Discrete Applied Mathematics 158 (2010) 659–665

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Bounds for visual cryptography schemes☆

Hossein Hajiabolhassan*, Abbas Cheraghi

Department of Mathematical Sciences, Shahid Beheshti University, G.C., P.O. Box 1983963113, Tehran, Iran
Department of Mathematics, Faculty of Khansar, University of Isfahan, Isfahan, Iran

ARTICLE INFO

Article history:
Received 22 October 2008
Received in revised form 3 December 2009
Accepted 15 December 2009
Available online 29 December 2009

Keywords:
Visual cryptography
Secret sharing scheme
Hypergraph
Basis matrices
Pixel expansion
Contrast

ABSTRACT

In this paper, we investigate the best pixel expansion of various models of visual cryptography schemes. In this regard, we consider visual cryptography schemes introduced by Tzeng and Hu (2002) [13]. In such a model, only minimal qualified sets can recover the secret image and the recovered secret image can be darker or lighter than the background. Blundo et al. (2006) [4] introduced a lower bound for the best pixel expansion of this scheme in terms of minimal qualified sets. We present another lower bound for the best pixel expansion of the scheme. As a corollary, we introduce a lower bound, based on an induced matching of hypergraph of qualified sets, for the best pixel expansion of the aforementioned model and the traditional model of visual cryptography scheme realized by basis matrices. Finally, we study access structures based on graphs and we present an upper bound for the smallest pixel expansion in terms of strong chromatic index.

1. Introduction

Visual cryptography schemes (VCS) are a special kind of secret sharing scheme in which secret is an image. For a set $\mathcal{P}$ of n participants, a VCS encrypts a secret image into n transparencies which constitute the shares given to the n participants. The power set of participants is usually divided into *qualified* sets, which can visually recover the secret image by stacking their transparencies without any cryptography knowledge, and *forbidden* sets which have no information on the secret image.

The fascinating idea of visual cryptography was first introduced by Naor and Shamir [12]. Naor and Shamir [12] have proved that the pixel expansion of any visual k out of k scheme must be at least 2^{k-1}. Also, they have presented a visual k out of k scheme with pixel expansion 2^{k-1}.

Most papers on visual cryptography investigate two parameters, the pixel expansion and the contrast. The pixel expansion is the number of subpixels used to encode each pixel of the secret image in a share, that should be as small as possible. The contrast measures the "difference" between a black and a white pixel in the reconstructed image. Several results on the contrast and the pixel expansion of VCSs can be found in [1–4,6,8,12,14]. Finding the best pixel expansion in the different models of VCS is the main challenge in visual cryptography. The problem of determining the best visual contrast (regardless of pixel expansion) is completely resolved [9,10], so that, for the sake of completeness, it is interesting to find the bound for the pixel expansion.

In this paper, we investigate the best pixel expansion of the different models of visual cryptography schemes. In the second section, we present several models of visual cryptography schemes. In the third section, we introduce some lower bounds for the best pixel expansion of different models of visual cryptography schemes. In this regard, we consider visual cryptography schemes introduced by Tzeng and Hu [13]. In such a model, only minimal qualified sets can recover the secret

☆ This paper is partially supported by Shahid Beheshti University.

* Corresponding author at: Department of Mathematical Sciences, Shahid Beheshti University, G.C., P.O. Box 1983963113, Tehran, Iran. Fax: +98 21 22431655.
E-mail addresses: hhaji@sbu.ac.ir (H. Hajiabolhassan), cheraghi@sci.ui.ac.ir (A. Cheraghi).

0166-218X/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2009.12.005

image and that the recovered secret image can be darker or lighter than the background. Blundo et al. [4] introduced a lower bound for the best pixel expansion of this scheme in terms of minimal qualified sets. We present another lower bound for the best pixel expansion of the scheme. As a corollary, we introduce a lower bound, based on an induced matching of hypergraph of qualified sets, for the best pixel expansion of the aforementioned model and the traditional model of visual cryptography realized by basis matrices. Finally, we study access structures based on graphs and we present an upper bound for the smallest pixel expansion in terms of strong chromatic index.

2. Models and notations

First, we mention some of definitions and notations which are referred to throughout the paper. Hereafter, the symbol $\mathcal{P}$ stands for the set of participants. Furthermore, we assume that $\mathcal{P} = \{1, 2, \ldots, n\}$ and let $2^{\mathcal{P}}$ denote the power set of $\mathcal{P}$, i.e., the set of all subsets of $\mathcal{P}$. A family $\mathcal{Q} \subseteq 2^{\mathcal{P}}$ is said to be *monotone* if for any $A \in \mathcal{Q}$ and any $B \subseteq \mathcal{P}$ such that $A \subseteq B$, it holds that $B \in \mathcal{Q}$. Throughout the paper we assume that $\mathcal{F}, \mathcal{Q} \subseteq 2^{\mathcal{P}}$, where $\mathcal{Q} \cap \mathcal{F} = \emptyset$, $\mathcal{Q} \cup \mathcal{F} = 2^{\mathcal{P}}$ and $\mathcal{Q}$ is monotone. The members of $\mathcal{Q}$ and $\mathcal{F}$ are termed *qualified* sets and *forbidden* sets, respectively. Denote the minimal qualified sets of $\mathcal{Q}$ by $\mathcal{Q}_0$. Also, we call $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ the *access structure* of the scheme.

Let $M = M_{n\times m}$ be an $n \times m$ Boolean matrix. The ith row vector of M is denoted by M_i. Set $M_i \circ M_j$ to be the bit-wise "OR" of vectors M_i and M_j. Suppose $X = \{i_1, i_2, \ldots, i_q\} \subseteq \{1, 2, \ldots, n\}$, and define $M_X \stackrel{\text{def}}{=} M_{i_1} \circ M_{i_2} \circ \cdots \circ M_{i_q}$, whereas $M[X] \stackrel{\text{def}}{=} M[X][\{1, \ldots, m\}]$ denotes the $|X| \times m$ matrix obtained from M by considering only the rows corresponding to members of X. Let $A \parallel B$ denote the concatenation of two matrices A and B of the same number of rows. Denote the Hamming weight of row vector v by $w(v)$. For two vectors u and v, denote their inner product by $u \cdot v$. Let T be a set of vectors. The vector space generated by T is denoted by $\text{span}(T)$.

In visual cryptography schemes we assume that the secret image consists of a collection of black and white pixels. Each pixel of secret image appears in n modified versions called shares, one for each transparency, and each share is divided into m black and white subpixels. The m subpixels of shares can be represented by an $n \times m$ Boolean matrix $M = [m_{ij}]$ where $m_{ij} = 1$ if and only if jth subpixel in the ith transparency is black. The resultant shares should meet the properties of visual cryptography. The conventional definition for VCS is as follows.

Definition 1. Let $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ be an access structure where $|\mathcal{P}| = n$. Two collections (multisets) $\mathcal{C}^0$ and $\mathcal{C}^1$ of $n \times m$ Boolean matrices constitute a (Γ, m)–VCS_1 if there exist a value $\alpha(m) > 0$ and a set $\{(X, t_X)\}_{X\in\mathcal{Q}}$ satisfying

1. Any qualified set $X = \{i_1, i_2, \ldots, i_q\} \in \mathcal{Q}$ can recover the shared image by stacking their transparencies. Formally, for any $M \in \mathcal{C}^0$, $\omega(M_X) \leq t_X - \alpha(m) \cdot m$, whereas for any $M' \in \mathcal{C}^1$, $\omega(M'_X) \geq t_X$.
2. Any forbidden set $X = \{i_1, i_2, \ldots, i_q\} \in \mathcal{F}$ has no information on the shared image. Formally, the two collections $\mathcal{D}^t, t \in \{0, 1\}$, of $q \times m$ matrices obtained by restricting each $n \times m$ matrix in $M \in \mathcal{C}^t$ to rows $i_1, i_2, \ldots, i_q$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The value m is called *pixel expansion*, and the value $\alpha(m)$ is termed *contrast*. The first and second conditions are called *contrast* and *security*, respectively. The notation $m_1(\Gamma)$ stands for the minimum value of m for which such a Γ–VCS_1 exists and called *the best pixel expansion* of Γ–VCS_1. □

The most of constructions in this paper are based on two $n \times m$ matrices, S^0 and S^1 called *basis matrices*. In this case, the collections $\mathcal{C}^0$ and $\mathcal{C}^1$ are generated by permuting the columns of the corresponding basis matrices S^0 and S^1, respectively, in all possible ways.

Definition 2. Let $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ be an access structure where $|\mathcal{P}| = n$. A (Γ, m)–VCS_2 is realized using two basis matrices S^0 and S^1 of $n \times m$ Boolean matrices if there exist a value $\alpha(m) > 0$ and a set $\{(X, t_X)\}_{X\in\mathcal{Q}}$ satisfying

1. Any qualified set $X = \{i_1, i_2, \ldots, i_q\} \in \mathcal{Q}$ can recover the shared image by stacking their transparencies. Formally, $\omega(S^0_X) \leq t_X - \alpha(m) \cdot m$, whereas $\omega(S^1_X) \geq t_X$.
2. Any forbidden set $X = \{i_1, i_2, \ldots, i_q\} \in \mathcal{F}$ has no information on the shared image. Formally, the two $q \times m$ matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots, i_q$ are equal up to a column permutation.

The notation $m_2(\Gamma)$ stands for the minimum value of m for which such a Γ–VCS_2 with basis matrices exists and called *the best pixel expansion* of Γ–VCS_2. □

For a given VCS, the collections $\mathcal{C}^0$ and $\mathcal{C}^1$ may have different size. Note that if the collections $\mathcal{C}^0$ and $\mathcal{C}^1$ do not have the same size, then one can obtain, from an arbitrary VCS, a new VCS having the same contrast and pixel expansion, with equally sized $\mathcal{C}^0$ and $\mathcal{C}^1$, see [1]. Hence, we only consider visual cryptography schemes in which $|\mathcal{C}^0| = |\mathcal{C}^1|$. Now, for a given (Γ, m)–VCS_1, it is possible to construct basis matrices S^0 and S^1 for the access structure Γ, by concatenating the matrices of $\mathcal{C}^0$ and the matrices of $\mathcal{C}^1$, respectively. Several constructions have been introduced in [1] to obtain basis matrices for any access structure.

Theorem 1 (*[1]*). *Assume that $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ is an access structure and let Z_M be the family of maximal forbidden sets in $\mathcal{F}$. Then, there exists a (Γ, m) –VCS$_2$ where $m = 2^{|Z_M|-1}$.*

Now, we recall the definition of visual cryptography scheme defined in [13]. In this scheme, only the sets in $\mathcal{Q}_0$ can recover the secret image by stacking their transparencies and that the image, which is revealed by stacking the transparencies of a minimal qualified set, can be darker or lighter than the background. Note that any non-minimal qualified set, by stacking their transparencies, has no information on the shared image, i.e., cannot distinguish a white pixel from a black one. Here is the formal definition [13].

Definition 3. Let $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ be an access structure where $|\mathcal{P}| = n$. A (Γ, m)–VCS$_3$ is realized using two basis matrices S^0 and S^1 of $n \times m$ Boolean matrices if there exist a value $\alpha(m) > 0$ and a set $\{(X, t_X)\}_{X\in\mathcal{Q}_0}$ satisfying

1. Any minimal qualified set $X = \{i_1, i_2, \ldots, i_q\} \in \mathcal{Q}_0$ can recover the shared image by stacking their transparencies. Formally, $\omega(S^0_X) = t_X$, whereas either, $\omega(S^1_X) \geq t_X + \alpha(m) \cdot m$ or, $\omega(S^1_X) \leq t_X - \alpha(m) \cdot m$.
2. Any forbidden set $X = \{i_1, i_2, \ldots, i_q\} \in \mathcal{F}$ has no information on the shared image. Formally, the two $q \times m$ matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots, i_q$ are equal up to a column permutation.
3. Any non-minimal qualified set $X = \{i_1, i_2, \ldots, i_q\} \in \mathcal{Q} \setminus \mathcal{Q}_0$, by stacking their transparencies, has no information on shared image. Formally, the two $1 \times m$ vectors V_0 and V_1, obtained by OR-ing the rows $i_1, i_2, \ldots, i_q$ of the matrix S^0 and S^1, respectively, are indistinguishable in the sense that they have the same Hamming weight.

Also, we will use the notation $m_3(\Gamma)$ to denote the minimum pixel expansion of basis matrices of Γ–VCS$_3$ and called *the best pixel expansion of* VCS$_3$. □

To achieve the smallest pixel expansion in the different models of visual cryptography schemes, we consider the following definition in which the minimal qualified subsets can recover the shared image by stacking their transparencies. Also, the revealed image can be darker or lighter than the background as well. Moreover, we do not mind whether non-minimal qualified subsets can obtain the secret.

Definition 4. Let $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ be an access structure where $|\mathcal{P}| = n$. Two collections (multisets) $\mathcal{C}^0$ and $\mathcal{C}^1$ of $n \times m$ Boolean matrices constitute a (Γ, m)–VCS$_4$ if there exist a value $\alpha(m) > 0$ and a set $\{(X, t_X)\}_{X\in\mathcal{Q}_0}$ satisfying

1. Any minimal qualified set $X = \{i_1, i_2, \ldots, i_q\} \in \mathcal{Q}_0$ can recover the shared image by stacking their transparencies. Formally, for any $M \in \mathcal{C}^0, \omega(M_X) = t_X$, whereas for any $M' \in \mathcal{C}^1$, either, $\omega(M'_X) \geq t_X + \alpha(m) \cdot m$ or, $\omega(M'_X) \leq t_X - \alpha(m) \cdot m$.
2. Any forbidden set $X = \{i_1, i_2, \ldots, i_q\} \in \mathcal{F}$ has no information on the shared image. Formally, the two collections $\mathcal{D}^t$, $t \in \{0, 1\}$, of $q \times m$ matrices obtained by restricting each $n \times m$ matrix in $M \in \mathcal{C}^t$ to rows $i_1, i_2, \ldots, i_q$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The notation $m_4(\Gamma)$ stands for the minimum value of m for which such a Γ–VCS$_4$ exists and called *the best pixel expansion* of Γ–VCS$_4$. □

Most constructions in this paper are realized using basis matrices; hence, we consider the following definition as well.

Definition 5. Let $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ be an access structure where $|\mathcal{P}| = n$. A (Γ, m)–VCS$_5$ is realized using two basis matrices S^0 and S^1 of $n \times m$ Boolean matrices if there exist a value $\alpha(m) > 0$ and a set $\{(X, t_X)\}_{X\in\mathcal{Q}_0}$ satisfying

1. Any minimal qualified set $X = \{i_1, i_2, \ldots, i_q\} \in \mathcal{Q}_0$ can recover the shared image by stacking their transparencies. Formally, $\omega(S^0_X) = t_X$, whereas either, $\omega(S^1_X) \geq t_X + \alpha(m) \cdot m$ or, $\omega(S^1_X) \leq t_X - \alpha(m) \cdot m$.
2. Any forbidden set $X = \{i_1, i_2, \ldots, i_q\} \in \mathcal{F}$ has no information on the shared image. Formally, the two $q \times m$ matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots, i_q$ are equal up to a column permutation.

Also, we will use the notation $m_5(\Gamma)$ to denote the minimum pixel expansion of basis matrices of Γ–VCS$_5$ and called *the best pixel expansion of* VCS$_5$. □

It is instructive to add some notes on different models we have introduced so far. First, VCS$_1$ has been considered. In fact, VCS$_1$ is the traditional model of VCS which was introduced by M. Naor and A. Shamir [12]. Constructing the families $\mathcal{C}^0$ and $\mathcal{C}^1$, mentioned in VCS$_1$, may seem a daunting task. However, it can be more convenient to handle with basis matrices. Hence, basis matrices are used in the most constructions of VCS found in the literature. That is why we consider the models VCS$_2$, VCS$_3$ and VCS$_5$. Finally, we consider VCS$_4$ to achieve the smallest pixel expansion among the different models of visual cryptography schemes.

3. Lower bounds for pixel expansion

In this section, we introduce some lower bounds for the best pixel expansion of the different models of visual cryptography schemes. First, for a given access structure $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$, we present a lower bound for the best pixel expansion of Γ–VCS$_2$ as follows.

Theorem 2. *Let $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ be an access structure and let $\Omega = \{F_1, F_2, \ldots, F_t\}$ be a collection of forbidden sets such that $\bigcup_{i=1}^{t} F_i \in \mathcal{F}$. Also, assume that for any two disjoint non-empty subsets $A, B \subset \Omega$, there exists a forbidden set $F' \in \mathcal{F}$ such that at least one of the following conditions holds*

- *For any $F_i \in A$, $F_i \cup F' \in \mathcal{F}$ and there exists an $F_j \in B$ such that $F_j \cup F' \in \mathcal{Q}$.*
- *For any $F_i \in B$, $F_i \cup F' \in \mathcal{F}$ and there exists an $F_j \in A$ such that $F_j \cup F' \in \mathcal{Q}$.*

Then we have $m_2(\Gamma) \geq t + 1$.

Proof. Let S^0 and S^1 be $n \times m_2(\Gamma)$ the basis matrices of access structure $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$. Consider the following sets

$$T^0 \stackrel{\text{def}}{=} \{S^0_{F_i} \mid 1 \leq i \leq t\},$$

$$T^1 \stackrel{\text{def}}{=} \{S^1_{F_i} \mid 1 \leq i \leq t\}.$$

We claim that the vectors of T^0 (resp. T^1) are linearly independent over the real numbers. On the contrary, suppose that there are some real coefficients a_{F_i} such that $\sum_{i=1}^{t} a_{F_i} S^0_{F_i} = 0$. Define $Y = \bigcup_{i=1}^{t} F_i$. Since $Y \in \mathcal{F}$, $S^0[Y]$ and $S^1[Y]$ are equal up to a permutation of columns; hence, $\sum_{i=1}^{t} a_{F_i} S^1_{F_i} = 0$. Therefore,

$$\sum_{a_{F_i}>0} a_{F_i} S^0_{F_i} = -\sum_{a_{F_j}<0} a_{F_j} S^0_{F_j} \quad \& \quad \sum_{a_{F_i}>0} a_{F_i} S^1_{F_i} = -\sum_{a_{F_j}<0} a_{F_j} S^1_{F_j}.$$

Set $A \stackrel{\text{def}}{=} \{F_j | a_{F_j} < 0\}$ and $B \stackrel{\text{def}}{=} \{F_i | a_{F_i} > 0\}$. Without loss of generality, assume that there exists a forbidden set F' such that for any $F_j \in A$, $F_j \cup F' \in \mathcal{F}$ and there exists a member of B such as F'' such that $F'' \cup F' \in \mathcal{Q}$. We have

$$S^0_{F'} \cdot \sum_{a_{F_i}>0} a_{F_i} S^0_{F_i} = S^0_{F'} \cdot \sum_{a_{F_j}<0} -a_{F_j} S^0_{F_j} \quad \& \quad S^1_{F'} \cdot \sum_{a_{F_i}>0} a_{F_i} S^1_{F_i} = S^1_{F'} \cdot \sum_{a_{F_j}<0} -a_{F_j} S^1_{F_j}. \tag{1}$$

Note that $w(S^0_{F'}) = w(S^1_{F'})$. Also, for any $F_j \in A$, $F' \cup F_j \in \mathcal{F}$; consequently, $S^0[F_j \cup F']$ and $S^1[F_j \cup F']$ are equal up to a permutation of columns. Hence, $S^0_{F'} \cdot S^0_{F_j} = S^1_{F'} \cdot S^1_{F_j}$. Moreover, there exists an $F'' \in B$ such that $F'' \cup F' \in \mathcal{Q}$. Thus,

$$S^0_{F'} \cdot S^0_{F''} > S^1_{F'} \cdot S^1_{F''}.$$

In view of Eqs. (1), one can obtain that for any $F_i \in \Omega$, $a_{F_i} = 0$; accordingly, $\dim(\text{span}(T^0)) = \dim(\text{span}(T^1)) = t$. In addition, $F' \cup Y \in \mathcal{Q}$; therefore, $w(S^0_{F'\cup Y}) \neq w(S^1_{F'\cup Y})$. Also, $w(S^0_{F'}) = w(S^1_{F'})$ and the matrices $S^0[Y]$ and $S^1[Y]$ are equal up to a permutation of columns. Now, it is easy to check that $\dim(\text{span}(T^1 \cup \{S^1_{F'}\})) = t + 1$. On the other hand, $m_2(\Gamma) \geq \dim(\text{span}(T^1 \cup \{S^1_{F'}\}))$. Thus, $m_2(\Gamma) \geq t + 1$. ■

For a given access structure $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$, a lower bound for the best pixel expansion of Γ–VCS$_3$ has been introduced in [4] as follows.

Theorem 3 ([4]). *Let $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ be an access structure. The best pixel expansion of Γ –VCS$_3$ satisfies*

$$m_3(\Gamma) \geq \left\lceil \frac{|\mathcal{Q}_0|}{2} \right\rceil.$$

Note that the aforementioned theorem is not effective when $|\mathcal{Q}_0|$ is small. Now, we present a theorem which can be considered as a counterpart of Theorem 3.

Theorem 4. *Let $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ be an access structure and let $\Omega = \{F_1, F_2, \ldots, F_t\}$ be a collection of forbidden sets such that $\bigcup_{i=1}^{t} F_i \in \mathcal{F}$. Also, assume that for any non-empty subset $A \subset \Omega$, there exist two forbidden sets $F' \in A$ and $F'' \in \mathcal{F}$ such that $F' \cup F'' \in \mathcal{Q}_0$ and for any $F_i \in A \setminus \{F'\}$, $F_i \cup F'' \notin \mathcal{Q}_0$. Then $m_3(\Gamma) \geq t + 1$.*

Proof. It is simple to prove that $m_3(\Gamma) \geq 2$ whenever $t = 1$; hence, assume that $t \geq 2$. Let S^0 and S^1 be $n \times m_3(\Gamma)$ the basis matrices of access structure $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$. Set $F_{t+1} \stackrel{\text{def}}{=} F_1 \cup \cdots \cup F_t$. Consider the following sets

$$T^0 \stackrel{\text{def}}{=} \{S^0_{F_i} \mid 1 \leq i \leq t+1\},$$

$$T^1 \stackrel{\text{def}}{=} \{S^1_{F_i} \mid 1 \leq i \leq t+1\}.$$

We claim that the vectors of T^0 (resp. T^1) are linearly independent over the real numbers. Suppose that there are some real coefficients a_{F_i} such that $\sum_{i=1}^{t+1} a_{F_i} S^0_{F_i} = 0$. Since $F_{t+1} \in \mathcal{F}$, $S^0[F_{t+1}]$ and $S^1[F_{t+1}]$ are equal up to a permutation of columns; consequently, $\sum_{i=1}^{t+1} a_{F_i} S^1_{F_i} = 0$. Set $A \stackrel{\text{def}}{=} \{F_i | i \leq t,\ a_{F_i} \neq 0\}$. If $A = \emptyset$, then the assertion follows easily. Hence, assume that $A \neq \emptyset$ and there exist two forbidden sets $F' \in A$ and $F'' \in \mathcal{F}$ such that $F' \cup F'' \in \mathcal{Q}_0$ and for any $F_i \in A \setminus \{F'\}$, $F_i \cup F'' \notin \mathcal{Q}_0$. We have

$$S^0_{F''} \cdot \sum_{a_{F_i} \neq 0} a_{F_i} S^0_{F_i} = 0 \quad \& \quad S^1_{F''} \cdot \sum_{a_{F_i} \neq 0} a_{F_i} S^1_{F_i} = 0. \tag{2}$$

Note that $w(S^0_{F''}) = w(S^1_{F''})$. Also, for any $F_i \in A \cup \{F_{t+1}\} \setminus \{F'\}$, $F'' \cup F_i \notin \mathcal{Q}_0$; consequently, $S^0_{F''} \cdot S^0_{F_i} = S^1_{F''} \cdot S^1_{F_i}$. Moreover, $F'' \cup F' \in \mathcal{Q}_0$. Thus,

$$S^0_{F''} \cdot S^0_{F'} \neq S^1_{F''} \cdot S^1_{F'}.$$

In view of Eqs. (2), one can obtain that for any $F_i \in A$, $a_{F_i} = 0$; accordingly, $\dim(\text{span}(T^0)) = \dim(\text{span}(T^1)) = t + 1$ which implies that $m_3(\Gamma) \geq t + 1$. ■

In the language of hypergraph theory, for a given access structure $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$, one can introduce a lower bound for the best pixel expansion of Γ–VCS$_2$ and Γ–VCS$_3$ in terms of an induced matching of the hypergraph $(\mathcal{P}, \mathcal{Q})$.

Theorem 5. *Let $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ be an access structure. Also, assume that there exist disjoint qualified sets $A_1, \ldots, A_t$ such that for any qualified set $B \subseteq A_1 \cup \cdots \cup A_t$ one should have $A_i \subseteq B$ for some $1 \leq i \leq t$. Then*

$$\min\{m_2(\Gamma), m_3(\Gamma)\} \geq \sum_{i=1}^{t} 2^{|A_i|-1} - (t-1).$$

Proof. Suppose that S^0 and S^1 are $n \times m_3(\Gamma)$ basis matrices for access structure $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$. Let $|A_i| = r_i$ and $A_i = \{p_{i1}, \ldots, p_{ir_i}\}$. Define $Y_i \stackrel{\text{def}}{=} \{p_{i1}, \ldots, p_{i(r_i-1)}\}$. Consider the non-empty members of power set of Y_i's. Set $\{F_{i1}, \ldots, F_{i(2^{r_i-1}-1)}\} \stackrel{\text{def}}{=} 2^{Y_i} \setminus \emptyset$ such that $|F_{i1}| \leq |F_{i2}| \leq \cdots \leq |F_{i(2^{r_i-1}-1)}|$. Define

$$\Omega \stackrel{\text{def}}{=} \{F_{ij} | 1 \leq i \leq t,\ 1 \leq j \leq 2^{r_i-1} - 1\}.$$

Consider the following ordering for Ω,

$$F_{11} \leq \cdots \leq F_{1(2^{r_1-1}-1)} \leq F_{21} \leq \cdots \leq F_{2(2^{r_2-1}-1)} \leq \cdots \leq F_{t(2^{r_t-1}-1)}.$$

Assume that A is a non-empty subsets of Ω. Without loss of generality, suppose that F_{rs} is the largest member of A. Set $F' \stackrel{\text{def}}{=} A_r \setminus F_{rs}$. It is straightforward to check that for any $F_{ij} \in A \setminus \{F_{rs}\}$ we have $F_{ij} \cup F' \in \mathcal{F}$, whereas $F_{rs} \cup F' \in \mathcal{Q}_0$. In view of Theorem 4, one can conclude that $m_3(\Gamma) \geq \sum_{i=1}^{t} 2^{|A_i|-1} - (t-1)$. Similarly, one can show that $m_2(\Gamma) \geq \sum_{i=1}^{t} 2^{|A_i|-1} - (t-1)$, as desired. ■

Access structure $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ with $|\mathcal{P}| = k$ and $\mathcal{Q} = \{\mathcal{P}\}$ is well known as k out of k scheme. Theorem 5 presents a simple proof that the pixel expansion of basis matrices of k out of k scheme is at least 2^{k-1}.

Corollary 1 *([12]). Let $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ be a k out of k scheme. Then*

$$\min\{m_2(\Gamma), m_3(\Gamma)\} \geq 2^{k-1}.$$

Now, we introduce a lower bound for the best pixel expansion of Γ–VCS$_5$. One can deduce the following theorem whose proof is almost identical to that of Theorem 4 and the proof is omitted for the sake of brevity.

Theorem 6. *Let $\Gamma = (\mathcal{P}, \mathcal{Q}, \mathcal{F})$ be an access structure and let $\Omega = \{F_1, F_2, \ldots, F_t\}$ be a collection of forbidden sets such that $\bigcup_{i=1}^{t} F_i \in \mathcal{F}$. Also, assume that for any non-empty subset $A \subset \Omega$, there exist two forbidden sets $F' \in A$ and $F'' \in \mathcal{F}$ such that $F' \cup F'' \in \mathcal{Q}_0$ and for any $F_i \in A \setminus \{F'\}$, $F_i \cup F'' \in \mathcal{F}$. Then we have $m_5(\Gamma) \geq t$.*

4. Graph access structure

In this section, we study access structures based on graphs. To begin, some definitions are given which are used throughout this section. A graph access structure is an access structure for which the set of participants is the vertex set $V(G)$ of a graph $G = (V(G), E(G))$, and the edge set of G constitutes the minimal qualified subsets of access structure, i.e., the qualified subsets are precisely those containing an edge of G. From G, one can define an access structure $G = (V(G), \mathcal{Q}, \mathcal{F})$ where $\mathcal{Q}_0 = E(G)$.

Throughout the paper the word graph is used for a finite simple graph. A subgraph H of a graph G is said to be induced if for any pair of vertices u and v of H, $\{u, v\}$ is an edge of H if and only if $\{u, v\}$ is an edge of G. Two graphs G and H are called disjoint if they have no vertex in common. A *matching* M_n is a set of n disjoint edges, that is, no two edges share a common vertex. A subgraph of G whose edge set is non-empty and forms a complete bipartite graph is called a *biclique* of G. A *biclique cover* $\mathcal{B}$ of G is a collection of bicliques covering $E(G)$ (every edge of G belongs to at least one biclique of the collection). The *biclique covering number* of G, $bc(G)$, is the fewest number of bicliques among all biclique covers of G.

A *homomorphism* $f : G \longrightarrow H$ from a graph G to a graph H is a map $f : V(G) \longrightarrow V(H)$ such that $\{u, v\} \in E(G)$ implies $\{f(u), f(v)\} \in E(H)$. Notation $\mathrm{Hom}^{\mathrm{e}}(G, H)$ denotes the sets of *onto-edges* homomorphisms from G to H, for more on graph homomorphism see [5,7].

Lemma 1. *Let G and H be two graphs such that $\mathrm{Hom}^{\mathrm{e}}(G, H) \neq \emptyset$. Then $m_1(G) \geq m_1(H)$ and $m_2(G) \geq m_2(H)$.*

Proof. First, we show that $m_1(G) \geq m_1(H)$. Without loss of generality, suppose that H does not have any isolated vertex. Assume that $V(G) = \{1, \ldots, n\}, V(H) = \{1, \ldots, n'\}$, and $\sigma \in \mathrm{Hom}^{\mathrm{e}}(G, H)$. Also, let $\mathcal{C}^0$ and $\mathcal{C}^1$ be two collections (multisets) of $n \times m_1(G)$ Boolean matrices constitute a $(G, m_1(G))$–VCS$_1$. For any $n \times m_1(G)$ matrix M, define $n' \times m_1(G)$ matrix M_σ as follows. For any $1 \leq i \leq n'$, the ith row of M_σ is the vector $M_{\sigma^{-1}(i)}$; i.e., the vector obtained by considering the bit-wise "OR" of the vectors corresponding to participants in $\sigma^{-1}(i)$. Now, construct two collections (multisets) of $n' \times m_1(G)$ Boolean matrices $\mathcal{D}^0$ and $\mathcal{D}^1$ as follows.

$$\mathcal{D}^0 \stackrel{\text{def}}{=} \{M_\sigma | M \in \mathcal{C}^0\} \quad \& \quad \mathcal{D}^1 \stackrel{\text{def}}{=} \{N_\sigma | N \in \mathcal{C}^1\}.$$

It is easy to check that $\mathcal{D}^0$ and $\mathcal{D}^1$ constitute an $(H, m_1(G))$–VCS$_1$. Similarly, one can show that $m_2(G) \geq m_2(H)$, as claimed. ■

Now, we provide an upper bound for $m_4(G)$. First, we specify the exact value of $m_4(M_n)$ as follows.

Lemma 2. *Let G be a graph such that each connected component of G is a biclique or an isolated vertex. Then $m_4(G) = 2$.*

Proof. First, we prove the assertion when G is a matching. Let M_n be a matching with n edges where $V(M_n) = \{1, 2, \ldots, 2n\}$ and $E(M_n) = \{\{2i - 1, 2i\} | 1 \leq i \leq n\}$. Set

$$\mathcal{D}^0 = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

and

$$\mathcal{D}^1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

For $i = 0, 1$, define

$$\mathcal{C}^i \stackrel{\text{def}}{=} \{(A_1^i \| \cdots \| A_n^i)^T | A_j^i \in \mathcal{D}^i,\ 1 \leq j \leq n\},$$

where $(A_1^i \| \cdots \| A_n^i)^T$ means the transpose of the matrix $A_1^i \| \cdots \| A_n^i$. Now, one can check that $\mathcal{C}^0$ and $\mathcal{C}^1$ constitute an $(M_n, 2)$–VCS$_4$; that is, $m_4(M_n) = 2$. Note that adding isolated vertices does not alter the pixel expansion of G. Since if G has isolated vertices, then one can add a zero row to any matrix of $\mathcal{C}^0$ and $\mathcal{C}^1$ corresponding to any isolated vertex. It is readily seen that the new collections of matrices constitute a $(G, 2)$–VCS$_4$. Similarly, if each connected components of G is a biclique or an isolated vertex, then one can show that $m_4(G) = 2$. ■

A strong edge coloring of a graph G is an edge coloring in which every color class is an induced matching; that is, any two vertices belonging to distinct edges with the same color are not adjacent. The strong chromatic index $s'(G)$ is the minimum number of colors in a strong edge coloring of G. It is well-known that $s'(G) \leq 2\Delta(G)^2$, see [11]. Now, we present an upper bound for $m_4(G)$ in terms of strong chromatic index and biclique covering number.

Theorem 7. *Let G be a non-empty graph. Then $m_4(G) \leq \min\{2bc(G), 2s'(G)\}$.*

Proof. It is well-known that $m_4(G) \leq m_1(G) \leq 2bc(G)$, see [1]. Consider a strong edge coloring with $s'(G)$ colors. Let $I_1, \ldots, I_{s'(G)}$ be the color classes of the strong edge coloring. For any $1 \leq i \leq s'(G)$, one can extend any I_i to a spanning subgraph of G, say J_i, such that I_i is an induced subgraph of J_i and $E(J_i) \setminus E(I_i) = \emptyset$. In view of Lemma 2, for any $1 \leq i \leq s'(G)$, there exist two collections $\mathcal{C}_i^0$ and $\mathcal{C}_i^1$ of matrices which constitute a $(J_i, 2)$–VCS$_4$. For $i = 0, 1$, set

$$\mathcal{D}^i \stackrel{\text{def}}{=} \{A_1^i \| \cdots \| A_{s'(G)}^i | A_j^i \in \mathcal{C}_j^i,\ 1 \leq j \leq s'(G)\}.$$

It is easy to see that $\mathcal{D}^0$ and $\mathcal{D}^1$ constitute a $(G, 2s'(G))$–VCS$_4$. ■

A *t-strong biclique covering* of a graph G is an edge covering, $E(G) = \cup_{i=1}^{t} E(H_i)$, where each H_i is a set of disjoint bicliques, say $H_{i1}, \ldots, H_{ir_i}$, such that the graph G has no edges between H_{ik} and H_{ij} for any $1 \leq j < k \leq r_i$. The *strong biclique covering number* $s(G)$ is the minimum number t for which there exists a t-strong biclique covering of G. It is easy to verify that $s(G) \leq \min\{bc(G), s'(G)\}$. The proof of the next theorem is identical to that of Theorem 7 and the proof is omitted for the sake of brevity. Here is a generalization of Theorem 7.

Theorem 8. *Let G be a non-empty graph. Then we have $m_4(G) \leq 2s(G)$.*

Suppose that P_4 is a path with the vertex set $\{v_1, v_2, v_3, v_4\}$ and the edge set $\{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}\}$. Set $F_1 \stackrel{\text{def}}{=} \{v_1\}$ and $F_2 \stackrel{\text{def}}{=} \{v_3\}$. It is easy to see that F_1 and F_2 satisfy Theorem 2; consequently, $m_2(P_4) \geq 3$. Furthermore, it is easy to check that

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

are the basis matrices of $(P_4, 3)$–VCS$_2$. Thus, $m_2(P_4) = 3$ which implies that the lower bound mentioned in Theorem 2 is sharp.

The following corollary is a special case of Theorem 5.

Corollary 2. *Let G be a graph access structure and $e_1, \ldots, e_t$ be an induced matching of G. Then we have*

$$\min\{m_2(G), m_3(G)\} \geq t + 1.$$

Now, we show that $m_3(M_2) = 3$. Consider the following matrices

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

One can check that S^0 and S^1 are the basis matrices of $(M_2, 3)$–VCS$_3$ which implies that the lower bound mentioned in Corollary 2 is sharp.

Acknowledgements

The authors wish to thank the anonymous referees for their invaluable comments.

References

[1] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Information and Computation 129 (1996) 86–106.
[2] C. Blundo, A. De Santis, D.R. Stinson, On the contrast in visual cryptography schemes, Journal of Cryptology 12 (1999) 261–289.
[3] C. Blundo, P. D'Arco, A. De Santis, D.R. Stinson, Contrast optimal threshold visual cryptography schemes, SIAM Journal Discrete Mathematics 16 (2003) 224–261.
[4] C. Blundo, S. Cimato, A. De Santis, Visual cryptography schemes with optimal pixel expansion, Theoretical Computer Science 369 (2006) 169–182.
[5] A. Daneshgar, H. Hajiabolhassan, Graph homomorphims through random walks, Journal of Graph Theory 44 (2003) 15–38.
[6] S. Droste, New results on visual cryptography, in: Proceedings of Advances in Cryptology–CRYPTO 96, in: LNCS, vol. 1109, Springer–Verlag, 1996, pp. 401–415.
[7] P. Hell, J. Nešetřil, Graphs and Homomorphisms, in: Oxford Lecture Series in Mathematics and its Applications, vol. 28, Oxford University press, Oxford, 2004.
[8] T. Hofmeister, M. Krause, H.U. Simon, Contrast-optimal k out of n secret sharing schemes in visual cryptography, computing and combinatorics (Shanghai, 1997), Theoretical Computer Science 240 (2000) 471–485.
[9] M. Krause, H. Ulrich Simon, Determining the optimal contrast for secret sharing schemes in visual cryptography, Combinatorics, Probability and Computing 12 (2003) 285–299.
[10] C. Kuhlmann, H. Ulrich Simon, Construction of visual secret sharing schemes with almost optimal contrast, in: Proceedings of the 11th Annual ACM-SIAM Symposium on Discrete Algorithms, 2000, pp. 262–272.
[11] M. Molloy, B. Reed, A bound on the strong chromatic index of a graph, Journal of Combinatorial Theory. Series B 69 (1997) 103–109.
[12] M. Naor, A. Shamir, Visual cryptography, in: Advances in Cryptology–EUROCRYPT 94, in: Lecture Notes in Computer Science, vol. 950, Springer, Berlin, 1995, pp. 197–202.
[13] W.-G. Tzeng, C.-M. Hu, A new approach for visual cryptography, Designs, Codes and Cryptography 27 (2002) 207–227.
[14] E.R. Verheul, H.C.A. Van Tilborg, Constructions and properties of k out of n visual secret sharing schemes, Designs, Codes and Cryptography 11 (1997) 179–196.