $A(n, \ell, g)$ is equal to (17). Note that $B(n, \ell, g, 3)$ can be rewritten as

$$\frac{\binom{n-4}{g-3}\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)} - 1\right]}{\binom{n-4}{\ell-3}\left[\frac{(n-\ell-1)(n-\ell-2)}{(\ell-1)(\ell-2)} - 1\right]} \binom{n-4}{\ell-3}\left[\frac{(n-\ell-1)(n-\ell-2)(n-3)}{\ell(\ell-1)(\ell-2)} - \frac{(n-3)}{(n-\ell)}\right]$$
$$-\binom{n-4}{g-3}\left[\frac{(n-g-1)(n-g-2)(n-3)}{g(g-1)(g-2)} - \frac{(n-3)}{(n-g)}\right]$$

which is equal to

$$\binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]\left[\frac{(n-\ell-1)(n-\ell-2)(n-3)}{\ell(\ell-1)(\ell-2)}-\frac{(n-3)}{(n-\ell)}\right]}{\left[\frac{(n-\ell-1)(n-\ell-2)}{(\ell-1)(\ell-2)}-1\right]}\right.$$
$$\left.-\left[\frac{(n-g-1)(n-g-2)(n-3)}{g(g-1)(g-2)}-\frac{(n-3)}{(n-g)}\right]\right\}.$$

A simple algebra shows that the above expression can be reduced to (17). Therefore, equality (14) holds for $q=3$ when $4\leq\ell<g$.

- For $q=1$, $\ell=1$ and $g=2$, we have that

$$A(n,1,2)=\frac{(n-3)(n-4)}{2}\quad\text{and}\quad B(n,1,2,1)=\frac{(n-3)(n-4)}{2}.$$

Therefore, $A(n,1,2)=B(n,1,2,1)$ and equality (14) in Theorem 6.1 is satisfied.

- For $q=1$, $\ell=1$ and $g=3$, we have that

$$A(n,1,3)=\frac{(n-2)(n-4)(n-6)}{3}\quad\text{and}\quad B(n,1,3,1)=\frac{(n-2)(n-4)(n-6)}{3}.$$

Therefore, $A(n,1,3)=B(n,1,3,1)$ and equality (14) in Theorem 6.1 is satisfied.

- For $q=1$, $\ell=2$ and $g=3$, we have that

$$A(n,2,3)=\frac{(n-1)(n-5)(n-6)}{12}\quad\text{and}\quad B(n,2,3,1)=\frac{(n-1)(n-5)(n-6)}{12}.$$

Therefore, $A(n,2,3)=B(n,2,3,1)$ and equality (14) in Theorem 6.1 is satisfied.

- For $q=2$, $\ell=1$ and $g=2$, we have that

$$A(n,1,2)=\frac{(n-3)(n-4)}{2}\quad\text{and}\quad B(n,1,2,2)=\frac{(n-3)(n-4)}{2}.$$

Therefore, $A(n,1,2)=B(n,1,2,2)$ and equality (14) in Theorem 6.1 is satisfied.

- For $q=2$, $\ell=1$ and $g=3$, we have that

$$A(n,1,3)=\frac{(n-2)(n-4)(n-6)}{3}\quad\text{and}\quad B(n,1,3,2)=\frac{(n-2)(n-4)(n-6)}{3}.$$

Therefore, $A(n,1,3)=B(n,1,3,2)$ and equality (14) in Theorem 6.1 is satisfied.

- For $q=2$, $\ell=2$ and $g=3$, we have that

$$A(n,2,3)=\frac{(n-1)(n-5)(n-6)}{12}\quad\text{and}\quad B(n,2,3,2)=\frac{(n-1)(n-5)(n-6)}{12}.$$

Therefore, $A(n,2,3)=B(n,2,3,2)$ and equality (14) in Theorem 6.1 is satisfied.

- For $q = 3$, $\ell = 1$ and $g = 2$, we have that

$$A(n,1,2) = \frac{(n-3)(n-4)}{2} \quad \text{and} \quad B(n,1,2,3) = \frac{(n-3)(n-4)}{2}$$

  Therefore, $A(n,1,2) = B(n,1,2,3)$ and equality (14) in Theorem 6.1 is satisfied.

- For $q = 3$, $\ell = 1$ and $g = 3$, we have that

$$A(n,1,3) = \frac{(n-2)(n-4)(n-6)}{3} \quad \text{and} \quad B(n,1,3,3) = \frac{(n-2)(n-4)(n-6)}{3}.$$

  Therefore, $A(n,1,3) = B(n,1,3,3)$ and equality (14) in Theorem 6.1 is satisfied.

- For $q = 3$, $\ell = 2$ and $g = 3$, we have that

$$A(n,2,3) = \frac{(n-1)(n-5)(n-6)}{12} \quad \text{and} \quad B(n,2,3,3) = \frac{(n-1)(n-5)(n-6)}{12}.$$

  Therefore, $A(n,2,3) = B(n,2,3,3)$ and equality (14) in Theorem 6.1 is satisfied.

- For $q = 1$, $\ell = 1$ and $g \geq 4$, we must show that $A(n,1,g) = B(n,1,g,1)$. Notice that

$$\begin{aligned} A(n,1,g) \quad &= \quad \binom{n-4}{g-3}\left\{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)} - 1\right](n-4)\right. \\ &\qquad \left. - \left[\frac{(n-g-1)(n-g-2)(n-g-3)}{g(g-1)(g-2)} - \frac{(g-3)}{(n-g)}\right]\right\} \end{aligned}$$

  and

$$\begin{aligned} B(n,1,g,1) \quad &= \quad \binom{n-4}{g-3}\left\{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)} - 1\right](n-2)\right. \\ &\qquad \left. - \left[\frac{(n-1)(n-2)(n-3)}{g(g-1)(g-2)} - \frac{(n-1)(n-2)(n-3)}{(g-1)(g-2)(n-g)}\right]\right\}. \end{aligned}$$

  After some algebra $A(n,1,g)$ and $B(n,1,g,1)$ can be reduced to

$$\binom{n-4}{g-3}\frac{(n-2)(n-3)(n-2g)(n-g-1)}{g(g-2)(n-g)}.$$

  Therefore, equality (14) in Theorem 6.1 is satisfied when $q = 1$, $\ell = 1$ and $g \geq 4$.

- For $q=1$, $\ell=2$ and $g \geq 4$, we must show that $A(n,2,g) = B(n,2,g,1)$. Notice that

$$
\begin{aligned}
A(n,2,g) &= \binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]}{(n-4)}\frac{(n-4)(n-5)}{2}\right. \\
&\qquad \left. -\left[\frac{(n-g-1)(n-g-2)(n-g-3)}{g(g-1)(g-2)}-\frac{(g-3)}{(n-g)}\right]\right\}
\end{aligned}
$$

and

$$
\begin{aligned}
B(n,2,g,1) &= \binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]\left[\frac{(n-1)(n-2)}{2}-(n-1)\right]}{(n-4)}\right. \\
&\qquad \left. \left[\frac{(n-1)(n-2)(n-3)}{g(g-1)(g-2)}-\frac{(n-1)(n-2)(n-3)}{(g-1)(g-2)(n-g)}\right]\right\}.
\end{aligned}
$$

After some algebra $A(n,2,g)$ and $B(n,2,g,1)$ can be reduced to

$$\binom{n-4}{g-3}\frac{(n-1)(n-3)(n-2g)(n-g-2)}{2g(g-1)(n-g)}$$

Therefore, equality (14) in Theorem 6.1 is satisfied when $q=1$, $\ell=2$ and $g \geq 4$.

- For $q=1$, $\ell=3$ and $g \geq 4$, we must show that $A(n,3,g) = B(n,3,g,1)$. Notice that

$$
\begin{aligned}
A(n,3,g) &= \binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]\frac{(n-4)(n-5)(n-6)}{6}}{\frac{(n-4)(n-5)}{2}-1}\right. \\
&\qquad \left. -\frac{(n-g-1)(n-g-2)(n-g-3)}{g(g-1)(g-2)}+\frac{(g-3)}{(n-g)}\right\}
\end{aligned}
$$

and

$$
\begin{aligned}
B(n,3,g,1) &= \binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]\left[\frac{(n-1)(n-2)(n-3)}{6}-\frac{(n-1)(n-2)}{2}\right]}{\frac{(n-4)(n-5)}{2}-1}\right. \\
&\qquad \left. -\frac{(n-1)(n-2)(n-3)}{g(g-1)(g-2)}+\frac{(n-1)(n-2)(n-3)}{(g-1)(g-2)(n-g)}\right\}.
\end{aligned}
$$

After some algebra $A(n,3,g)$ and $B(n,3,g,1)$ can be reduced to

$$\binom{n-4}{g-3}\frac{(n-1)(n-2)(g-3)(n-2g)(n-g-3)}{3g(g-1)(g-2)(n-g)}.$$

Therefore, equality (14) in Theorem 6.1 is satisfied for $q=1$, $\ell=3$ and $g \geq 4$.

- For $q=2$, $\ell=1$ and $g\geq 4$, we must show that $A(n,1,g)=B(n,1,g,2)$. Notice that

$$\begin{aligned} B(n,1,g,2) &= \binom{n-4}{g-3}\left\{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right](n-2)\right. \\ &\qquad \left. -\left[\frac{(n-g-1)(n-2)(n-3)}{g(g-1)(g-2)}-\frac{(n-2)(n-3)}{(g-2)(n-g)}\right]\right\}. \end{aligned}$$

After some algebra $B(n,1,g,2)$ can be reduced to

$$\binom{n-4}{g-3}\frac{(n-2)(n-3)(n-2g)(n-g-1)}{g(g-2)(n-g)}.$$

Therefore, equality (14) in Theorem 6.1 is satisfied when $q=2$, $\ell=1$ and $g\geq 4$.

- For $q=2$, $\ell=2$ and $g\geq 4$, we must show that $A(n,2,g)=B(n,2,g,2)$. Notice that

$$\begin{aligned} B(n,2,g,2) &= \binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]\left[\frac{(n-2)(n-3)}{2}-1\right]}{(n-4)}\right. \\ &\qquad \left. -\left[\frac{(n-g-1)(n-2)(n-3)}{g(g-1)(g-2)}-\frac{(n-2)(n-3)}{(g-2)(n-g)}\right]\right\}. \end{aligned}$$

After some algebra $B(n,2,g,2)$ can be reduced to

$$\binom{n-4}{g-3}\frac{(n-1)(n-3)(n-2g)(n-g-2)}{2g(g-1)(n-g)}.$$

Therefore, equality (14) in Theorem 6.1 is satisfied when $q=2$, $\ell=2$ and $g\geq 4$.

- For $q=2$, $\ell=3$ and $g\geq 4$, we must show that $A(n,3,g)=B(n,3,g,2)$. Notice that

$$\begin{aligned} B(n,3,g,2) &= \binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]\left[\frac{(n-2)(n-3)(n-4)}{6}-(n-2)\right]}{\frac{(n-4)(n-5)}{2}-1}\right. \\ &\qquad \left. -\left[\frac{(n-g-1)(n-2)(n-3)}{g(g-1)(g-2)}-\frac{(n-2)(n-3)}{(g-2)(n-g)}\right]\right\}. \end{aligned}$$

After some algebra $B(n,3,g,2)$ can be reduced to

$$\binom{n-4}{g-3}\frac{(n-1)(n-2)(g-3)(n-2g)(n-g-3)}{3g(g-1)(g-2)(n-g)}.$$

Therefore, equality (14) in Theorem 6.1 is satisfied for $q=2$, $\ell=3$ and $g\geq 4$.

- For $q = 3$, $\ell = 1$ and $g \geq 4$, we must show that $A(n, 1, g) = B(n, 1, g, 3)$. Notice that

$$
\begin{aligned}
B(n,1,g,3) &= \binom{n-4}{g-3}\left\{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right](n-3)\right. \\
&\qquad \left. - \left[\frac{(n-g-1)(n-g-2)(n-3)}{g(g-1)(g-2)} - \frac{(n-3)}{(n-g)}\right]\right\}.
\end{aligned}
$$

After some algebra $B(n, 1, g, 3)$ can be reduced to

$$
\binom{n-4}{g-3}\frac{(n-2)(n-3)(n-2g)(n-g-1)}{g(g-2)(n-g)}.
$$

Therefore, equality (14) in Theorem 6.1 is satisfied when $q = 3$, $\ell = 1$ and $g \geq 4$.

- For $q = 3$, $\ell = 2$ and $g \geq 4$, we must show that $A(n, 2, g) = B(n, 3, g, 3)$. Notice that

$$
\begin{aligned}
B(n,2,g,3) &= \binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]\left[\frac{(n-3)(n-4)}{2}\right]}{(n-4)}\right. \\
&\qquad \left. - \left[\frac{(n-g-1)(n-g-2)(n-3)}{g(g-1)(g-2)} - \frac{(n-3)}{(n-g)}\right]\right\}.
\end{aligned}
$$

After some algebra $B(n, 2, g, 3)$ can be reduced to

$$
\binom{n-4}{g-3}\frac{(n-1)(n-3)(n-2g)(n-g-2)}{2g(g-1)(n-g)}.
$$

Therefore, equality (14) in Theorem 6.1 is satisfied when $q = 3$, $\ell = 2$ and $g \geq 4$.

- For $q = 3$, $\ell = 3$ and $g \geq 4$, we must show that $A(n, 3, g) = B(n, 3, g, 3)$. Notice that

$$
\begin{aligned}
B(n,3,g,3) &= \binom{n-4}{g-3}\left\{\frac{\left[\frac{(n-g-1)(n-g-2)}{(g-1)(g-2)}-1\right]\left[\frac{(n-3)(n-4)(n-5)}{6}-1\right]}{\frac{(n-4)(n-5)}{2}-1}\right. \\
&\qquad \left. - \left[\frac{(n-g-1)(n-g-2)(n-3)}{g(g-1)(g-2)} - \frac{(n-3)}{(n-g)}\right]\right\}.
\end{aligned}
$$

After some algebra $B(n, 3, g, 3)$ can be reduced to

$$
\binom{n-4}{g-3}\frac{(n-1)(n-2)(g-3)(n-2g)(n-g-3)}{3g(g-1)(g-2)(n-g)}.
$$

Therefore, equality (14) in Theorem 6.1 is satisfied for $q = 3$, $\ell = 3$ and $g \geq 4$.

In the following we prove that equality (18) in the proof of Theorem 6.1 holds for the cases $1 \leq \ell \leq 3$ with $g \geq 4$ and $1 \leq \ell < g \leq 3$. In order to prove (18), we must show that

$$F(n,\ell,g) \triangleq \frac{s_{(n,\ell,g)}\left[\binom{n-5}{\ell-1} - \binom{n-5}{\ell-4}\right] - t_{(n,\ell,g)}\left[\binom{n-5}{g-1} - \binom{n-5}{g-4}\right]}{s_{(n,\ell,g)}\left[\binom{n}{\ell} + \binom{n-4}{\ell} - \binom{n-4}{\ell-4}\right] + t_{(n,\ell,g)}\left[\binom{n}{g} + \binom{n-4}{g-4} - \binom{n-4}{g}\right]}$$

is equal to

$$D(n,\ell,g) \triangleq \frac{\ell(g-\ell)(n-g)(n-2g)(n-2\ell)}{2(n+2\ell-2g)(n-1)(n-2)(n-3)(n-4)}.$$

Recall that in the proof of Theorem 6.1 we have defined

$$a \triangleq s_{(n,\ell,g)}\left[\binom{n-5}{\ell-1} - \binom{n-5}{\ell-4}\right] \qquad b \triangleq t_{(n,\ell,g)}\left[\binom{n-5}{g-1} - \binom{n-5}{g-4}\right]$$

$$c \triangleq s_{(n,\ell,g)}\left[\binom{n}{\ell} + \binom{n-4}{\ell} - \binom{n-4}{\ell-4}\right] \qquad d \triangleq t_{(n,\ell,g)}\left[\binom{n}{g} + \binom{n-4}{g-4} - \binom{n-4}{g}\right].$$

- If $\ell = 1$ and $g \geq 4$ it holds that:

  $$\frac{a}{c} = \frac{1}{2(n-2)}, \qquad \frac{b}{a} = \frac{(n^2 - ng - 6n + 11 + g^2)}{(n-3)(n-4)},$$

  and

  $$\frac{d}{c} = \frac{(2n^2 - 3gn - 3n + 2g^2 + 2)}{(n-g)(n-2g)(n-2)}.$$

  Since

  $$\frac{(a-b)}{(c+d)} = \frac{a(1-\frac{b}{a})}{c(1+\frac{d}{c})} \tag{21}$$

  we have that

  $$F(n,1,g) = \frac{(n-g)(n-2g)(g-1)}{2(n-2g+2)(n-1)(n-3)(n-4)}$$

  and

  $$D(n,1,g) = \frac{(n-g)(n-2g)(g-1)}{2(n-2g+2)(n-1)(n-3)(n-4)}.$$

  Therefore, equality (18) is satisfied.

- If $\ell = 2$ and $g \geq 4$ it holds that:

  $$\frac{a}{c} = \frac{(n-5)}{(n^2-5n+10)}, \qquad \frac{b}{a} = \frac{(n^2 - ng - 6n + 11 + g^2)}{(n-3)(n-5)}$$

  and

  $$\frac{d}{c} = \frac{2(2n^2 - 3gn - 3n + 2g^2 + 2)(n-4)}{(n-g)(n-2g)(n^2-5n+10)}.$$

From (21), we have that

$$F(n,2,g) = \frac{(n-g)(n-2g)(g-2)}{(n-2g+4)(n-1)(n-2)(n-3)}$$

and

$$D(n,2,g) = \frac{(n-g)(n-2g)(g-2)}{(n-2g+4)(n-1)(n-2)(n-3)}.$$

Therefore, equality (18) is satisfied.

- If $\ell = 3$ and $g \geq 4$ we have

$$\frac{a}{c} = \frac{3(n-5)(n-6)}{(n(n-1)(n-2)+(n-4)(n-5)(n-6))}, \quad \frac{b}{a} = \frac{(n^2-ng-6n+11+g^2)}{(n-4)(n-5)}$$

and

$$\frac{d}{c} = \frac{3(n-6)(2n^2-3gn-3n+2g^2+2)}{(n-g)(n-2g)(n^2-6n+20)}.$$

From (21), we have that

$$F(n,3,g) = \frac{3(n-g)(n-2g)(g-3)(n-6)}{2(n-2g+6)(n-1)(n-2)(n-3)(n-4)}$$

and

$$D(n,3,g) = \frac{3(n-g)(n-2g)(g-3)(n-6)}{2(n-2g+6)(n-1)(n-2)(n-3)(n-4)}.$$

Therefore, equality (18) is satisfied.

- If $\ell = 1$ and $g = 2$ it is easy to see that

$$F(n,1,2) = D(n,1,2) = \frac{1}{2(n-1)(n-3)}.$$

- If $\ell = 1$ and $g = 3$ it is easy to see that

$$F(n,1,3) = D(n,1,3) = \frac{(n-6)}{2(n-1)(n-4)}.$$

- If $\ell = 2$ and $g = 3$ it is easy to see that

$$F(n,2,3) = D(n,2,3) = \frac{(n-6)}{2(n-1)(n-2)}.$$

Therefore, equality (18) is satisfied.

B Appendix B

$n \setminus k$	2			3			4			5			6		
	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α
2	$0,1$ $2,1$	$1,1$	2 $1/2$	–	–	–	–	–	–	–	–	–	–	–	–
3	$0,2$ $3,1$	$1,1$	3 $1/3$	$0,1$ $2,1$	$1,1$ $3,1$	4 $1/4$	–	–	–	–	–	–	–	–	–
4	$0,3$ $4,3$	$2,1$	6 $1/3$	$0,2$ $3,1$	$1,1$ $4,2$	6 $1/6$	$0,1$ $2,1$ $4,1$	$1,1$ $3,1$	8 $1/8$	–	–	–	–	–	–
5	$0,6$ $5,4$	$1,1$	10 $3/10$	$0,3$ $4,1$	$1,1$ $5,3$	8 $1/8$	$0,3$ $2,1$ $5,2$	$1,2$ $4,1$	15 $1/15$	$0,1$ $2,1$ $4,1$	$1,1$ $3,1$ $5,1$	16 $1/16$	–	–	–
6	$0,10$ $6,10$	$3,1$	20 $3/20$	$0,4$ $5,1$	$1,1$ $6,4$	10 $1/10$	$0,8$ $3,1$ $6,8$	$1,3$ $5,3$	36 $1/18$	$0,3$ $2,1$ $5,2$	$1,2$ $4,1$ $6,3$	30 $1/30$	$0,1$ $2,1$ $4,1$ $6,1$	$1,1$ $3,1$ $5,1$	32 $1/32$

$n \setminus k$	2			3			4			5			6		
	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α
7	0, 20 7, 15	3, 1	35 2/7	0, 9 5, 1	2, 1 7, 9	30 1/10	0, 20 3, 1 7, 15	1, 6 6, 4	70 3/70	0, 6 2, 1 6, 3	1, 3 5, 1 7, 6	48 1/48	0, 4 2, 2 5, 1 7, 3	1, 3 3, 1 6, 2	70 1/70
8	0, 35 8, 35	4, 1	70 2/7	0, 14 6, 1	2, 1 8, 14	42 2/21	0, 45 4, 1 8, 45	1, 10 7, 10	160 3/80	0, 16 3, 1 7, 5	1, 5 5, 1 8, 16	112 1/56	0, 15 2, 3 6, 3 8, 15	1, 8 4, 1 7, 8	198 1/99
9	0, 70 9, 56	4, 1	126 5/18	0, 20 7, 1	2, 1 9, 20	56 5/56	0, 105 4, 1 9, 84	1, 20 8, 15	315 2/63	0, 35 3, 1 8, 9	1, 9 6, 1 9, 35	200 3/200	0, 45 2, 6 7, 4 9, 36	1, 20 4, 1 8, 15	441 1/147
10	0, 126 10, 126	5, 1	252 5/18	0, 180 7, 2	2, 7 10, 105	420 1/12	0, 224 5, 1 10, 224	1, 35 9, 35	700 1/35	0, 64 3, 1 9, 14	1, 14 7, 1 1, 164	324 1/81	0, 128 3, 5 7, 5 10, 128	1, 35 5, 3 9, 35	1456 1/182
11	0, 210 11, 252	6, 1	462 3/11	0, 75 8, 1	3, 1 11, 75	240 1/12	0, 140 6, 1 11, 168	2, 6 9, 8	770 3/110	0, 162 4, 1 10, 28	1, 28 7, 1 1, 1162	800 9/800	0, 105 3, 2 8, 3 11, 126	1, 24 6, 1 10, 30	1056 5/1056

$n \setminus k$	7			8			9			10			11		
	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α	$j, h_{j,0}$	$j, h_{j,1}$	m, α
7	$0,1$ $2,1$ $4,1$ $6,1$	$1,1$ $3,1$ $5,1$ $7,1$	64 $1/64$	–	–	–	–	–	–	–	–	–	–	–	–
8	$0,4$ $2,2$ $5,1$ $7,3$	$1,3$ $3,1$ $6,2$ $8,4$	140 $1/140$	$0,1$ $2,1$ $4,1$ $6,1$ $8,1$	$1,1$ $3,1$ $5,1$ $7,1$	128 $1/128$	–	–	–	–	–	–	–	–	–
9	$0,9$ $2,2$ $5,1$ $8,5$	$1,5$ $4,1$ $7,2$ $9,9$	252 $1/252$	$0,5$ $2,3$ $4,1$ $7,2$ $9,4$	$1,4$ $3,2$ $6,1$ $8,3$	315 $1/315$	$0,1$ $2,1$ $4,1$ $6,1$ $8,1$	$1,1$ $3,1$ $5,1$ $7,1$ $9,1$	256 $1/256$	–	–	–	–	–	–
10	$0,35$ $2,5$ $6,1$ $9,16$	$1,16$ $4,1$ $8,5$ $10,35$	630 $1/315$	$0,24$ $2,8$ $5,1$ $8,8$ $10,24$	$1,15$ $3,3$ $7,3$ $9,15$	1020 $1/510$	$0,5$ $2,3$ $4,1$ $7,2$ $9,4$	$1,4$ $3,2$ $6,1$ $8,3$ $10,5$	630 $1/630$	$0,1$ $2,1$ $4,1$ $6,1$ $8,1$ $10,1$	$1,1$ $3,1$ $5,1$ $7,1$ $9,1$	512 $1/512$	–	–	–
11	$0,90$ $2,9$ $7,1$ $10,35$	$1,35$ $4,1$ $9,9$ $11,90$	1300 $3/1300$	$0,84$ $2,20$ $5,1$ $9,15$ $11,70$	$1,45$ $3,6$ $8,4$ $10,36$	2541 $1/847$	$0,14$ $2,5$ $5,1$ $8,2$ $10,9$	$1,9$ $3,2$ $6,1$ $9,5$ $11,14$	1180 $1/1180$	$0,6$ $2,4$ $4,2$ $7,1$ $9,3$ $11,5$	$1,5$ $3,3$ $5,1$ $8,2$ $10,4$	1386 $1/1386$	$0,1$ $2,1$ $4,1$ $6,1$ $8,1$ $10,1$	$1,1$ 31 $5,1$ $7,1$ $9,1$ $11,1$	1024 $1/1024$