Iranian Journal of Mathematical Sciences and Informatics
Vol. 5, No. 2 (2010), pp 45-54
DOI: 10.7508/ijmsi.2010.02.005

On the Pixel Expansion of Hypergraph Access Structures in Visual Cryptography Schemes

Abbas Cheraghi

Department of Mathematics, Faculty of Khansar, University of Isfahan,
Isfahan, Iran

E-mail: cheraghi@sci.ui.ac.ir

Abstract. In a visual cryptography scheme, a secret image is encoded into n shares, in the form of transparencies. The shares are then distributed to n participants. Qualified subsets of participants can recover the secret image by superimposing their transparencies, but non-qualified subsets of participants have no information about the secret image. Pixel expansion, which represents the number of subpixels in the encoding of the secret image, should be as small as possible. Optimal schemes are those that have the minimum pixel expansion. In this paper we study the pixel expansion of hypergraph access structures and introduce a number of upper bounds on the pixel expansion of special kinds of access structures. Also we demonstrate the minimum pixel expansion of induced matching hypergraph is sharp when every qualified subset is exactly one edge with odd size. Furthermore we explain that the minimum pixel expansion of every graph access structure P_n is exactly $\lceil \frac{n+1}{2} \rceil$. It indicates the lower bound mentioned in [4] is sharp.

Keywords: visual cryptography, secret sharing scheme, hypergraph, basis matrices, pixel expansion.

2000 Mathematics subject classification: 94A62.

Received 22 March 2010; Accepted 07 July 2010

1. Introduction

A visual cryptography scheme (VCS for short) for a set P of n participants is a method to encode a secret image into n shadow images in the form of transparencies, called shares, where each participant in P receives one share. Certain subsets of participants, called qualified sets, can visually recover the secret image, but other subsets of participants, called forbidden sets, have no information on the secret image. This system can be used by anyone without any knowledge of cryptography. A visual recovery for a set $X \subseteq P$ consists of superimposing the shares (transparencies) given to the participants in X. The participants in a qualified set X will be able to see the secret image "visually" and without performing any cryptographic computation. Forbidden sets of participants will have no information on the secret image. This cryptographic paradigm was introduced by Naor and Shamir [6]. They analyzed the case of (k, n)-threshold VCS, in which a black and white secret image is visible if and only if any k transparencies are stacked together. It should be noted that the color white is actually the transparent color. In order to implement a visual cryptography scheme, each pixel of the secret image is subdivided into a certain number m of subpixels. Hence, there is a loss of resolution proportional to m. The pixel expansion m is the most important measure of the goodness of a scheme. Obviously, pixel expansion, which represents the number of subpixels in the encoding of the original image, should be as small as possible. Optimal schemes are those that have the minimum pixel expansion. Another important measure for the goodness of a scheme is the contrast, which is a measure of the quality of the reconstructed image; roughly speaking, the contrast tells us how much the reconstructed image differs from the original one. Most of the work done is focused on black and white VCS, where the secret image to be shared is composed of black and white pixels. Several results on the contrast and the pixel expansion of visual cryptography schemes can be found in [1, 2, 3, 5, 6, 7].

A lower bound has been introduced in [4], based on an induced matching 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. In this paper we apply the scheme mentioned in [6] in order to construct our basis matrices for hypergraph access structure with the minimum pixel expansion presented in [4]. It indicates the lower bound mentioned in [4] is sharp.

Naor and Shamir in their seminal paper [6] provide a construction of black and white (k, k)-threshold schemes with perfect reconstruction of black pixels whose pixel expansion is 2^{k-1}. We will apply such schemes in order to construct our basis matrices with the minimum pixel expansion for hypergraph access structure.

First, we mention some of the definitions and notations which are referred throughout the paper. Let $P = \{1, 2, \ldots, n\}$ be a set of elements called participants and let 2^P denote the set of all subsets of P. A family Q of subsets of P is said to be *monotone* if for any $A \in Q$ and any $B \subseteq P$ such that $A \subseteq B$, it holds that $B \in Q$. Let $Q, F \subset 2^P$, where $Q \cap F = \emptyset$, $Q \cup F = 2^P$. The members of Q and F are referred to as *qualified* sets and *forbidden* sets, respectively. Indicate the minimal qualified sets in Q by *the basis access structure* Q_0. We call $\Gamma = (P, Q, F)$ the *access structure* of the scheme. Define a graph access structure is an access structure in which the vertex set $V(G)$ of a graph $G = (V(G), E(G))$ is the set of participants, and the sets of qualified participants are exactly those including an edge of G. We can define an access structure $G = (V(G), Q, F)$ by specifying that the basis access structure is $Q_0 = E(G)$.

Suppose that $P = \{1, 2, \ldots, n\}$ and $E_i \subseteq P$ for every $1 \leq i \leq r$. A *hypergraph access structure* on P is a family $H = (E_1, E_2, \ldots, E_r)$ of minimal qualified subsets of P satisfying the first two properties:

(1) $E_i \neq \varnothing \quad 1 \leq i \leq r$,

(2) $\bigcup_{i=1}^{r} E_i = P$,

(3) $E_i \cap E_j = \varnothing$ for every $i \neq j$.

Hypergraphs satisfying the third property as well will be called here *induced matchings* of hypergraphs access structure. Let M be an $n \times m$ Boolean matrix and denote the i-th row vector of M by M_i. Let $M_i \circ M_j$ be the bit-wise OR of vectors M_i and M_j. Suppose $X = \{i_1, i_2, \ldots, i_q\}$ is a subset of a participant set $P = \{1, 2, \ldots, n\}$, and define $M_X = M_{i_1} \circ M_{i_2} \circ \cdots \circ M_{i_q}$; whereas $M[X] = M[X][\{1, \ldots, m\}]$ denotes the $|X| \times m$ matrix obtained from M by considering only the rows corresponding to participants in X. Indicate the Hamming weight of row vector v by $w(v)$.

A *visual cryptography scheme* (VCS) is a method to share an image secretly among a given group of participants. If X is qualified then the participants in X can visually recover the secret image SI by stacking their transparencies without any cryptography knowledge and without performing any cryptographic computation. If X is forbidden then its participants have no information on SI. The simplest version of the visual cryptography assumes that the secret image consists of a collection of black and white pixels. Each pixel appears in n versions called shares, one for each transparency. Each share is a collection of m black and white subpixels. The resulting structure can be described by an $n \times m$ Boolean matrix $M = [m_{ij}]$ where $m_{ij} = 1$ if and only if j-th subpixel in the i-th transparency is black. The resultant shares need to satisfy the properties of visual cryptography which will be explain in the next definition. The conventional definition for VCS is as follows.

Definition 1.1. *Let $\Gamma = (P, Q, F)$ be an access structure. Two basis matrices S^0 and S^1 of $n \times m$ Boolean matrices constitute a (Γ, m)-VCS, if there exist a value $\alpha(m) > 0$, an integer number t_X and a set $\{(X, t_X)\}_{X \in Q}$ satisfying*

1. *Any qualified set $X = \{i_1, i_2, \ldots, i_q\} \in Q$ 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 $X = \{i_1, i_2, ..., i_q\} \in F$ 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 value m is called pixel expansion, the value $\alpha(m)$ is called contrast. The first and second conditions are called contrast and security, respectively.

The best way to understand visual cryptography is by resorting to an example.

Example 1.1. *Suppose $P = \{1, 2, 3\}$ and consider the access structure with the basis access structure $Q_0 = \{P\}$. This access structure is equivalent to a 3-out-of-3 threshold structure. The following basis matrices represent a VCS for the access structure on the set of participants P with basis Q_0.*

$$S^0 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \qquad S^1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

In this scheme any pixel of the original image is encoded into four subpixels. Any single share in either S^0 or S^1 is a random choice of two black and two white subpixels, so the analysis of one or two shares (equal to a forbidden set with one or two participants) makes it impossible to distinguish between S^0 and S^1. Three shares of a white pixel have a combined Hamming weight of 3, whereas three shares of a black pixel have a combined Hamming weight of 4, which looks darker. Then it is straightforward to verify that S^0 and S^1 are basis matrices of a VCS for the basis access structure Q_0. In this scheme, $m = 4$ and $\alpha(m) = 1/4$.

For preventing from distort the aspect ratio of the original image, it is convenient to arrange the subpixels in a 2×2 array where each share has the form depicted in Figure 1. These shares correspond to the rows of the basis matrices S^0 and S^1, respectively. The subpixels are disposed in a clockwise fashion starting from the upper-left corner of the 2×2 array. Clearly, to any permutation of the columns of S^0 and S^1 will correspond a new rearrangement of the subpixels into the 2×2 array.

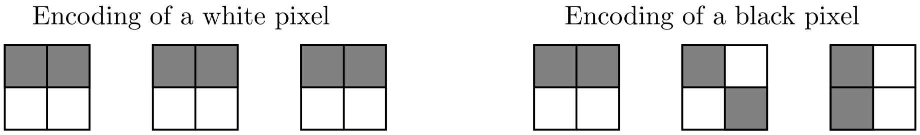

Figure 1. Shares of the 2 out of 3 Threshold VCS

2. Hypergraph access structure

The pixel expansion m is the most important measure of the goodness of a scheme. Obviously, pixel expansion which represents the number of subpixels in the encoding of the secret image, should be as small as possible. Optimal schemes are those that have the minimum pixel expansion. As is always the case, we are interested in the minimum value m, for which a VCS with basis matrices exists and we will use the notation $m^*(\Gamma)$ to denote the minimum expansion of basis matrices of Γ-VCS, this parameter called *the best pixel expansion.* In this paper we study the best pixel expansion of induced matching hypergraph when the qualified subsets are edges with odd size. In addition, we demonstrate the best pixel expansion of graph access structure P_n is exactly $\lceil \frac{n+1}{2} \rceil$. This indicates the lower bound mentioned in [4] is sharp. For a given access structure $\Gamma = (P, Q, F)$, a lower bound for the best pixel expansion has been introduced in [4] as follows.

Theorem 2.1. *([4]) Let $\Gamma = (P, Q, F)$ be an access structure. If there exist forbidden sets $F_1, F_2, \dots, F_t$ and $F'_1, F'_2, \dots, F'_t$ such that $\bigcup\limits_{i=1}^{t} F_i \notin Q$ and for every $1 \leq i \leq t$, $F_i \cup F'_i \in Q$ also for every $j > i$, $F_j \cup F'_i \notin Q$. Then $m^*(\Gamma) \geq t + 1$.*

A lower bound for the best pixel expansion of induced matching hypergraph has been introduced in [4] as follows. The next Theorem follows directly from the Theorem 2.1.

Theorem 2.2. *([4]) Let $\Gamma = (P, Q, F)$ be an access structure in which $Q = (E_1, E_2, \dots, E_r)$ is an induced matching hypergraph. Then $m^*(\Gamma) \geq \sum\limits_{i=1}^{r} 2^{|E_i|-1} - (r-1)$.*

Let rK_2 be a hypergraph matching access structure on the set of $2r$ participants with $|E_i| = 2$ for every $1 \leq i \leq r$. The resulting graph is called the *matching graph access structure.*

The following corollary is a special case of Theorem 2.2.

Corollary 2.1. *([4]) Let rK_2 be a matching graph access structure. Then $m^*(rK_2) \geq r+1$.*

In 1995, Naor and Shamir [6] proposed the k-out-of-k visual cryptography scheme with pixel expansion 2^{k-1} such that only k participants can visually recover the secret through superimposing their transparencies. We apply their scheme in order to construct our basis matrices for hypergraph access structure with the best pixel expansion presented in [4]. Naor and Shamir [6] construction mentions as follows.

Consider the set $P = \{p_1, p_2, \dots, p_k\}$ of k elements and let $\pi_1, \pi_2, \dots, \pi_{2^{k-1}}$ be a list of all the subsets of even size and let $\sigma_1, \sigma_2, \dots, \sigma_{2^{k-1}}$ be a list of all the subsets of P with odd size (the order is not important). Each list defines the following $k \times 2^{k-1}$ matrices S^0 and S^1. For $1 \leq i \leq k$ and $1 \leq j \leq 2^{k-1}$ let $S^0[i,j] = 1$ if and only if $p_i \in \pi_j$ and $S^1[i,j] = 1$ if and only if $p_i \in \sigma_j$.

Lemma 2.1. *([6]) The above scheme is a k-out-of-k scheme with parameters $m = 2^{k-1}$ and $\alpha(m) = 1/2^{k-1}$.*

Now we present an experimental result for a special kind of matching graph access structure which implies that the lower bound mentioned in Corollary 2.1 is sharp for this structure.

Corollary 2.2. *The lower bound $r+1$ is sharp for the non-monotone matching graph access structure in which any qualified subset is exactly one edge of rK_2.*

Proof. Suppose that $P = \{1, 2, \dots, 2r\}$, we construct $2r \times (r+1)$ basis matrices for the access structure by induction on r. When $r = 1$ the matrices $S^0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ and $S^1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ are basis matrices of access structure K_2. Assume that S'^0 and S'^1 are basis matrices of $(r-1)K_2$ scheme with pixel expansion equal to r. Let

$$S^0 = \begin{pmatrix} & & & & 0 \\ & S'^0 & & & \vdots \\ 1 & \cdots & 1 & 1 & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}, \qquad S^1 = \begin{pmatrix} & & & & 0 \\ & S'^1 & & & \vdots \\ 1 & \cdots & 1 & 1 & 0 \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

.

By considering that the last column of matrix S^0 is entirely zero, it is easy to check that matrices S^0 and S^1 are basis matrices with qualified set of participants exactly equal to one edge of rK_2. □

Now under the above construction, the next corollary follows directly from the Corollary 2.1.

Corollary 2.3. *Let rK_2 be a matching graph access structure in which any qualified subset is exactly one edge of rK_2. Then $m^*(rK_2) = r + 1$.*

Let $\Gamma = (P, Q, F)$ be an access structure in which $Q = (E_1, E_2, \dots, E_r)$ is an induced matching hypergraph, where every E_i has odd size for every $1 \le i \le r$. Assume $F = 2^P \setminus \{E_1, E_2, \dots, E_r\}$, it means that this access structure is non-monotone. Now we provide an upper bound for $m^*(\Gamma)$, for this purpose, it is enough to present one scheme by basis matrices with the pixel expansion equal to $\sum_{i=1}^{r} 2^{|E_i|-1} - (r-1)$, which specifies the exact value of $m^*(\Gamma)$.

Corollary 2.4. *Let $\Gamma = (P, Q, F)$ be a non-monotone access structure and $Q = (E_1, E_2, \dots, E_r)$ is an induced matching hypergraph, in which every qualified subset E_i has odd size for every $1 \le i \le r$. Then $m^*(\Gamma) = \sum_{i=1}^{r} 2^{|E_i|-1} - (r-1)$.*

Proof. Theorem 2.2 presents a lower bound for the best pixel expansion of Γ. On the other hand the pixel expansion of every scheme for access structure Γ, actually induces an upper bound for $m^*(\Gamma)$. So it is enough to present one scheme with the pixel expansion equal to $\sum_{i=1}^{r} 2^{|E_i|-1} - (r-1)$, as an upper bound for $m^*(\Gamma)$. Let $P = \{p_1, p_2, \dots, p_n\}$ be a finite set of participants and $Q = (E_1, E_2, \dots, E_r)$ be an induced matching hypergraph in which every E_i has odd size for every $1 \le i \le r$. With applying the Naor and Shamir construction [6], for every subset of participants E_i, there is a $|E_i|$-out-of-$|E_i|$ visual cryptography scheme with pixel expansion $2^{|E_i|-1}$ and basis matrices $S^0_{E_i}$ and $S^1_{E_i}$ for every $1 \le i \le r$. Now we put these $S^0_{E_i}$ and $S^1_{E_i}$ matrices as the main diagonal arrays of matrices D'^0 and D'^1 respectively, and let the other arrays be equal to 1. That is,

$$(1) \qquad D'^j = \begin{pmatrix} S^j_{E_1} & 1 & \cdots & 1 \\ 1 & S^j_{E_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & S^j_{E_r} \end{pmatrix} \qquad for \quad j \in \{0, 1\}.$$

So we have two $n \times \sum_{i=1}^{r} 2^{|E_i|-1}$ matrices. According to the Naor and Shamir construction every column of these matrices labeled by a subset of $E_1, \dots, E_r$, since we can remove all of the columns corresponding to empty subsets from matrix D'^0 and remove all of the columns corresponding to sets E_i from matrix D'^1 for every $1 \le i \le r$. Finally add a column with all the entries equal to 0 to D'^0 matrix for constructing D^0 matrix, and add a column with all the entries equal to 1 to D'^1 matrix for constructing D^1 matrix. It is straightforward to check that matrices D^0 and D^1 are basis matrices of induced matching hypergraph access structure $Q = (E_1, E_2, \dots, E_r)$ with the pixel expansion equal to $\sum_{i=1}^{r} 2^{|E_i|-1} - (r-1)$. Theorem 2.2 shows that this pixel expansion of non-monotone induced matching hypergraph access structure is sharp when the qualified subsets are $E_1, E_2, \dots, E_r$ with odd size.

□

Let P_n is a path graph with the vertex set and the edge set equal to $\{v_1, v_2, \cdots, v_n\}$ and $\{\{v_i, v_{i+1}\} \mid 1 \leq i \leq n-1\}$, respectively. As a motivation, consider the vertex set $V(P_n)$ is the set of participants, such that all of them stay in a queue and everybody is able to make a qualified set only with before or after participant who stays beside him in the queue.

The following Theorem introduces an upper bound on the best pixel expansion of path graph access structure. It shows the lower bound presented in Theorem 2.1 is sharp.

Theorem 2.3. *Let P_n be the graph access structure. Then $m^*(P_n) = \lceil \frac{n+1}{2} \rceil$.*

Proof. Assertion is clear for $n = 1$. Consider the graph access structure P_n, $n \geq 2$, with the vertex set $\{v_1, v_2, \cdots, v_n\}$ and the edge set $\{\{v_i, v_{i+1}\} \mid 1 \leq i \leq n-1\}$. Define $F_i = \{v_{2i}\}$ and $F'_i = \{v_{2i-1}\}$ for each $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$. It is easy to see that F_i's and F'_i's satisfy theorem 2.1, consequently $m^*(P_n) \geq \lceil \frac{n+1}{2} \rceil$. Hence, it is sufficient to present $n \times (\lceil \frac{n+1}{2} \rceil)$ basis matrices of the access structure P_n. The $n \times (\lceil \frac{n+1}{2} \rceil)$ basis matrices of the access structure P_n are constructed by induction. Note that two matrices $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ are basis matrices of access structure P_2. Assume S'^0 and S'^1 are basis matrices of P_{n-1} scheme. Basis matrices S^0 and S^1 of access structure P_n are constructed according to the parity n.

- If n is odd then construct S^0 and S^1 by concatenating row $(0, 0, \dots, 0, 1)$, as n-th row, to both of $(n-1) \times \lceil \frac{n}{2} \rceil$ matrices S'^0 and S'^1, respectively.
- If n is even, set

$$U = \begin{pmatrix} S'^1_{1,1} \\ \vdots \\ S'^1_{n-2,1} \\ 1 \end{pmatrix}, \ where\ S'^1_{i,1}\ is\ (i,1)-entry\ of\ basic\ matrix\ S'^1.$$

First, construct matrices S''^0 and S''^1 by concatenating the matrix U to both of matrices S'^0 and S'^1, respectively, as $\lceil \frac{n+1}{2} \rceil$-th column. Finally, concatenate the matrices $(0, \dots, 0, 1)$ and $(1, 0, \dots, 0)$, as n-th row, to matrices S''^0 and S''^1, respectively. In fact, we have,

$$S^0 = \begin{pmatrix} & & & S'^1_{1,1} \\ & S'^0 & & \vdots \\ & & & S'^1_{n-2,1} \\ & & & 1 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \quad and \quad S^1 = \begin{pmatrix} & & & S'^1_{1,1} \\ & S'^1 & & \vdots \\ & & & S'^1_{n-2,1} \\ & & & 1 \\ 1 & \cdots & 0 & 0 \end{pmatrix}.$$

It is straightforward to check that matrices S^0 and S^1 are basis matrices of access structure of P_n. □

Finally we present a construction for the basis matrices of induced matching hypergraph $Q = (E_1, E_2, \ldots, E_{2r})$ in which $E_1, E_2, \ldots$ and E_r are the qualified subsets with odd size and $E_{r+1}, E_{r+2}, \ldots$ and E_{2r} are the qualified subsets with even size. Let the access structure is non- monotone.

Lemma 2.2. *Let $\Gamma = (P, Q, F)$ be the above access structure with n participants. Then $m^*(\Gamma) \leq \sum_{i=1}^{2r} 2^{|E_i|-1} - r$.*

Proof. Construct two $n \times \sum_{i=1}^{2r} 2^{|E_i|-1}$ matrices D'^0 and D'^1 with the same way presented in the Equation 1 in corollary 2.4. Now remove the columns corresponding to the sets $E_{r+1}, E_{r+2}, \ldots, E_{2r}$ and $E_1, E_2, \ldots, E_r$ from D'^0 and D'^1, respectively. In fact we remove r number of same columns with entries equal to 1 from these matrices. It is easy to check that the new matrices are basis matrices of Γ with the pixel expansion equal to $\sum_{i=1}^{2r} 2^{|E_i|-1} - r$. □

We close by presenting the following open problem for all of the induced matching hypergraphs.

Conjecture: Let $\Gamma = (P, Q, F)$ be an access structure in which $Q = (E_1, E_2, \ldots, E_r)$ is an induced matching hypergraph. Then $m^*(\Gamma) = \sum_{i=1}^{r} 2^{|E_i|-1} - (r - 1)$.

Conclusion

Visual cryptography scheme is widely applied in cryptographic field. In this article, we have given the upper bound for the best pixel expansion of special kind of hypergraph access structure. This result presents a sharp bound for the best pixel expansion of induced matching hypergraph, in which every qualified subset is an edge with odd size, where the access structure is non-monotone. Finally we have introduced the best pixel expansion of basis matrices of graph access structure P_n and proved $m^*(P_n) = \lceil \frac{n+1}{2} \rceil$. This indicates the lower bound mentioned in Theorem 2.1 is sharp. As a further remark, the conjecture indicates that the lower bound referred in [4] is sharp for all induced matching hypergraph access structures.

Acknowledgements. The author wishes to thank the anonymous referee for their invaluable comments. This research was partially supported by the Center of Excellence for Mathematics, University of Isfahan.

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, Visual cryptography for general access structures, *Information and Computation*, **129** (1996), 86–106.

[2] C. Blundo, P. D'Arco, A. De Santis, and D.R. Stinson, Contrast optimal threshold visual cryptography schemes, *SIAM Journal Discrete Mathematics*, **16** (2003), 224–261.

[3] C. Blundo, A. De Santis, and D.R. Stinson, On the contrast in visual cryptography schemes, *Journal of Cryptology*, **12** (1999), 261–289.

[4] H. Hajiabolhassan, and A. Cheraghi, Bounds for visual cryptography schemes, *Discrete Applied Mathematics*, **158** (2010), 659–665

[5] T. Hofmeister, M. Krause and 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.

[6] M. Naor, and A. Shamir, *Visual cryptography*, in: Advances in Cryptology–EUROCRYPT'94, Lecture Notes in Computer Science, **950**, Springer, Berlin, 1995, pp. 197–202.

[7] E.R. Verheul and H.C.A. Van Tilborg, Constructions and properties of k out of n visual secret sharing schemes, *Designs, Codes and Cryptography*, **11** (1997), 179-196.