IUST International Journal of Engineering Science, Vol. **19**, *No.***1-2**, **2008**, *Page* **13-16**
Mathematics & Industrial Engineering Special Issue

MAXIMAL INDEPENDENT SETS FOR THE PIXEL EXPANSION OF GRAPH ACCESS STRUCTURE

Massoud Hadian Dehkordi and Abbas Cheraghi

Abstract :*A visual cryptography scheme based on a given graph G is a method to distribute a secret image among the vertices of G, the participants, so that a subset of participants can recover the secret image if they contain an edge of G, by stacking their shares, otherwise they can obtain no information regarding the secret image. In this paper a maximal independent sets of the graph G was applied to propose a lower bound on the pixel expansion of visual cryptography schemes with graph access structure* $\Gamma(G)$*. In addition a lower bound on the pixel expansion of basis matrices* C_5 *and Peterson graph access structure were presented.*

Keywords: *Sharing Schemes, Visual Cryptography, Graph Access Structure.*

1. Introduction

Secret sharing scheme is a method of distributing a secret data among a set of participants so that only qualified subsets are able to recover the data. If, in addition, unqualified subsets have no extra information, i.e. their joint shares are statistically independent of the secret. A kind of secret sharing scheme called *visual cryptography scheme*, was first proposed by Naor and Shamir in 1994 [1]. They analyzed the case of a k out of n threshold visual cryptography scheme, in which the secret image is visible if and only if k or more transparencies are stacked together. The shared secret is an image such as printed texts, handwritten notes, pictures, etc. It provides an unconditionally secure way to encode the shared secret into shadow images. The decoder is the human visual system. Therefore, one can easily recover the shared secret by using the eyes of human beings.

Suppose that there are n participants, that is $P=\{1,2,\cdots,n\}$, and $Q\subseteq 2^P$ defines the qualified sets. Q is monotonically increasing if $X\in Q$ implies that for all $X\subseteq X'$, $X'\in Q$. The pair $\Gamma=(P,Q)$ is called the *access structure* of the scheme. Define Q_0 to consist of all the *minimal qualify sets*: $Q_0=\{A\in Q: A'\notin Q \ \ for\ \ all\ \ A'\subset A\}$. We assume that the message consists of a collection of black and white pixels. Each pixel appears in n versions called the shares, one for each transparency. Each share is a collection of m black and white sub pixels.

The resulting structure can be described by a $n\times m$ Boolean matrix $S=[s_{ij}]$ where $s_{ij}=1$ if and only if the j-th sub pixel in the i-th transparency is black. Therefore the grey level of the combined shares, obtained by stacking the transparencies $i_1,i_2,\cdots,i_s$ is proportional to the Hamming weight $\omega(V)$ such that, m −vector $V=OR(r_{i_1},r_{i_2},\cdots,r_{i_s})$, where $r_{i_1},r_{i_2},\cdots,r_{i_s}$ ($s\le n$) 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 rules of contrast.

Definition 1.1 Let $\Gamma=(P,Q)$ be an access structure on a set of n participants. A VCS with relative difference $\alpha(m)$, positive integer t_X and set of thresholds $\{(X,t_X)\}_{X\in Q}$ is realized using the two $n\times m$ basis matrices S^0 and S^1 if the following two conditions hold.

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

Paper first received Jun. 03, 2007 and in revised form March. 03, 2008.
Massoud Hadian Dehkordi & Abbas Cheraghi, Department of Mathematics, Iran University of Science & Technology, mhadian@iust.ac.ir, a_cheraghi@iust.ac.ir

Each pixel of the original image will be encoded into n pixels, each of which consists of m sub pixels. To share a white (black, respectively) pixel, we choose one matrix obtained by permuting the columns of the S^0 (S^1, respectively), and distribute row i to participant i. The chosen matrix defines the m sub pixels in each of the n transparencies.

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.

The value $\alpha(m)$ is called *relative difference*; the number $\alpha(m)\cdot m$ is referring to as the *contrast* of the image. We want the contrast to be as large as possible and at least one, that is, $\alpha(m) \geq 1/m$. In particular, several results on the contrast and the pixel expansions of VCSs can be found in [1- 6].

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. Matrices S^0 and S^1 called *basis matrices*.

In most constructions, there is a function *f* such that the combined shares from every unqualified subset with *q* participants consist of the V's with $\omega(V) = f(q)$ with uniform probability distribution. Such a scheme is called a *uniform scheme*.

Let *G* be a graph, we denoted the set of its vertices by *V*, and the number of the vertices by *n*. A subset *U* of *V* is independent or stable, if there is no edge between vertices in *U*.

The *complete multipartite graph* $K_{n_1 n_2 \cdots n_t}$ is a graph on $\sum_{i=1}^{t} n_i$ vertices, in which the vertex set is partitioned into subsets of size n_i *(1≤i≤t), the parts*, such that *vw* is an edge if and only if *v* and *w* are in different parts. We can define an access structure Γ*(G)* by specifying that the minimal qualified set is *E(G)*.

Thus a subset X of participants is qualified set if the induced sub graph *G[X]* contains at least one edge (otherwise X is unqualified). As always is the case, we are interested in the minimum value m for which such a VCS exists.

We will use the notation $m^*(\Gamma)$ to denote the minimum value of expansion of Γ-VCS with basis matrices and called *the best pixel expansion*. The best way to understand visual cryptography is by restoring to an example.

Example 1.2 Suppose P = {1, 2, 3, 4} and consider the access structures with basis Q_0= {{1, 3}, {1, 4}, {2, 3}, {2, 4}}, then one can stipulate that all independent subsets of *V(G)* are unqualified. This access structure is based on the complete bipartite graph with 4 vertices, depicted in Figure 1.

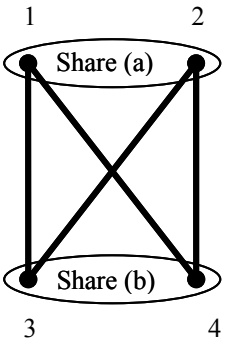
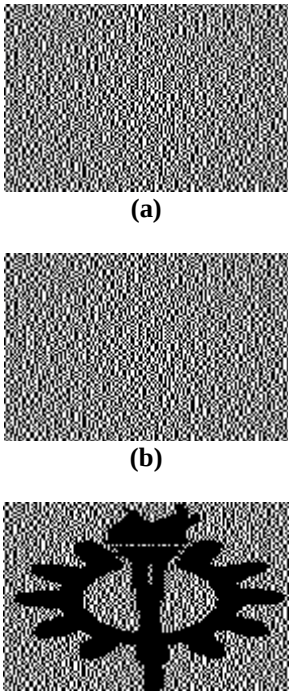


Fig 1. Complete bipartite graph $K_{2,2}$

The participants 1 and 2 receive share (a) and the participants 3 and 4 receive share (b), depicted in Figure 2. So every qualified set in Q_0 can recover the image by stacking shares (a) and (b). The Figure 2 (c) is stacked of (a) and (b).



(a)

(b)

(c)

Fig 2. The shares of a complete bipartite graph access structure and the reconstructed image (c) by shares (a) and (b)

Define S^0 and S^1 as follows:

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

Any single share in either S^0 or S^1 is a random choice of one black and one white sub pixels. Any two shares of a white pixel have a combined Hamming weight of 1, whereas any two shares of a black pixel have a combined Hamming weight of 2, which looks darker. The visual difference between the two cases becomes clearer as we stack additional transparencies. Then it is

straightforward to verify that S^0 and S^1 are basis matrices of a VCS for the access structure Γ ($K_{2,2}$). In this scheme, m = 2 and $\alpha(m) = 1/2$. In section 2 maximal independent sets of the graph G was applied to propose a lower bound on the pixel expansion of visual cryptography schemes with graph access structure $\Gamma(G)$, and also the lower bound on the pixel expansion of basis matrices C_5 and Peterson graph access structure were presented in this section.

2. Lower Bounds on the Pixel Expansion

In this section we studied access structure based on graphs and obtain a lower bound on the pixel expansion of each graph access structure. More background information about optimal pixel expansion can be found in [2- 3, 5]. The *complete graph* K_n is the graph on *n* vertices in which any two vertices are joined by an edge. Note that the complete graph K_n can be thought of as a complete multipartite graph with *n* parts of size 1. In the case where $G=K_n$, it is equivalent to a 2 out of *n* threshold access structure.

Theorem 2.1 The best pixel expansion $m^*(K_n)$ is the smallest integer *m* such that $n \le \left(\left\lfloor \frac{m}{\lfloor \frac{m}{2} \rfloor} \right\rfloor \right)$. [1]

Thus $m^*(K_2)= 2$; $m^*(K_3)=3$; $m^*(K_n)= 4$ for n=4, 5, 6; $m^*(K_n)= 5$ for n= 7, 8, 9, 10; etc. In this theorem we obtain a lower bound on the value of $m^*(K_n)$ which is met with equality when the VCS for Γ is constructed from a Sperner family in a ground set of *m* elements. In such a scheme we have $\alpha(m) = 1/m$.

Theorem 2.2 Let *G* be the graph with the number of maximal independent sets *l*, then $m^*(\Gamma(G)) \ge t$, whereas *t* is the smallest integer such that $l \le \left(\left\lfloor \frac{t}{\lfloor \frac{t}{2} \rfloor} \right\rfloor \right)$

Proof. Let *G* be a graph with the vertex set *V(G)*, the edge set *E(G)* and the distinct maximal independent sets $P_1, P_2, ..., P_l$, in which $P_i \subseteq V(G)$ for every $1 \le i \le l$.

Suppose that $\Gamma(G)$ is an access structure such that every minimal qualified set is an edge of *G*. We claim that for every visual cryptography scheme constructed on $\Gamma(G)$ with the pixel expansion $m(\Gamma(G))$, we can construct 2 out of *l* scheme with the same pixel expansion.

In fact by stacking the transparencies of the participants in P_i (for every $1 \le i \le l$), we obtain the *i*-th share of a 2 out of *l* scheme. As the union of every two distinct maximal independent sets in *G* contains at least an edge of *G*, therefore the new *l* shares construct the transparencies of a 2 out of *l* scheme. So the pixel expansion of graph access structure $\Gamma(G)$ is at least $m^*(K_l)$. On the other hand, Theorem 2.1 implies that $m^*(K_l) \ge t$, whereas *t* is the smallest integer such that $l \le \left(\left\lfloor \frac{t}{\lfloor \frac{t}{2} \rfloor} \right\rfloor \right)$, thus $m^*(\Gamma(G)) \ge t$. ■

Corollary 2.3 Let C_5 be a circle with *5* vertices, then $m^*(C_5) \ge 5$.

Proof. Let $V(C_5)=\{1, 2, 3, 4, 5\}$ and edge set $E(C_5)=\{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{5, 1\}\}$, so C_5 has at most *5* maximal independent sets *{1, 3}, {1, 4}, {2, 4}, {2, 5}, {3, 5}*. By stacking transparencies *{1, 3}* we obtain the first share and so on. It is easy to check that the 5 new shares form the *2* out of *5* schemes, hence $m^*(C_5) \ge m^*(K_5)$. Also Theorem 2.1 implies that $m^*(K_5) \ge 5$, so $m^*(C_5) \ge 5$.

Consider the "Peterson graph" *P*, depicted in Figure 3. It is also the Kneser graph *KG* (5, 2); this means that whose vertices are the 2-element subsets of a 5-element set and connecting two vertices by an edge if the corresponding 2-element subsets are disjoint from each other.

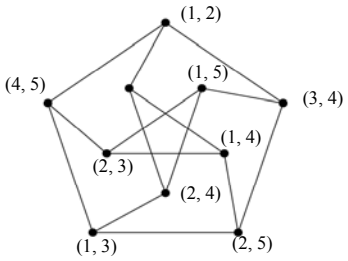


Fig 3. The peterson graph as the kneser graph *KG* (5, 2)

Corollary 2.4 The best pixel expansion for the Peterson graph access structure is at least 6.

Proof. Notice that maximal independent sets of the Kneser graph *KG* (5, 2) are $P_1, P_2, ..., P_{15}$ such as follows:

- $P_i=\{(i,2), (i,3), (i,4), (i,5)\}$ for every $1 \le i \le 5$
- $P_i= \{(i, j), (i, k), (j, k)\}$ for every distinct triple $\{i, j, k\} \subset \{1,2,3,4,5\}$. The number of this case is $\binom{5}{3} = 10$.

Thus the number of maximal independent sets is at most $5 + \binom{5}{3} = 15$, furthermore Theorem 2.1 implies $m^*(K_{15}) \ge 6$, so with applying Theorem 2.2 on the Peterson graph we have $m^*(P) \ge 6$. ■

3. Conclusion

In this paper, the method of maximal independent sets

of a graph was applied to find a lower bound on the pixel expansion of the basis matrices C_5 and Peterson graph.

References

[1] Naor, M., Shamir, A., "*Visual Cryptography, in: Advances in Cryptology – Eurocrypt'94"*, Lecture Notes in Computer Science, 950, Springer, Berlin, 1995, PP. 197–202.

[2] Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R., "*Visual Cryptography for General Access Structures"*, Information and Computation, 129 1996, PP. 86–106.

[3] Blundo, C., D'Arco, P., De Santis, A., Stinson, D.R., "*Contrast Optimal threshold Visual Cryptography Schemes"*, SIAM Journal of Discrete Mathematics, 16, 2003, PP. 224–261.

[4] Blundo, C., De Santis, A., Stinson, D.R., *"On the Contrast in Visual Cryptography Schemes"*, Journal of Cryptology, 12, 1999, PP.261–289.

[5] Hofmeister, T., Krause, M., Simon, H.U., *"Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography*", Computing and combinatorics (Shanghai, 1997), Theoretical Computer Science, 240, 2000, PP. 471–485.

[6] Verheul, E.R., Van Tilborg, H.C.A., *"Constructions and Properties of k out of n Visual Secret Sharing Schemes*", Designs, Codes and Cryptography, 11, 1997, PP. 179-196.