Visual Cryptography Schemes with Optimal Pixel Expansion

Carlo Blundo[1], Stelvio Cimato[2] and Alfredo De Santis[1]

[1]Dipartimento di Informatica ed Applicazioni
Università degli Studi di Salerno, 84081, Baronissi (SA), Italy

[2]Dipartimento di Tecnologie dell'Informazione
Università degli Studi di Milano, 26013 Crema, Italy

Abstract

A visual cryptography scheme encodes a black & white secret image into n shadow images called shares which are distributed to the n participants. Such shares are such that only qualified subsets of participants can "visually" recover the secret image.

Usually, the reconstructed image will be darker than the background of the image itself. In this paper we consider visual cryptography schemes satisfying the model introduced by Tzeng and Hu (Designs, Codes and Cryptography, Vol. 27, No. 3, pp. 207–227, 2002). In such a model the recovered secret image can be darker or lighter than the background.

We prove a lower bound on the pixel expansion of the scheme and, for $(2, n)$-threshold visual cryptography schemes, we provide schemes achieving the bound. Our schemes improve on the ones proposed by Tzeng and Hu.

Keywords: Visual cryptography, Pixel expansion.

1 Introduction

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

This cryptographic paradigm was introduced by Naor and Shamir in their seminal paper [3]. They analyzed the case of (k, n)-threshold visual cryptography schemes, in which the secret image is visible if any k or more transparencies are stacked together. If fewer than k transparencies are stacked together, then the resulting image will be indistinguishable from random noise. More generally, any set of $k-1$ participants can analyze their collection of shares by any means, but they will obtain no information about the secret image.

In order to implement a visual cryptography scheme, each pixel of the original image is encoded into n version called *shares*, one for each transparency. Each share is composed of m black and white subpixels. When we superimpose two white subpixels we obtain a white subpixel; while, superimposing one black subpixel to any other subpixel we get a black subpixel. Thus, the grey level of the combined share obtained by stacking some transparencies is proportional to the number of black subpixels appearing in it. This grey level is interpreted by the visual system of the users as black or as white in according with some rule of contrast.

In the model introduced by Naor and Shamir the grey level of a "reconstructed" black pixel will be greater than the grey level of a "reconstructed" white one. In other words, the reconstructed image will be darker than the background of the image itself.

In this paper we consider visual cryptography schemes satisfying the model introduced by Tzeng and Hu in [4]. In such a model the recovered secret image can be darker or lighter than the background.

The best way to understand such a new model is by resorting to an example. We want to realize a $(2, 3)$-threshold visual cryptography schemes. Hence, there are three participants, that is $\mathcal{P} = \{1, 2, 3\}$, and any two of them can recover the secret image. We want to encode the secret image "TCS". For this example, the visual cryptography scheme satisfying the model in [4] is described in (5). The original image and the three shares generated by are as follows.

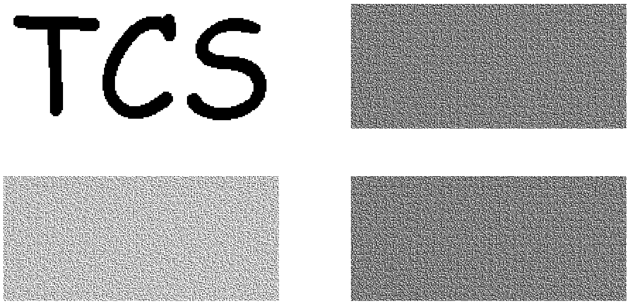

Figure 1: The original image and the shares of a $(2, 3)$-threshold VCS

Three of them look like random patterns and, indeed, no individual share provides any information, even to an infinitely powerful computer, on the original image. If we superimpose the transparencies associated to participants 1 and 2 and to participants 1 and 3, respectively, we get the following result.

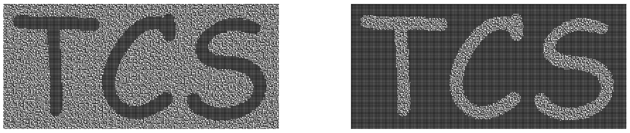

Figure 2: Images reconstructed by participants 1 and 2 and 1 and 3, respectively

In this paper we restrict our attention to $(2, n)$-threshold visual cryptography schemes. We prove a lower bound on the pixel expansion of the scheme and we provide visual cryptography schemes achieving the bound. Our schemes improve, with respect to the pixel expansion, on the ones presented in [4].

2 Model and Notation

Let $\mathcal{P} = \{1, \ldots, n\}$ be a set of elements called *participants*, and let $2^{\mathcal{P}}$ denote the set of all subsets of $\mathcal{P}$. Let $\Gamma_{\mathsf{Qual}} \subseteq 2^{\mathcal{P}}$ and $\Gamma_{\mathsf{Forb}} \subseteq 2^{\mathcal{P}}$, where $\Gamma_{\mathsf{Qual}} \cap \Gamma_{\mathsf{Forb}} = \emptyset$. We refer to members of Γ_{Qual} as *qualified sets* and we call members of Γ_{Forb} *forbidden sets*. The pair $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is called the *access structure* of the scheme.

Define Γ_0 to consist of all the minimal qualified sets:

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

A qualified set X that does not belong to Γ_0, i.e., $X \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$, is referred to as *not-minimal* qualified set.

A (k, n)-threshold VCS is a visual cryptography scheme for the access structure with basis $\Gamma_0 = \{B \subseteq \mathcal{P} : |B| = k\}$.

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

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

1. Any (qualified) set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Qual}}$ can recover the shared image by stacking their transparencies.

Formally, for any $M \in \mathcal{C}_0$, the "or" V of rows $i_1, i_2, \ldots, i_p$ satisfies $w(V) \leq t_X - \alpha(m) \cdot m$; whereas, for any $M \in \mathcal{C}_1$ it results that $w(V) \geq t_X$.

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

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

In the following we recall the definition of visual cryptography scheme provided in [4]. The main difference between the such definition of VCS and the "traditional" one is that the property of contrast of the reconstructed image is changed as the revealed image can be darker or lighter than the background (i.e., some qualified sets recover the original image, while other qualified sets recover the "negative" of the image itself). Moreover, as also done in [4], we assume that only the sets in Γ_0 can recover the shared image by stacking their transparencies. If a set X is a not-minimal qualified (i.e., it belongs to $\Gamma_{\mathsf{Qual}} \backslash \Gamma_0$), then we assume that the participants in X, stacking their transparencies, cannot distinguish a white pixel from a black one. This is formalized by the next definition [4].

Definition 2.2 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set of n participants. Two collections (multisets) of $n \times m$ boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ constitute a* visual cryptography scheme $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS *if there exist the value $\alpha(m)$ and the set $\{(X, t_X)\}_{X \in \Gamma_{\mathsf{Qual}}}$ satisfying:*

1. Any minimal qualified set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_0$ can recover the shared image by stacking their transparencies.
Formally, for any $M \in \mathcal{C}_0$, the "or" V of rows $i_1, i_2, \ldots, i_p$ satisfies $w(V) = t_X$; whereas, either, for any $M \in \mathcal{C}_1$, it results that $w(V) \geq t_X + \alpha(m) \cdot m$ or, for any $M \in \mathcal{C}_1$, it results that $w(V) \leq t_X - \alpha(m) \cdot m$.

2. Any (forbidden) set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Forb}}$ has no information on the shared image.

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

3. Any not minimal qualified set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$, by stacking their transparencies, has no information on the shared image. *Formally, the two collections of $1 \times m$ vectors $\mathcal{V}_t$, with $t \in \{0, 1\}$, obtained by OR-ing the rows $i_1, i_2, \ldots, i_p$ of each matrix in $\mathcal{C}_t$ are indistinguishable in the sense that they contain the same vectors with the same frequencies.*

We see that Condition 1 of Definitions 2.1 and 2.2 are different. According to Definition 2.1 the revealed image is darker than the background; while, according to Definition 2.2 the revealed image can be darker or lighter than the background. Moreover, in this model we rule out the possibility that by stacking all the transparencies of the participants in $X \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$, some information about the secret image is revealed. However, notice that, if a set of participants X is a superset of a minimal qualified set X' and they know the form of the access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$, then, they can recover the shared image by considering only the shares of the set X'. Moreover, when the participants in X do not know the access structure they belong to, they can always recover the original image. Indeed, by inspecting their transparencies all together they can distinguish whether the shares come from a matrix in $\mathcal{C}_0$ or a matrix in $\mathcal{C}_1$.

In view of the above observations we make few considerations about the structure of Γ_{Qual} and Γ_{Forb}. It is clear that any subset of a forbidden subset is forbidden, so Γ_{Forb} is necessarily monotone decreasing. Hence, no superset of a qualified subset is forbidden. Finally, w.l.o.g., we can assume that Γ_{Qual} is monotone increasing that is

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

and we say that Γ_{Qual} is the *closure* of Γ_0.

All 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 2.3 *Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure on a set of n participants. A $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS with relative difference $\alpha(m)$ and set of thresholds $\{(X, t_X)\}_{X \in \Gamma_{\mathsf{Qual}}}$ is realized using the two $n \times m$ basis matrices S^0 and S^1 if the following two conditions hold.*

1. *If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_0$ (i.e., if X is a minimal qualified set), then the "or" V of rows $i_1, i_2, \ldots, i_p$ of S^0 satisfies $w(V) = t_X$; whereas, for S^1 it results that either $w(V) \geq t_X + \alpha(m) \cdot m$ or $w(V) \leq t_X - \alpha(m) \cdot m$.*

2. *If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Forb}}$ (i.e., if X is a forbidden set), then the two $p \times m$ matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots, i_p$ are equal up to a columns permutation.*

3. *If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$, (i.e., X is a qualified set which is not minimal), then the two $1 \times m$ vectors V_0 and V_1, obtained by OR-ing the rows $i_1, i_2, \ldots, i_p$ of S^0 and S^1, respectively, have the same Hamming weight, that is, $w(V_0) = w(V_1)$.*

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.

A visual cryptography scheme $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS which is optimal with respect to the pixel expansion m will be referred to as an *m-optimal VCS*.

3 The Structure of VCS

Before to provide some useful properties of VCS, we need to set up our notation. Let M be a $n \times m$ binary matrix. For $X \subseteq \{1, \ldots, n\}$, let M_X denote the m-vector obtained by considering the *or* of the rows corresponding to the indices in X; whereas $M[X]$ denotes the $|X| \times m$ matrix obtained from M by considering only the rows corresponding to the indices in X. If $X = \{r\}$, then instead of using $M[\{r\}]$ to denote the row r of M we will use the shortened notation $M[r]$. For any binary vector V, with $\overline{w}(V)$ we denote the number of zeroes in V (i.e., the "complement" of the Hamming weight). By abusing of notation, given two matrices A and B having the same number of rows, with $A \cap B = \emptyset$ we denote the fact that the same column does not appear in both matrices. In this case, the matrices A and B are referred as *non-redundant* matrices. Finally, with $A||B$ we denote the matrix obtained by concatenating the matrices A and B.

We restrict our attention to $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS realized by non-redundant basis matrices S^0 and S^1. In this case, if the access structure is not an (n, n)-threshold access structures, we will prove that Condition 3 of Definition 2.3 reduces to $w(S^0_X) = w(S^1_X) = m$, for any $X \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$. We will also prove that the matrix $S = S^0||S^1$ has to contain some predefined sub-matrices. The columns of such sub-matrices are referred to as "unavoidable patterns".

Theorem 3.1 *In any $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS realized by the non-redundant basis matrices S^0 and S^1, for any $X \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$, it holds that*

$$w(S^0_X) = w(S^1_X) = m.$$

Proof. We will prove the theorem by contradiction by showing that if some set $X \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$ does not satisfy $w(S^0_X) = w(S^1_X) = m$, then $S^0 \cap S^1 \neq \emptyset$. We will consider the sets in $\Gamma_{\mathsf{Qual}} \backslash \Gamma_0$ in non-increasing order by size. Let $\mathcal{P} = \{1, \ldots, n\}$ be the set of n participants the access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is realized on. For $1 \leq i \leq n$, let $\mathcal{Q}(i)$ be the family of all qualified sets of size i which are not minimal, i.e., $\mathcal{Q}(i) = \{X \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0 : |X| = i\}$. Since we are considering Γ_{Qual} monotone increasing, it results that if $X \in \mathcal{Q}(i)$, then $X \cup \{j\} \in \mathcal{Q}(i+1)$ for any $j \in \mathcal{P} \backslash X$.
Let $X \in \mathcal{Q}(n)$ (notice that there is only one set in $\mathcal{Q}(n)$ as we do not consider (n, n)-threshold access structures) and let Σ be a VCS for $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ such

that $S^0 \cap S^1 = \emptyset$ and $w(S^0_X) = w(S^1_X) = m_X < m$. In this case, there exist $m - m_X$ columns both in S^0 and S^1 whose entries are all equal to zero. This implies that $S^0 \cap S^1 \neq \emptyset$ which contradicts the hypothesis. Hence, in the scheme Σ we have that $w(S^0_X) = w(S^1_X) = m$, for $X \in \mathcal{Q}(n)$.

If $\mathcal{Q}(n-1) = \emptyset$, then there do not exist qualified sets $X \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$ of cardinality $n-1$. Therefore, there is nothing to prove. If $\mathcal{Q}(n-1) \neq \emptyset$, then, consider any set $X \in \mathcal{Q}(n-1)$ and assume that $w(S^0_X) = w(S^1_X) = m_X < m$. In this case there exist $m - m_X$ columns both in $S^0[X]$ and $S^1[X]$ whose entries are equal to zero. For the sake of simplicity assume these are the first $m - m_X$ columns of both $S^0[X]$ and $S^1[X]$. Let $\{i\} = \mathcal{P} \backslash X$. Since for $Y = \{i\} \cup X \in \mathcal{Q}(n)$ we proved that $w(S^0_Y) = w(S^1_Y) = m$, it must be the case that $S^0[i,1] = \cdots = S^0[i, m-m_X] = 1$ and that $S^1[i,1] = \cdots = S^1[i, m-m_X] = 1$. Therefore, the first $m - m_X$ columns of both S^0 and S^1 are equal. This implies that $S^0 \cap S^1 \neq \emptyset$ which contradicts the hypothesis of the theorem. Hence, in the scheme Σ we have that $w(S^0_X) = w(S^1_X) = m$, for any $X \in \mathcal{Q}(n-1)$, too.

In general, if for some value q, we have that $\mathcal{Q}(n-q) \neq \emptyset$ and that $w(S^0_X) = w(S^1_X) = m$ for any $X \in \mathcal{Q}(n-q+1)$, then we can proceed as follows. Consider any set $X \in \mathcal{Q}(n-q)$ and assume that $w(S^0_X) = w(S^1_X) = m_X < m$. In this case there exist $m - m_X$ columns both in $S^0[X]$ and $S^1[X]$ whose entries are equal to zero. For the sake of simplicity assume these are the first $m - m_X$ columns of both $S^0[X]$ and $S^1[X]$. Since, for any $i \in \mathcal{P} \backslash X$, it holds that $w(S^0_Y) = w(S^1_Y) = m$, where $Y = \{i\} \cup X \in \mathcal{Q}(n-q+1)$, then $S^0[i,j] = S^1[i,j] = 1$, for $1 \leq j \leq m - m_X$ and $i \in \mathcal{P} \backslash X$. Therefore, the first $m - m_X$ columns of both S^0 and S^1 are equal as they contain a zero in position $j \in X$ and a one in position $i \in \mathcal{P} \backslash X$. This implies that $S^0 \cap S^1 \neq \emptyset$ which contradicts the hypothesis of the theorem. Thus, we can conclude that for any $X \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$, it holds that $w(S^0_X) = w(S^1_X) = m$ and the theorem is proved. □

The next corollary is a consequence of the above theorem.

Corollary 3.2 *For any (k,n)-threshold VCS realized by the non-redundant basis matrices S^0 and S^1, there is no column in $S^0||S^1$ of weight less than $n-k$.*

Proof. Let $S = S^0||S^1$. According to Theorem 3.1, for any $X \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$, it holds that $w(S_X) = 2m$. Suppose by contradiction that there is a column in $S^0||S^1$ of weight $t < n-k$. This implies that in such a column there are $n-t > k$ entries, say the first $n-t$, all equal to zero. Hence, $w(S_X) = 2m-1$, where $X = \{1, \ldots, n-t\}$. This contradicts $w(S_X) = 2m$, for any $X \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$. Thus, the corollary holds. □

The next lemma states that if there exists a VCS having basis matrices S^0 and S^1 such that $S^0 \cap S^1 \neq \emptyset$, then we can always construct a new VCS with non-redundant basis matrices $\widehat{S}^0$ and $\widehat{S}^1$.

Lemma 3.3 *If Σ is a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS having contrast $\alpha(m)$ realized by basis matrices S^0 and S^1 such that $S^0 \cap S^1 \neq \emptyset$, then there exists a $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, \widehat{m})$-VCS having contrast $\widehat{\alpha}(\widehat{m}) = \alpha(m) \cdot m / \widehat{m}$ realized by non-redundant basis matrices.*

Proof. Let $R = S^0 \cap S^1$, then the basis matrices S^0 and S^1 are equal, up to a column permutation, to the matrices $\widehat{S}^0||R$ and $\widehat{S}^1||R$, respectively. Assume that the matrix $\widehat{S}^b$, for $b = 0, 1$, has dimension $n \times \widehat{m}$. We will prove that the matrices $\widehat{S}^0$ and $\widehat{S}^1$ satisfy Definition 2.3.
For any $X \in \Gamma_0$ by Condition 1 of Definition 2.3, we have that $w(S^0_X) = w(\widehat{S}^0_X) + w(R_X) = t_X$ and either $w(S^1_X) = w(\widehat{S}^1_X) + w(R_X) \geq t_X + \alpha(m) \cdot m$ or $w(S^1_X) = w(\widehat{S}^1_X) + w(R_X) \leq t_X - \alpha(m) \cdot m$. Setting $\widehat{t}_X = t_X - w(R_X)$ and $\widehat{\alpha}(\widehat{m}) = \alpha(m) \cdot m / \widehat{m}$ we have that $w(\widehat{S}^0_X) = \widehat{t}_X$ and either $w(\widehat{S}^1_X) \geq \widehat{t}_X + \widehat{\alpha}(\widehat{m}) \cdot \widehat{m}$ or $w(\widehat{S}^1_X) \leq \widehat{t}_X - \widehat{\alpha}(\widehat{m}) \cdot \widehat{m}$. Therefore , the matrices $\widehat{S}^0$ and $\widehat{S}^1$ satisfy Condition 1 of Definition 2.3.
For any $X \in \Gamma_{\mathsf{Forb}}$, Condition 2 of Definition 2.3 states that $S^0[X]$ is equal, up to a column permutation, to $S^1[X]$. Therefore, the matrices $\widehat{S}^0[X]$ and $\widehat{S}^1[X]$ are equal, up to a column permutation, too. Hence, the matrices $\widehat{S}^0$ and $\widehat{S}^1$ satisfy Condition 2 of Definition 2.3.
Finally, For any $X \in \Gamma_{\mathsf{Qual}} \backslash \Gamma_0$, Condition 2 of Definition 2.3 states that $w(S^0_X) = w(S^1_X)$. Since $w(S^0_X) = w(\widehat{S}^0_X) + w(R_X)$ and $w(S^1_X) = w(\widehat{S}^1_X) + w(R_X)$, we get that $w(\widehat{S}^0_X) = w(\widehat{S}^1_X)$. Therefore, the matrices $\widehat{S}^0$ and $\widehat{S}^1$ satisfy Condition 3 of Definition 2.3. Thus, the lemma holds.

□

In the following theorem we will prove that the matrices S^0 and S^1 have to contain some predefined patterns which we call *unavoidable patterns*. More precisely, for any VCS the matrix $S^0||S^1$ has to contain some fixed columns determined by Γ_0.

Theorem 3.4 *In any $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS realized by the basis matrices S^0 and S^1, for any $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_0$, either S^0 or S^1 contains at least $\alpha(m) \cdot m$ columns with a '0' in the rows $\{i_1, i_2, \ldots, i_p\}$ and '1's in the other rows.*

Proof. Assume that the VCS is realized by non-redundant basis matrices S^0 and S^1. If this is not the case, then, by applying Lemma 3.3, we can construct a new VCS whose basis matrices have empty intersection and whose pixel expansion $\widehat{m}$ and contrast $\widehat{\alpha}(\widehat{m})$ satisfy $\widehat{\alpha}(\widehat{m}) \cdot \widehat{m} = \alpha(m) \cdot m$. Consider any set of participants $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_0$. From Condition 1 of Definition 2.2, we have that $w(S^0_X) = t_X$ and that either $w(S^1_X) \geq t_X + \alpha(m) \cdot m$ or $w(S^1_X) \leq t_X - \alpha(m) \cdot m$. Assuming that $w(S^1_X) \geq t_X + \alpha(m) \cdot m$, we get $w(S^1_X) - w(S^0_X) \geq \alpha(m) \cdot m$. Therefore, the matrix $S^0[X]$ must contain at least $\alpha(m) \cdot m$ columns with all entries equal to zero. Moreover, by Theorem 3.1, we have that $w(S^0_Y) = w(S^1_Y) = m$, for any Y such that $X \subset Y$. Therefore, the matrix S^0 contains at least $\alpha(m) \cdot m$ columns with a '0' in the rows $\{i_1, i_2, \ldots, i_p\}$ and '1's in the other rows. We can apply the same reasoning as above when $w(S^1_X) \leq t_X - \alpha(m) \cdot m$ proving that the matrix S^1 contains at least $\alpha(m) \cdot m$ columns with a '0' in the rows $\{i_1, i_2, \ldots, i_p\}$ and '1's in the other rows. Thus, the theorem is proved. □

From the above theorem one can easily get that in any visual cryptography scheme realized by non-redundant basis matrices (i.e., $S^0 \cap S^1 = \emptyset$), the number of columns of $S^0||S^1$ is at least $|\Gamma_0| \cdot \alpha(m) \cdot m$. Therefore, since $\alpha(m) \cdot m \geq 1$ and m has to be an integer value, we can immediately get a bound on the pixel expansion for *any* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS as stated by the next theorem.

Theorem 3.5 *In any $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}}, m)$-VCS realized by basis matrices, the pixel expansion satisfies*

$$m \geq \lceil |\Gamma_0|/2 \rceil.$$

We give the following two examples to illustrate the definition of unavoidable patterns and the use of Theorem 3.5, when $\mathcal{P} = \{1,2,3,4\}$.

Example 3.1 Define $\Gamma_0 = \Big\{\{1,2\},\{2,3\},\{3,4\}\Big\}$. The unavoidable patterns are:

$$\begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

The following basis matrices S^0 and S^1 realize a VCS for Γ_0.

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

The unavoidable patterns

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}$$

belongs to S^0; while, the unavoidable pattern

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

belongs to S^1. In this scheme, $m = 3$ and $\alpha(m) = 1/3$. △

Example 3.2 Define $\Gamma_0 = \Big\{\{1,2\},\{2,3\},\{3,4\},\{1,4\}\Big\}$. The unavoidable patterns are:

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

The basis matrices S^0 and S^1 realizing a VCS for Γ_0 are as follows:

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

In this scheme, $m = 2$ and $\alpha(m) = 1/2$. According to Theorem 3.5 the VCS realized by S^0 and S^1 is optimal with respect to the pixel expansion. $\triangle$

Recall that a (k, n)-threshold VCS is a visual cryptography scheme for the access structure with basis $\Gamma_0 = \{B \subseteq \mathcal{P} : |B| = k\}$. In [3] Naor and Shamir proved that for any (n, n)-threshold VCS the pixel expansion satisfies $m \geq 2^{n-1}$. The structure of basis matrices (n, n)-threshold VCS was completely characterized in [2]. The proof of Theorem 7.1 in [2] can easily be modified in order to prove that for any (n, n)-threshold VCS satisfying Definition 2.3 the pixel expansion is lower bounded by 2^{n-1}, too. In the case of (k, n)-threshold access structures, with $k < n$, the next corollary provides a bound on m.

Corollary 3.6 *In any (k, n)-threshold VCS, with $2 \leq k < n$, realized by basis matrices, the pixel expansion satisfies*

$$m \geq \left\lceil \binom{n}{k} \Big/ 2 \right\rceil.$$

In the next section we will see that above bound is tight for $(2, n)$-threshold VCS when $n \equiv 1 \bmod 4$. For the other cases we will provide stronger bounds.

4 Optimal $(2, n)$-threshold VCS

In this section we will prove a bound on the pixel expansion of $(2, n)$-threshold VCS, with $n > 2$, realized by basis matrices. We will show that such bound is tight by presenting $(2, n)$-threshold VCS meeting it.

4.1 The Bound

In this section we prove a lower bound on the pixel expansion stronger than the one provided by Corollary 3.6 when n is even or $n \equiv 3 \bmod 4$.

Theorem 4.1 *In any $(2, n)$-threshold VCS, with $n > 2$, constructed using basis matrices the pixel expansion satisfies*

$$m \geq \begin{cases} \frac{n^2}{4} & \text{if } n \equiv 0 \ mod\ 2 \\ \\ \frac{n(n-1)}{4} & \text{if } n \equiv 1 \ mod\ 4 \\ \\ \frac{n^2-n+6}{4} & \text{if } n \equiv 3 \ mod\ 4 \\ \end{cases}$$

Proof. Assume that n is even and let Σ be a $(2,n)$-threshold VCS constructed using the basis matrices S^0 and S^1. Let S be the binary matrix equal to $S = S^0||S^1$. Because of Condition 2 of Definition 2.3 it results that that both the number of zeroes and the number of ones in any row of S is even. According to Corollary 3.2 all columns in S have weight at least $n-2$. Moreover, from Theorem 3.4, all the $\binom{n}{2}$ distinct columns of weight $n-2$ (i.e., the unavoidable patterns) have to appear in S. Therefore, S is equal, up to a columns permutation to the matrix $A||B$, where A is a $n \times \binom{n}{2}$ matrix composed by all the distinct unavoidable patterns and B is some binary matrix whose columns have weight at least $n-2$.
Notice that, for $1 \le r \le n$, we have that the number of zeroes in $A[r]$ is equal to $n-1$ which is odd. This means that, for $1 \le r \le n$, the matrix B must contain at least a column whose r-th entry is equal to zero. Since all B's columns have weight at least $n-2$, to have that in any row of $A||B$ there is an even number of zeroes, it results that the number of columns in B should be at least $n/2$. Therefore, the number of columns in S is at least $n(n-1)/2 + n/2 = n^2/2$. Hence,

$$m \ge \frac{n^2}{4}.$$

Thus, the theorem is proved for n even.

If $n \equiv 1 \bmod 4$, then we can apply directly Corollary 3.6. So we are left with proving that the last inequality holds.

Consider $n \equiv 3 \bmod 4$ and let Σ be a $(2,n)$-threshold VCS realized by the basis matrices S^0 and S^1. By Corollary 3.6, the pixel expansion is lower bounded by $\lceil n(n-1)/4 \rceil = (n^2-n+2)/4$. We will prove that there does not exist a VCS with pixel expansion equal to $(n^2-n+2)/4$. Therefore, m should be at least $(n^2-n+2)/4+1 = (n^2-n+6)/4$ and the theorem is proved.
Assume by contradiction that Σ has pixel expansion equal to $m = (n^2-n+2)/4$. According to Theorem 3.4, each of the $\binom{n}{2}$ columns of weight $n-2$ has to appear either in S^0 or in S^1. Therefore, since $\binom{n}{2} = 2m-1$, one matrix, say S^0, will contain $m-1 = (n^2-n-2)/4$ of such columns; while, S^1 will comprise the others $m = (n^2-n+2)/4$.
Let U_0 the sub-matrix of S^0 composed of only $m-1$ distinct unavoidable patterns. Now, we prove that there exists at least an index j, with $1 \le j \le n$, such that $\overline{w}(U_0[j]) \le (n-3)/2$. Assume by contradiction that $\overline{w}(U_0[i]) \ge (n-1)/2$ for all i with $1 \le i \le n$. Then, we have that the total number of zeroes in U_0 is at least $n(n-1)/2$ which is a contradiction as, by construction, the total number of zeroes in U_0 is $2(m-1) = (n^2-n-2)/2$. Hence, there exists an index j, with $1 \le j \le n$, such $\overline{w}(U_0[j]) \le (n-3)/2$. Since any row of $U_0||S^1$ (the matrix of all unavoidable patterns) contains $n-1$ zeroes, then, for the index j, we have that

$$\overline{w}(U_0[j]) \le \frac{n-3}{2} \qquad \text{and} \qquad \overline{w}(S^1[j]) \ge n-1-\frac{n-3}{2} = \frac{n+1}{2}.$$

Since $\overline{w}(S^1[j]) - \overline{w}(U_0[j]) \ge 2$ and the matrix S^0 has just one more column besides the columns in U_0, there does not exist a $(2,n)$-threshold VCS realized by the basis matrices S^0 and S^1 with pixel expansion equal to $(n^2 - n + 2)/4$. Hence,

$$m \geq \frac{n^2 - n + 6}{4}.$$

Thus, the theorem holds. $\square$

4.2 Constructions

In this section we provide some constructions for $(2, n)$-threshold VCS. Such constructions are optimal with respect to the pixel expansion as they meet the bound of Theorem 4.1.

In order to present constructions for $(2, n)$-threshold VCSs, we need to set up our notation. If $c \in \{0, 1\}^n$ (i.e., c is a binary vector of length n), then by $c(i)$ we denote the i-th entry of c, where $1 \leq i \leq n$. Moreover, we denote by $c_{i,j} \in \{0, 1\}^n$ the binary column such that $w(c_{i,j}) = n - 2$ and $c(i) = c(j) = 0$. Let I be set such that $I \subseteq \{1, \ldots, n\}^2$. We denote by $M(I)$ the binary matrix *induced* by the set of pairs belonging to I, that is $M(I)$ is formed by the columns $c_{i,j}$ with $(i, j) \in I$. Since, for our construction, the order in which the pairs in I are chosen is immaterial, then the matrix $M(I)$ is one of the $|I|!$ matrices that can be constructed considering, in any order, the pairs belonging to I. Finally, with $\mathcal{UP}(2, n)$ we denote an $n \times \binom{n}{2}$ binary matrix containing all unavoidable patterns for a $(2, n)$-threshold VCS (i.e., $\mathcal{UP}(2, n)$ contains all the columns of weight $n - 2$).

The Case $n \equiv 0$ mod 4 To define the basis matrices of a $(2, n)$-threshold VCS, we will divide the columns of $\mathcal{UP}(2, n)$ in two matrices. The first matrix will contain $n^2/4$ distinct unavoidable patterns. The second matrix will contain all the $n(n-1)/2 - n^2/4$ remaining patters and the duplication of $n/2$ of them. Define the sets I_1, I_2, and I_3 as follows:

$$\begin{aligned}
I_1 &= \{(i, j) : 1 \leq i \leq n/2 \text{ and } (n + 2)/2 \leq j \leq n\} \\
I_2 &= \{(i, j), (i + n/2, j + n/2) : 1 \leq i < j \leq n/2\} \\
I_3 &= \{(i, i + 1) : i = 2p - 1 \text{ with } 1 \leq p \leq n/2\}
\end{aligned}$$

We construct the matrices S^0 and S^1 as depicted in Figure 3.

We now illustrate the realization of the basis matrices of a $(2, n)$-threshold VCS for $n \equiv 0$ mod 4, by considering an example of the construction depicted in Figure 3.

Example 4.1 For $n = 8$, the matrices induced by the sets I_1, I_2, and I_3 are as

- The matrix S^0 is equal to the matrix $M(I_1)$.
- The matrix S^1 is formed by concatenating the matrices $M(I_2)$ and $M(I_3)$.

Figure 3: Basis Matrices of a $(2, n)$-threshold VCS for $n \equiv 0 \bmod 4$

follows:

$$M(I_1) = \begin{bmatrix} 0000111111111111 \\ 1111000011111111 \\ 1111111100001111 \\ 1111111111110000 \\ 0111011101110111 \\ 1011101110111011 \\ 1101110111011101 \\ 1110111011101110 \end{bmatrix} \quad M(I_2) = \begin{bmatrix} 000111111111 \\ 011001111111 \\ 101010111111 \\ 110100111111 \\ 111111000111 \\ 111111011001 \\ 111111101010 \\ 111111110100 \end{bmatrix}$$

$$M(I_3) = \begin{bmatrix} 0111 \\ 0111 \\ 1011 \\ 1011 \\ 1101 \\ 1101 \\ 1110 \\ 1110 \end{bmatrix}.$$

Therefore, the matrix S^0 and S^1 generated by the construction depicted in Figure 3 are:

$$S^0 = \begin{bmatrix} 0000111111111111 \\ 1111000011111111 \\ 1111111100001111 \\ 1111111111110000 \\ 0111011101110111 \\ 1011101110111011 \\ 1101110111011101 \\ 1110111011101110 \end{bmatrix} \quad S^1 = \begin{bmatrix} 0001111111110111 \\ 0110011111110111 \\ 1010101111111011 \\ 1101001111111011 \\ 1111110001111101 \\ 1111110110011101 \\ 1111111010101110 \\ 1111111101001110 \end{bmatrix}.$$

In this scheme, $m = 16$ and $\alpha(m) = 1/16$. △

In the next theorem we prove that the matrices S^0 and S^1 defined by the scheme in Figure 3 realize a $(2, n)$-threshold VCS for $n \equiv 0 \bmod 4$. According to Theorem 4.1 the scheme is optimal with respect to the pixel expansion.

Theorem 4.2 *The matrices S^0 and S^1 defined by the scheme in Figure 3 realize an m-*optimal *$(2, n)$-threshold VCS for $n \equiv 0 \ mod\ 4$.*

Proof. It is immediate to see that both matrices S^0 and S^1 defined by the scheme in Figure 3 have n rows. The number of columns of S^0 is equal to $|I_1| = n^2/4$; while, the number of columns of S^1 is equal to $|I_2| + |I_3| = n(n-2)/4 + n/2 = n^2/4$. Hence, S^0 and S^1 have the same dimensions n and $m = |S^0| = |S^1|$.
To prove that Condition 1 of Definition 2.3 is satisfied, notice that I_1 and I_2 partition the set $\{(i, j) : 1 \leq i \leq n, 1 \leq j \leq n, \text{ and } i \neq j\}$ and that $I_3 \subseteq I_2$. According to the construction in Figure 3, for any set $X = \{i, j\}$, we have that

$$w(S^0_X) = \begin{cases} n^2/4 - 1 & \text{if } (i, j) \in I_1 \\ \\ n^2/4 & \text{if } (i, j) \in I_2 \end{cases}$$

and

$$w(S^1_X) = \begin{cases} n^2/4 & \text{if } (i, j) \in I_1 \\ \\ n^2/4 - 1 & \text{if } (i, j) \in I_2 \backslash I_3 \\ \\ n^2/4 - 2 & \text{if } (i, j) \in I_3. \end{cases}$$

Therefore, Condition 1 of Definition 2.3 is satisfied.
To prove that Condition 2 of Definition 2.3 holds, we will prove that, for any $1 \leq r \leq n$, it holds that $\overline{w}(S^0[r]) = \overline{w}(S^1[r])$. It is immediate to see that for any $1 \leq r \leq n$ there are $n/2$ zeroes in $S^0[r]$. Hence, $\overline{w}(S^0[r]) = n/2$. The matrix S^1 is equal to $M(I_2)||M(I_3)$. Hence, $\overline{w}(S^1[r]) = \overline{w}(M(I_2)[r]) + \overline{w}(M(I_3)[r]) = (n/2 - 1) + 1 = n/2$. Thus, for $1 \leq r \leq n$ we have that $\overline{w}(S^0[r]) = \overline{w}(S^1[r])$ and Condition 2 of Definition 2.3 is satisfied.
Finally, notice that since all columns of both S^0 and S^1 have weight $n - 2$, then, for any set X of participants of size at least three, it holds that $w(S^0_X) = w(S^1_X) = m$. Hence, Condition 3 of Definition 2.3 is satisfied, too. Thus, the matrices S^0 and S^1 defined by the scheme in Figure 3 realize a $(2, n)$-threshold VCS with pixel expansion equal to $n^2/4$. According to Theorem 4.1, such pixel expansion is the smallest achievable and the theorem is proved. □

The Case $n \equiv 1$ mod 4 Notice that, when $n \equiv 1$ mod 4, the matrix $\mathcal{UP}(2, n)$ has an even number of columns and that the number of zeroes in any row of $\mathcal{UP}(2, n)$ is also even and it is equal to $n - 1$. To define the basis matrices of a $(2, n)$-threshold VCS, we will partition the columns of $\mathcal{UP}(2, n)$ into two matrices in such a way that such matrices have the same number of columns and each row has $(n - 1)/2$ entries equal to zero. Define the sets I_1, I_2, I_3, and I_4 as follows

$$I_1 \quad = \quad \{(i, j) : 1 \leq i < j \leq n\}$$

$$\begin{aligned} I_2 &= \{(i,j) : 2 \leq i \leq (n+1)/2 \text{ and } (n+3)/2 \leq j \leq n\} \\ I_3 &= \{(1,j),(1,j+(n-1)/2) : 2 \leq j \leq (n+3)/4\} \\ I_4 &= \{(i,i+(n-1)/2) : 2 \leq i \leq (n+3)/4\} \end{aligned}$$

Notice that the set $M(I_1) = \mathcal{UP}(2,n)$. We construct the matrices S^0 and S^1 as depicted in Figure 4.

- Let I be the set $(I_2 \cup I_3) \backslash I_4$
- The matrix S^0 is equal to the matrix $M(I)$.
- The matrix S^1 is equal to the matrix $M(I_1 \backslash I)$.

Figure 4: Basis Matrices of a $(2,n)$-threshold VCS for $n \equiv 1 \bmod 4$

We now illustrate the realization of the basis matrices of a $(2,n)$-threshold VCS for $n \equiv 1 \bmod 4$, by considering an example of the construction depicted in Figure 4.

Example 4.2 For $n = 9$, the matrices induced by the sets I_2, I_3, and I_4 are as follows:

$$M(I_2) = \begin{bmatrix} 1111111111111111 \\ 0000111111111111 \\ 1111000011111111 \\ 1111111100001111 \\ 1111111111110000 \\ 0111011101110111 \\ 1011101110111011 \\ 1101110111011101 \\ 1110111011101110 \end{bmatrix} \quad M(I_3) = \begin{bmatrix} 0000 \\ 0111 \\ 1011 \\ 1111 \\ 1111 \\ 1101 \\ 1110 \\ 1111 \\ 1111 \end{bmatrix} \quad M(I_4) = \begin{bmatrix} 11 \\ 01 \\ 10 \\ 11 \\ 11 \\ 01 \\ 10 \\ 11 \\ 11 \end{bmatrix}$$

Therefore, the matrix S^0 and S^1 generated by the above construction are:

$$S^0 = \begin{bmatrix} 111111111111110000 \\ 000111111111110111 \\ 111000111111111011 \\ 111111000011111111 \\ 111111111100001111 \\ 111011011101111101 \\ 011111101110111110 \\ 101101110111011111 \\ 110110111011101111 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 000011111111111111 \\ 111101000111111111 \\ 111110011001111111 \\ 011111101010111111 \\ 101111110100111111 \\ 111101111111000111 \\ 111110111111011001 \\ 110111111111101010 \\ 111011111111110100 \end{bmatrix}$$

In this scheme, $m = 18$ and $\alpha(m) = 1/18$. △

In the following theorem we prove that the matrices S^0 and S^1 defined by the scheme in Figure 4 constitute an *m-optimal* $(2, n)$-threshold VCS for $n \equiv 1$ mod 4.

Theorem 4.3 *The matrices S^0 and S^1 defined by the scheme in Figure 4 realize an m-*optimal *$(2, n)$-threshold VCS for $n \equiv 1$ mod 4.*

Proof. It is immediate to see that both matrices S^0 and S^1 defined by the scheme in Figure 4 have n rows. The matrices S^0 and S^1 are a partition of $\mathcal{UP}(2, n)$. Indeed, the matrix $S = S^0||S^1$ is equal, up to a columns permutation, to $\mathcal{UP}(2, n)$. Since

$$I_4 \subseteq I_2 \text{ and } I_2 \cap I_3 = \emptyset \tag{1}$$

the number of columns of S^0 is equal to

$$|S^0| = |I_2| + |I_3| - |I_4| = \frac{(n-1)^2}{4} + \frac{n-1}{2} - \frac{n-1}{4} = \frac{n(n-1)}{4}. \tag{2}$$

As $|S^1| = |\mathcal{UP}(2, n)| - |S^0| = n(n-1)/4$, we get that S^0 and S^1 have the same dimensions n and $m = |S^0| = |S^1| = n(n-1)/4$.
Since S^0 and S^1 constitute a partition of $\mathcal{UP}(2, n)$, we have that for any set X of size two the matrix $S[X]$ contains an unique columns with entries equal to zero. Therefore, either $w(S^0_X) = m$ and $w(S^1_X) = m - 1$ or $w(S^0_X) = m - 1$ and $w(S^1_X) = m4$. Hence, Condition 1 of Definition 2.3 is satisfied.
Notice that, in any row of S there are $n - 1$ entries equal to zero. Hence, to prove that Condition 2 of Definition 2.3 is satisfied, it is enough to prove that $\overline{w}(S^0[r]) = (n - 1)/2$, for $1 \leq r \leq n$. According to (1) and the construction illustrated in Figure 4, one has that

$$\overline{w}(S^0[r]) = \overline{w}(M(I_2)[r]) + \overline{w}(M(I_3)[r]) - \overline{w}(M(I_4)[r]).$$

For $r = 1$, we have that

$$\overline{w}(M(I_2)[r]) = 0,\ \overline{w}(M(I_3)[r]) = \frac{n-1}{2}, \quad \text{and } \overline{w}(M(I_4)[r]) = 0.$$

Hence,

$$\overline{w}(S^0[r]) = \frac{n-1}{2}.$$

For $2 \leq r \leq n$, we have that

$$\overline{w}(M(I_2)[r]) = \frac{n-1}{2}, \overline{w}(M(I_3)[r]) = 1, \quad \text{and } \overline{w}(M(I_4)[r]) = 1$$

Hence,

$$\overline{w}(S^1[r]) = \frac{n-1}{2}.$$

Therefore, Condition 2 of Definition 2.3 is satisfied.
Finally, notice that since all columns of both S^0 and S^1 have weight $n - 2$,

then, for any set X of participants of size at least three, it holds that $w(S^0_X) = w(S^1_X) = m$. Hence, Condition 3 of Definition 2.3 is satisfied, too. Thus, the matrices S^0 and S^1 defined by the scheme in Figure 4 realize a $(2, n)$-threshold VCS with pixel expansion equal to $n(n-1)/4$. According to Theorem 4.1, such pixel expansion is the smallest achievable and the theorem is proved. □

The Case $n \equiv 2$ mod 4 The $(2, 2)$-threshold VCS described by Naor and Shamir [3] satisfies Definition 2.3 and it is an *m-optimal* VCS. For completeness, we report the basis matrices realizing it:

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

For $n \equiv 2 \bmod 4$, $n > 2$, our construction is based on the technique used to realize the $(2, n)$-threshold VCS for $n \equiv 0 \bmod 4$. To define the basis matrices of a $(2, n)$-threshold VCS, we will divide the columns of $\mathcal{UP}(2, n)$ in two matrices. The first matrix will contain $n^2/4$ distinct unavoidable patterns. The second matrix will contain all the $n(n-1)/2 - n^2/4$ remaining patters and the duplication of $n/2$ of them. For $n \equiv 2 \bmod 4$ and $n > 2$, define the set I_1, I_2, I_3, I_4, and I_5 as follows:

$$\begin{aligned}
I_1 &= \{(i, j) : 1 \le i \le n/2 \text{ and } (n+2)/2 \le j \le n\} \\
I_2 &= \{(i, j), (i + n/2, j + n/2) : 1 \le i < j \le n/2\} \\
I_3 &= \{(i, i + n/2) : 1 \le i \le n/2\} \\
I_4 &= \{(i, i + n/2 + 1) : 1 \le i \le n/2 - 1\} \cup \{(n/2, n/2 + 1)\} \\
I_5 &= \{(i, i + 1), (i + n/2, i + 1 + n/2) : 1 \le i \le n/2 - 1\} \cup \\
&\quad \{(1, n/2), (n/2 + 1, n)\}
\end{aligned}$$

Setting $I_6 = I_3$, we can construct the matrices S^0 and S^1 as depicted in Figure 5.

- The matrix S^0 is formed by the columns $c_{i,j}$, where $(i, j) \in (I_1 \cup I_5) \setminus (I_3 \cup I_4)$.
- The matrix S^1 is formed by concatenating the matrix $M(I_6)$ and the matrix formed by the columns $c_{i,j}$, where $(i, j) \in (I_3 \cup I_4) \cup (I_2 \setminus I_5)$.

Figure 5: Basis matrices of a $(2, n)$-threshold VCS for $n \equiv 2 \bmod 4$, $n > 2$

We now illustrate the realization of the basis matrices of a $(2, n)$-threshold VCS for $n \equiv 2 \bmod 4$ and $n > 2$, by considering an example of the construction depicted in Figure 5.

Example 4.3 For $n = 6$, the matrices induced by the sets $I_1, \ldots, I_6$ are as follows:

$$M(I_1) = \begin{bmatrix} 000111111 \\ 111000111 \\ 111111000 \\ 011011011 \\ 101101101 \\ 110110110 \end{bmatrix} \qquad M(I_2) = \begin{bmatrix} 001111 \\ 010111 \\ 100111 \\ 111001 \\ 111010 \\ 111100 \end{bmatrix} \qquad M(I_3) = \begin{bmatrix} 011 \\ 101 \\ 110 \\ 011 \\ 101 \\ 110 \end{bmatrix}$$

$$M(I_4) = \begin{bmatrix} 011 \\ 101 \\ 110 \\ 110 \\ 011 \\ 101 \end{bmatrix} \qquad M(I_5) = \begin{bmatrix} 001111 \\ 100111 \\ 010111 \\ 111001 \\ 111100 \\ 111010 \end{bmatrix} \qquad M(I_6) = \begin{bmatrix} 011 \\ 101 \\ 110 \\ 011 \\ 101 \\ 110 \end{bmatrix}.$$

Therefore, the matrix S^0 and S^1 generated by the above construction are:

$$S^0 = \begin{bmatrix} 011001111 \\ 101100111 \\ 110010111 \\ 101111001 \\ 110111100 \\ 011111010 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 011011011 \\ 101101101 \\ 110110110 \\ 011011110 \\ 101101011 \\ 110110101 \end{bmatrix}.$$

In this scheme, $m = 9$ and $\alpha(m) = 1/9$. $\triangle$

In the following theorem we prove that the matrices S^0 and S^1 described in Figure 5 realize an *m-optimal* $(2, n)$-threshold VCS for $n \equiv 2 \bmod 4$ and $n > 2$.

Theorem 4.4 *The matrices S^0 and S^1 defined by the scheme in Figure 5 realize an m-*optimal *$(2, n)$-threshold VCS for $n \equiv 2$ mod 4 and $n > 2$.*

Proof. It is immediate to see that both matrices S^0 and S^1 defined by the scheme in Figure 5 have n rows. Notice that

$$I_3 \cup I_4 \subseteq I_1, \quad I_1 \cap I_5 = \emptyset, \quad \text{and} \quad I_3 \cap I_4 = \emptyset. \tag{3}$$

Hence, the number of columns of S^0 is equal to

$$|S^0| \quad = \quad |I_1| + |I_5| - |I_3| - |I_4| = \frac{n^2}{4} + n - \frac{n}{2} - \frac{n}{2} = \frac{n^2}{4}.$$

Moreover, notice that

$$I_2 \cap I_3 = \emptyset, \quad I_3 \cap I_4 = \emptyset, \quad I_4 \cap I_2 = \emptyset, \quad \text{and} \quad I_5 \subseteq I_2. \tag{4}$$

Hence, the number of columns of S^1 is equal to

$$|S^1| \quad = \quad |I_6| + |I_3| + |I_4| + |I_2| - |I_5| = \frac{n}{2} + \frac{n}{2} + \frac{n}{2} + \frac{n(n-2)}{4} - n = \frac{n^2}{4}.$$

Therefore, S^0 and S^1 have the same dimensions n and $m = |S^0| = |S^1|$.
To prove that Condition 1 of Definition 2.3 is satisfied notice that, from (3) and (4) we have

$$[(I_1 \cup I_5) \backslash (I_3 \cup I_4)] \cup [(I_3 \cup I_4) \cup (I_2 \backslash I_5)] = (I_1 \cup I_5) \cup (I_2 \backslash I_5) = I_1 \cup I_2.$$

Hence, since $I_3 = I_6$, the matrix $S = S^0 || S^1$ is equal, up to a columns permutation, to the matrix $M(I_1)||M(I_2)||M(I_3)$.
Let $X = \{i,j\}$ with $(i,j) \notin I_3$. Since the matrix $\mathcal{UP}(2,n)$ is equal, up to a columns permutation, to the matrix $M(I_1)||M(I_2)$, then, the column $c(i,j)$ appears once in the matrix S. Thus, either $w(S^0_X) = m$ and $w(S^1_X) = m-1$ or $w(S^0_X) = m-1$ and $w(S^1_X) = m$.
If $X = \{i,j\}$ with $(i,j) \in I_3$, then the column $c(i,j)$ appears twice in the matrix S^1. Hence, $w(S^0_X) = m$ and $w(S^1_X) = m-2$. Thus, Condition 1 of Definition 2.3 is satisfied.
To prove that Condition 2 of Definition 2.3 holds, we will prove that, for any $1 \leq r \leq n$, the number of zeroes in $S^0[r]$ is equal to the number of zeroes in $S^1[r]$ (i.e., $\overline{w}(S^0[r]) = \overline{w}(S^1[r])$). For $1 \leq r \leq n$, we have that

$$\overline{w}(S[r]) = \overline{w}(\mathcal{UP}(2,n)[r]) + \overline{w}(M(I_3)[r]) = (n-1) + 1 = n.$$

For $1 \leq r \leq n$, from (3), we have that

$$\begin{aligned} \overline{w}(S^0[r]) &= \overline{w}(M(I_1)[r]) + \overline{w}(M(I_5)[r]) - \overline{w}(M(I_4)[r]) - \overline{w}(M(I_4)[r]) \\ &= n/2 + 2 - 1 - 1 \\ &= n/2. \end{aligned}$$

Therefore, since $\overline{w}(S^1[r]) = \overline{w}(S[r]) - \overline{w}(S^0[r]) = n/2$, for $1 \leq r \leq n$, we get that $\overline{w}(S^0[r]) = \overline{w}(S^1[r])$ and Condition 2 of Definition 2.3 holds.
Finally, notice that since all columns of both S^0 and S^1 have weight $n-2$, then, for any set X of participants of size at least three, it holds that $w(S^0_X) = w(S^1_X) = m$. Hence, Condition 3 of Definition 2.3 is satisfied, too. Thus, the matrices S^0 and S^1 defined by the scheme in Figure 5 realize, for $n \equiv 2 \bmod 4$ and $n > 2$, a $(2,n)$-threshold VCS with pixel expansion equal to $n^2/4$. According to Theorem 4.1, such pixel expansion is the smallest achievable and the theorem is proved. □

The Case $n \equiv 3$ mod 4 An *m-optimal* $(2,3)$-threshold VCS is described by the following basis matrices.

$$S^0 = \begin{bmatrix} 110 \\ 100 \\ 101 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 110 \\ 001 \\ 110 \end{bmatrix}. \tag{5}$$

To define the basis matrices of a $(2, n)$-threshold VCS for $n \equiv 3 \bmod 4$ and $n > 3$, we will use the matrices induced by the following sets.

$$\begin{array}{rcl}
I_1 & = & \{(i, j) : 1 \leq i < j \leq n\} \\
I_2 & = & \{(i, j) : 2 \leq i \leq (n+1)/2 \text{ and } (n+3)/2 \leq j \leq n\} \\
I_3 & = & \{(i, i + (n-1)/2) : 2 \leq i \leq (n+1)/4\} \\
I_4 & = & \{(1, 2), (1, (n+3)/2)\} \\
I_5 & = & \{(2, (n+3)/2)\} \\
I_6 & = & \{(1, i), (1, i + (n-1)/2) : 2 \leq i \leq (n+1)/4\}.
\end{array}$$

We construct the basis matrices S^0 and S^1 of a $(2, n)$-threshold VCS for $n \equiv 3 \bmod 4$ and $n > 3$ as depicted in Figure 6.

- Let I be the set $I_2 \backslash I_3$.
- The matrix S^0 is formed by concatenating the matrix $M(I_6)$ and the matrix formed by the columns $c_{i,j}$, where $(i, j) \in I \cup I_4$.
- The matrix S^1 is formed by concatenating the matrix $M(I_5)$ and the matrix formed by the columns $c_{i,j}$, where $(i, j) \in I_1 \backslash (I \cup I_6)$.

Figure 6: Basis matrices of a $(2, n)$-threshold VCS for $n \equiv 3 \bmod 4$, $n > 3$

We now illustrate the realization of the basis matrices of a $(2, n)$-threshold VCS for $n \equiv 2 \bmod 4$ and $n > 3$, by considering an example of the construction depicted in Figure 6.

Example 4.4 For $n = 7$, the matrix induced by the set I_1 is $\mathcal{UP}(2, n)$; while, the matrices induced by the sets $I_2, \ldots, I_6$ are as follows:

$$M(I_2) = \begin{bmatrix} 111111111 \\ 000111111 \\ 111000111 \\ 111111000 \\ 011011011 \\ 101101101 \\ 110110110 \end{bmatrix}$$

$$M(I_3) = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} \quad M(I_4) = \begin{bmatrix} 00 \\ 01 \\ 11 \\ 11 \\ 10 \\ 11 \\ 11 \end{bmatrix} \quad M(I_5) = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} \quad M(I_6) = \begin{bmatrix} 00 \\ 01 \\ 11 \\ 11 \\ 10 \\ 11 \\ 11 \end{bmatrix}.$$

Therefore, the matrix S^0 and S^1 generated by the above construction are:

$$S^0 = \begin{bmatrix} 001111111100 \\ 010011111101 \\ 111100011111 \\ 111111100011 \\ 101101101110 \\ 110110110111 \\ 111011011011 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 100001111111 \\ 011110011110 \\ 101110101111 \\ 110111001111 \\ 011111110010 \\ 111011110101 \\ 111101111001 \end{bmatrix}.$$

In this scheme, $m = 12$ and $\alpha(m) = 1/12$. △

In the next theorem we prove that the matrices S^0 and S^1 defined by the scheme in Figure 6 realize a $(2, n)$-threshold VCS for $n \equiv 3 \bmod 4$ and $n > 3$. According to Theorem 4.1 the scheme is optimal with respect to the pixel expansion.

Theorem 4.5 *The matrices S^0 and S^1 defined by the scheme in Figure 6 realize an m-*optimal *$(2, n)$-threshold VCS for $n \equiv 3 \bmod 4$ and $n > 3$.*

Proof. It is immediate to see that both matrices S^0 and S^1 defined by the scheme in Figure 6 have n rows. Notice that

$$I_3 \subset I_2 \text{ and } I_4 \cap I_2 = \emptyset. \tag{6}$$

Hence, the number of columns of S^0 is equal to

$$|S^0| = |I_6| + |I_2| - |I_3| + |I_4| = \frac{n-3}{2} + \frac{(n-1)^2}{4} - \frac{n-3}{4} + 2 = \frac{n^2 - n + 6}{4}.$$

Moreover, notice that

$$I \cup I_6 \subseteq I_1, \; I_6 \cap I_2 = \emptyset, \; \text{ and } I_3 \subseteq I_2. \tag{7}$$

Hence, the number of columns of S^1 is equal to

$$\begin{aligned} |S^1| &= |I_5| + |I_1| - (|I_2| - |I_3| + |I_6|) \\ &= 1 + \frac{n(n-1)}{2} - \frac{(n-1)^2}{4} + \frac{n-3}{4} - \frac{n-3}{2} \\ &= \frac{n^2 - n + 6}{4}. \end{aligned}$$

Therefore, S^0 and S^1 have the same dimensions n and $m = |S^0| = |S^1|$.
To prove that Condition 1 of Definition 2.3 is satisfied, notice that, from (6) and (4) we have

$$[I \cup I_4] \cup [I_1 \backslash (I \cup I_6)] = (I_1 \backslash I_6) \cup I_4$$

and the matrix $S = S^0||S^1$ is equal, up to a columns permutation, to the matrix $M(I_1)||M(I_4)||M(I_5)$.
Let $X = \{i, j\}$ with $(i, j) \in I_1 \backslash (I_4 \cup I_5)$. Since $I_4 \cap I_5 = \emptyset$ and $I_4 \cup I_5 \subseteq I_1$, then, the column $c(i, j)$ appears once in the matrix S. Hence, either $w(S^0_X) = m$ and $w(S^1_X) = m - 1$ or $w(S^0_X) = m - 1$ and $w(S^1_X) = m$.
Consider now the set $X = \{i, j\}$ with $(i, j) \in I_4$. Since $I_4 \subseteq I_1$, then the column $c(i, j)$ appears twice in the matrix S^0. Hence, $w(S^0_X) = m - 2$ and $w(S^1_X) = m$.
Finally, consider the set $X = \{i, j\}$ with $(i, j) \in I_5$. The column $c(i, j)$ appears twice in the matrix S^1. Hence, $w(S^0_X) = m$ and $w(S^1_X) = m - 2$. Thus, Condition 1 of Definition 2.3 is satisfied.
To prove that Condition 2 of Definition 2.3 holds, we will prove that, for any $1 \le r \le n$, the number of zeroes in $S^0[r]$ is equal to the number of zeroes in $S^1[r]$ (i.e, $\overline{w}(S^0[r]) = \overline{w}(S^1[r])$). For $1 \le r \le n$, one has that

$$\overline{w}(S[r]) = \overline{w}(M(I_1)[r]) + \overline{w}(M(I_4)[r]) + \overline{w}(M(I_5)[r]).$$

Hence,

$$\overline{w}(S[r]) \quad = \quad \begin{cases} n+1 & \text{if } i = 1, 2, (n+3)/2 \\ \\ n-1 & \text{otherwise.} \end{cases}$$

Since $I_3 \subseteq I_2$ and $I_4 \cap I_2 = \emptyset$, one has that

$$\overline{w}(S^0[r]) = \overline{w}(M(I_6)[r]) + \overline{w}(M(I_2)[r]) - \overline{w}(M(I_3)[r]) + \overline{w}(M(I_4)[r]).$$

Hence, for $1 \le r \le n$, we get that

$$\overline{w}(S^0[r]) = \begin{cases} \frac{n-3}{2} + 0 - 0 + 2 & \text{if } r = 1 \\ \\ 1 + \frac{n-1}{2} - 1 + 1 & \text{if } r = 2, (n+3)/2 \\ \\ 1 + \frac{n-1}{2} - 1 + 0 & \text{if } 3 \le r \le (n+1)/4 \text{ or } (n+5)/2 \le r \le (3n-1)/4 \\ \\ 0 + \frac{n-1}{2} - 0 + 0 & \text{otherwise.} \end{cases}$$

Thus,

$$\overline{w}(S^0[r]) = \begin{cases} \frac{n+1}{2} & \text{if } r = 1, 2, (n+3)/2 \\ \\ \frac{n-1}{2} & \text{otherwise.} \end{cases}$$

Therefore, since $\overline{w}(S^1[r]) = \overline{w}(S[r]) - \overline{w}(S^0[r]) = \overline{w}(S[r])/2$, for $1 \le r \le n$, we get that $\overline{w}(S^0[r]) = \overline{w}(S^1[r])$ and Condition 2 of Definition 2.3 is satisfied.

Finally, notice that since all columns of both S^0 and S^1 have weight $n-2$, then, for any set X of participants of size at least three, it holds that $w(S^0_X) = m$. Hence, Condition 3 of Definition 2.3 is satisfied, too. Therefore, the matrices S^0 and S^1 described in Figure 6 are the basis matrices of a $(2, n)$-threshold VCS for $n \equiv 3 \bmod 4$ and $n > 3$. According to Theorem 4.1, such pixel expansion is the smallest achievable and the theorem is proved. $\square$

Comparison We have seen that, in order to implement a visual cryptography scheme, each pixel of the secret image is subdivided into m subpixels. Hence, there is a loss of resolution proportional to m. Therefore, schemes with smaller pixel expansion are better. In [4] the authors described a $(2, n)$-threshold visual cryptography scheme having pixel expansion m such that

$$m = \begin{cases} \frac{(n-1)(n+3)}{4} & \text{if } n \text{ is odd} \\ \\ \frac{n(n+2)}{4} & \text{if } n \text{ is even} \end{cases}$$

It is immediate to see that the pixel expansion of the schemes presented in this paper is smaller. Hence, our schemes are better.

Another important measure to measure the goodness of a visual cryptography scheme is the *relative difference*. Schemes with higher relative difference are better. Since, the relative difference of our schemes and of the ones proposed in [4] is equal to $1/m$, then our schemes improves on the relative difference, too.

References

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

[2] 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.

[3] 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.

[4] W.-G. Tzeng and C.-M. Hu, *A New Approach for Visual Cryptography*, Designs, Codes and Cryptography, Vol. 27, No. 3, pp. 207–227, 2002.