Visual cryptography scheme for the mindom access structure of a graph

R. LAKSHMANAN, S. ARUMUGAM*

National Centre for Advanced Research in Discrete Mathematics (n-CARDMATH)

Kalasalingam University

Anand Nagar, Krishnankoil-626 126, India.

e-mail: *lakshmsc2004@yahoo.co.in, s.arumugam.klu@gmail.com*

and

ATULYA K. NAGAR

Department of Computer and Mathematical Sciences

Centre for Applicable Mathematics and Systems Science (CAMSS)

Liverpool Hope University

Hope Park, Liverpool, L16 9JD. UK.

e-mail: *nagara@hope.ac.uk*

Abstract

Let $G = (V, E)$ be a connected graph with domination number $\gamma \geq 2$. In this paper we discuss the construction of a visual cryptography scheme for the mindom access structure $\Gamma_D(G)$ with basis consisting of all γ-sets of G. We prove that the access structure $\Gamma_D(G)$ is a $(2, n)$-threshold access structure if and only if n is even and $G = K_n - M$, where M is a perfect matching in K_n. Further the (k, n)-VCS with $k < n$ can be realized as a $\Gamma_D(G)$-VCS if and only if $k = 2$ and n is even. We also construct $\Gamma_D(G)$-VCS for several classes of graphs such as complete bipartite graphs, cycle $C^{\emptyset}_n$ and $K_n - C_n$ and we have achieved substantial reduction in the pixel expansion, when compared to the VCS constructed by using other known methods.

Keywords: dominating set, domination number, visual cryptography scheme, mindom access structure, pixel expansion, relative contrast.

2010 Mathematics Subject Classification Number: 94A60.

*Also at School of Electrical Engineering and Computer Science, The University of Newcastle, NSW 2308, Australia; Department of Computer Science, Liverpool Hope University, Liverpool, UK; Department of Computer Science, Ball State University, USA.

1 Introduction

A visual cryptography scheme (VCS) for a set P of n participants is a method to encode a secret image, which consists of a collection of black and white pixels, into n shadow images called *shares*, where each participant in P receives one share. Certain qualified subsets of P can visually recover the secret image by xeroxing their shares onto transparencies and stacking them, but any forbidden set of participants have no information about the secret image.

This cryptographic paradigm was introduced by Naor and Shamir [9]. They analysed the case of (k, n)-threshold visual cryptography scheme ((k, n)-VCS), where $2 \leq k \leq n$, for black and white images. In a (k, n)-VCS a subset S of P is a qualified set if and only if $|S| \geq k$. Another construction principle for a (k, n)-VCS is given in Droste [5].

Naor and Shamir's (k, n)-VCS has been extended to general access structures by Ateniese et al. [1, 2]. Let $P = \{1, 2, \ldots, n\}$ be a set of participants. Let 2^P denote the set of all subsets of P. Let $Q \subseteq 2^P$ and $F \subseteq 2^P$ where $Q \cap F = \emptyset$. Then the pair $\Gamma = (Q, F)$ is called an *access structure* on P. The elements of Q are called *qualified sets* and the elements of F are called *forbidden sets*. If further Q is monotone increasing and F is monotone decreasing and $Q \cup F = 2^P$, then Γ is said to be a *strong access structure*. Let $\Gamma_0 = \{A \in Q : A' \notin Q \text{ for all } A' \subsetneq A\}$ be the set of all minimal qualified subsets of P. The set Γ_0 is called the *basis* for the strong access structure and the strong access structure is completely determined by its basis.

Let S be an $n \times m$ boolean matrix and $X \subseteq P = \{1, 2, \ldots, n\}$ and $Z \subseteq M = \{1, 2, \ldots, m\}$. Then $S[X][Z]$ denotes the $|X| \times |Z|$ matrix obtained from S by considering its restriction to rows corresponding to the elements in X and columns corresponding to the elements in Z. Also $S[X]$ denotes the $|X| \times m$ matrix obtained from S by considering only the rows corresponding to the elements in X. For $X \subseteq P$, the vector obtained by applying the boolean OR operation to the rows of S corresponding to the elements in X is denoted by S_X. Also the Hamming weight of the row vector S_X, which is the number of ones in the vector S_X, is denoted by $w(S_X)$. If A and B are $n \times m_1$ and $n \times m_2$ matrices, then the $n \times (m_1 + m_2)$ matrix obtained by concatenating the columns of A and B is denoted by $[A \circ B]$. If A and B are $n_1 \times m$ and $n_2 \times m$ matrices, then the $(n_1 + n_2) \times (m)$ matrix obtained by concatenating the rows of A and B is denoted by $\begin{bmatrix} A \\ B \end{bmatrix}$. A VCS can be defined in terms of two $n \times m$ boolean matrices S^0 and S^1, called basis matrices.

Definition 1.1. [1] Let $\Gamma = (Q, F)$ be an access structure on a set P of n participants. A (Γ, m)-VCS is realized using two $n \times m$ boolean matrices

S^0 and S^1 called *basis matrices*, if there exist a positive real number α and a set of thresholds $\{t_X | X \in Q\}$ satisfying the following two conditions.

1. Any qualified set $X = \{i_1, i_2 \ldots, i_q\} \in Q$ can recover the image by stacking their transparencies. Formally $w(S^0_X) \leq t_X - \alpha m$, whereas $w(S^1_X) \geq t_X$.

2. Any forbidden set $X = \{i_1, \ldots, i_q\} \in F$ has no information on the shared image. Formally, the two $q \times m$ matrices $S^0[X]$ and $S^1[X]$ are equal up to a column permutation.

A VCS with basis matrices S^0 and S^1 is used to encrypt an image as follows. Let π be a random permutation of $\{1, 2, \ldots, m\}$. If a pixel in the secret image is white (resp. black), then π is applied to the columns of S^0 (resp.S^1) and row i of the permuted matrix forms the share for the i^{th} participant. In this way every pixel of the image is encrypted and distributed into n shares. The first property is related to the contrast of the image and the second property is called security. The number α is called the *relative contrast*, and m is the *pixel expansion*. The pixel expansion is the number of subpixels used to encode one pixel of the secret image in a share and the relative contrast measures the difference in grey level between a black pixel and a white pixel in the reconstructed image, which gives a measure of the clarity with which the image becomes visible. The basic problem is to maximize the relative contrast and minimize the pixel expansion. The relative contrast and the pixel expansion cannot be optimized simultaneously. Thus, in general, optimality with respect to relative contrast and optimality with respect to pixel expansion cannot be achieved by the same scheme.

We need the following theorems.

Theorem 1.2. [9] *There exists a (k, k)-VCS with $m = 2^{k-1}$ and $\alpha = 1/2^{k-1}$. The basis matrices S^0 and S^1 for this VCS have the following properties*

(i) $w(S^1_X) - w(S^0_X) = 1$ if $X = \{1, 2, \ldots k\}$,

(ii) The matrices $S^0[X]$ and $S^1[X]$ are equal up to column permutation for any proper subset $X \subset \{1, 2, \ldots k\}$.

Further for any (k, k)-VCS, $m \geq 2^{k-1}$ and $\alpha \leq \frac{1}{2^{k-1}}$.

The following two theorems give the existence of a VCS for any strong access structure.

Theorem 1.3. [1] *Let $\Gamma = (Q, F)$ be a strong access structure and let Z_M be the family of all maximal forbidden sets in F. Then there exists a VCS for Γ with $m = 2^{|Z_M|-1}$, $\alpha = 1/m$ and $t_X = m$ for any $X \in Q$.*

Theorem 1.4. [3] *Let $\Gamma = (Q, F)$ be a strong access structure on a set P of n participants with basis $\Gamma_0 = \{B_1, B_2, \ldots, B_k\}$. Let σ be a permutation on $\{1, 2, \ldots, k\}$. Then there exists a strong VCS with pixel expansion M_σ and $t_X = M_\sigma$ for any $X \in Q$, where M_σ is defined as follows:*

$$M_\sigma = \begin{cases} \sum_{i=1}^{l} 2^{|B_{\sigma(2i-1)} \cup B_{\sigma(2i)}|-2} & \text{if } k = 2l, l \geq 1 \\ \sum_{i=1}^{l} 2^{|B_{\sigma(2i-1)} \cup B_{\sigma(2i)}|-2} + 2^{|B_{\sigma(2l+1)}|-1} & \text{if } k = 2l+1, l \geq 0. \end{cases}$$

The method used in Theorem 1.3 for constructing the VCS is called cumulative array method. The formula for the pixel expansion M_σ given in Theorem 1.4 depends on the choice of the permutation σ.

Ateniese et al. [1] investigated access structures based on graphs. Given a graph $G = (V, E)$ with $|V| = n$, they considered the strong access structure whose basis consists of the edge set E. Thus a subset X of V is qualified if the induced subgraph $G[X]$ contains at least one edge of G. A few basic results for the VCS of this access structure are given in [1]. Dehkordi and Cheragi [6] obtained further results on the VCS of the above strong access structure for several classes of graphs. In this paper we consider the access structure arising from the dominating sets of a graph $G = (V, E)$ and discuss the problem of constructing a VCS for such access structures. For basic terminology in graphs we refer to Chartrand and Lesniak. [4].

Definition 1.5. Let $G = (V, E)$ be a graph. A subset S of V is called a *dominating set* of G if every vertex in $V - S$ is adjacent to a vertex in S. The minimum cardinality of a dominating set of G is called the *domination number* of G and is denoted by $\gamma(G)$ or simply γ. Any dominating set S of G with $|S| = \gamma$ is called a *γ-set* of G.

For an excellent treatment of the fundamentals of domination, we refer to the book by Haynes et al. [8].

Definition 1.6. Let $G = (V, E)$ be a graph. Let $S \subseteq V$ and $u \in S$. We say that a vertex $v \in V$ is a *private neighbor* of u with respect to S if $N[v] \cap S = \{u\}$ where $N[v]$ is the closed neighborhood of v, which consists of v and all vertices adjacent to v.

Theorem 1.7. [7] *A dominating set S of a graph G is a minimal dominating set if and only if every vertex $u \in S$ has at least one private neighbor.*

We observe that if S is a minimal dominating set and if u is an isolated vertex in the induced subgraph $G[S]$, then u is its own private neighbor. If u is not an isolated vertex in $G[S]$, then u has a private neighbor $v \in V - S$.

Definition 1.8. For any graph $G = (V, E)$, the graph H obtained from G by adding a new vertex w_i for each $v_i \in V$ and joining w_i and v_i is called the *corona* of G and is denoted by $G \circ K_1$.

2 Main Results

Let $G = (V, E)$ be a graph with $\gamma(G) \geq 2$. Let $Q = \{X \subseteq V : X$ contains a γ-set of $G\}$ and let $F = 2^V - Q$. Clearly $\Gamma = (Q, F)$ is a strong access structure on V and the basis for Γ is given by $\Gamma_0 = \{X \subseteq V : X$ is a γ-set of $G\}$. The set of all maximal forbidden sets for this access structure is given by $Z_M = \{S \subseteq V : S$ does not contain a γ-set and $S \cup \{v\}$ contains a γ-set for all $v \in V - S\}$. This access structure $\Gamma = (Q, F)$ is called the *mindom-access structure* of the graph G and is denoted by $\Gamma_D(G)$. We proceed to construct a VCS for this access structure for several families of graphs. We start with an example.

Example 2.1. Consider the graph $G = (V, E)$ given in Figure 1, which is the cycle on 5 vertices. Clearly $\gamma(G) = 2$ and the γ- sets of G are $\{1, 3\}$, $\{1, 4\}$, $\{2, 4\}$, $\{2, 5\}$, $\{3, 5\}$. The set of maximal forbidden sets for this access structure is given by $Z_M = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{5, 1\}\}$.Hence by Theorem 1.3 the VCS constructed by using the cumulative array method for this access structure has $m = 2^{|Z_M|-1} = 16$ and $\alpha = \frac{1}{16}$. However, the following matrices S^0 and S^1 are basis matrices for a VCS for this access structure with $m = 6$ and $\alpha = \frac{1}{6}$, thus giving a substantial reduction in the pixel expansion.

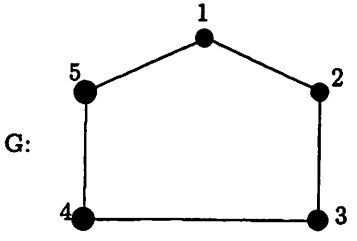


Fig.1

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

Clearly $S^0[X]$ and $S^1[X]$ are equal up to column permutation for all $X \in F$. Also $w(S^1_X) = 6$ and $w(S^0_X) = 5$ for all $X \in Q$. Hence $\alpha = \frac{1}{6}$ and $m = 6$. Any pixel of an original image is encoded on each of the five shares as six subpixels. Figure 2 shows the representation of a black pixel and a white pixel of the original image in each of the five shares.

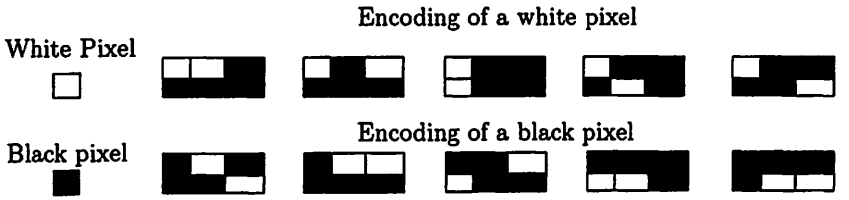
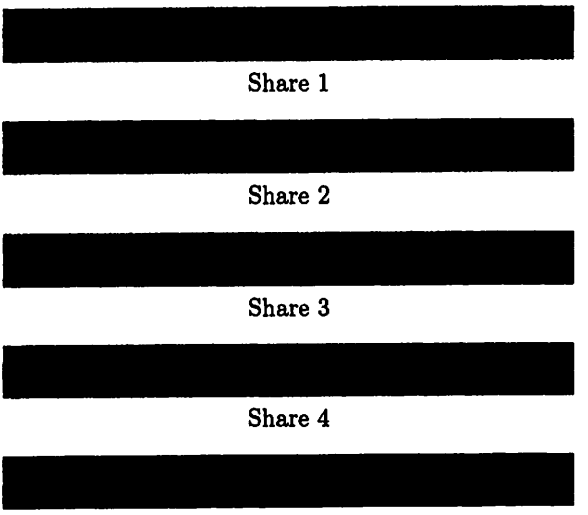


Fig.2

For the secret image given in Figure 3, the five shares are given in Figure 4. The reconstructed image by the superimposition of shares $\{1,3\}$, $\{2,4\}$, $\{3,5\}$, $\{1,2\}$ and $\{1,5\}$ are given in Figure 5.

DOMINATION

Figure 3



Share 1

Share 2

Share 3

Share 4

Share 5

Figure 4

Superimposition of shares 1 and 3

Superimposition of shares 2 and 4

Superimposition of shares 3 and 5

Superimposition of shares 1 and 2

Superimposition of shares 1 and 5
Figure 5

We observe that this VCS is different from the usual $(2,5)$-VCS, since a subset X with $|X| = 2$ cannot recover the image if X is not a dominating set of G. Thus the participants 1 and 2 cannot recover the secret image by superimposing their shares.

Example 2.2. Consider the graph $G = C_7 = (1,2,3,4,5,6,7,1)$, the cycle on 7 vertices. Then $\gamma(G) = 3$. Also the set of all γ-sets of G is given by $\Gamma_0 = \{\{1,2,5\}, \{1,3,5\}, \{1,3,6\}, \{1,4,5\}, \{1,4,6\}, \{1,4,7\}, \{2,3,6\}\ \{2,4,5\}, \{2,4,7\}, \{2,5,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,7\}, \{3,6,7\}\}$. The set of all maximal forbidden sets are given by $Z_M = \{\{1,2,3,4\}, \{2,3,4,5\}, \{3,4,5,6\}, \{4,5,6,7\}, \{5,6,7,1\}, \{6,7,1,2\}, \{7,1,2,3\}\}$. The basis matrices S^0 and S^1 for a $\Gamma_D(G)$-VCS are given below.

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

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

For this VCS, we have $m = 8$ and $\alpha = \frac{1}{8}$.

We observe that for the VCS obtained by using the CA method, the pixel expansion $m = 2^{|Z_M|-1} = 64$. Further the cardinality of the union of any two sets in Γ_0 is at least 4. Hence the pixel expansion M_σ for the VCS obtained by using Theorem 1.4 is given by $M_\sigma = \sum_{i=1}^{7} 2^{|B_{\sigma(2i-1)} \cup B_{\sigma(2i)}|-2} \geq 28$. Thus we have a substantial improvement in the pixel expansion.

Example 2.3. Let $n \geq 4$ be an even integer and let $G = K_n - M$, where M is a perfect matching in K_n. Then $\gamma(G) = 2$ and any subset S of $V(G)$ with $|S| = 2$ is a minimum dominating set of G. Hence any $\Gamma_D(G)$-VCS is the same as $(2, n)$-VCS.

We observe that for any integer $k \geq 2$, the (k, k)-VCS is the $\Gamma_D(G)$-VCS where $G = \overline{K}_k$, the empty graph on k vertices. If $k < n$, then the (k, n)-VCS can be realized as a $\Gamma_D(G)$-VCS if and only if $k = 2$ and n is even, as shown in the following two Theorems.

Theorem 2.4. *Let $G = (V, E)$ be a graph of order n with $\gamma(G) = 2$. Then any subset S of V with $|S| = 2$ is a dominating set of G if and only if n is even and $G = K_n - M$ where M is a perfect matching in K_n.*

Proof. Since $\gamma(G) = 2$, we have $\Delta(G) \leq n - 2$. If $n = 2$, then $G = \overline{K}_2 = K_2 - M$. Suppose $n \geq 3$. Let $u \in V$ and select $v \in V$ such that v is nonadjacent with u. Let $x \in V - \{u, v\}$. Then $S = \{x, v\}$ is a dominating set of G and since u is nonadjacent to v, it follows that u is adjacent to x. Thus $deg\ u = n - 2$. Thus G is $(n-2)$-regular, so that n is even and $G = K_n - M$ where M is a perfect matching in K_n. The converse is obvious. □

Corollary 2.5. *The $(2, n)$-VCS where n is odd, cannot be realized as a $\Gamma_D(G)$-VCS of a graph G.*

Theorem 2.6. *There is no graph G of order n such that $\gamma(G) = k \geq 3$, $k < n$ and every subset S of V with $|S| = k$ is a dominating set of G.*

Proof. Let $G = (V, E)$ be a graph of order n with $\gamma(G) = k$, where $3 \leq k < n$. Suppose every subset S of V with $|S| = k$ is a dominating set of G. If G has an isolated vertex v, then any subset S of V with $|S| = k$ and $v \notin S$, is not a dominating set of G. Hence it follows that G has no isolated vertices. Choose a subset $S = \{v_1, v_2 \ldots, v_k\}$ such that the induced subgraph $G[S]$ has no isolated vertices and v_1, v_k are not adjacent in G. Since S is a minimum dominating set of G and $\langle S \rangle$ has no isolated vertices, it follows from Theorem 1.7 that every $v_i \in S$ has a private neighbor $w_i \in V - S$. Thus w_i is adjacent to v_i and is non-adjacent to every vertex in $S - \{v_i\}$. Now $S_1 = \{v_1, w_1, w_2, \ldots, w_{k-1}\}$ is not a dominating set of G, since v_k is not adjacent to any vertex in S_1, a contradiction. □

Corollary 2.7. *Any (k, n)-VCS with $k \geq 3$ cannot be realized as a $\Gamma_D(G)$-VCS of a graph G.*

Theorem 2.8. *Let G be a graph with vertex set $V = \{1, 2 \ldots, n\}$. Let $\gamma(G) \geq 2$ and let $X_1, X_2, \ldots, X_d \subseteq V$ be the set of all γ-sets of G. Then there exists a VCS for the access structure $\Gamma_D(G)$ with $m = d2^{\gamma-1}$ and $\alpha = \frac{1}{d2^{\gamma-1}}$.*

Proof. Let B^0 and B^1 be the basis matrices for a (γ, γ)-VCS. Then B^0 and B^1 are $\gamma \times 2^{\gamma-1}$ matrices. Let $X_i = \{i_1, i_2, \ldots, i_\gamma\}$. Let S_i^0(resp.S_i^1) be the $n \times 2^{\gamma-1}$ matrix whose i_j^{th} row is the j^{th} row of B^0(resp.B^1) and each of the remaining rows is a vector all of whose entries are zero. It follows from Theorem 1.2 that if $X \subseteq V$ and $X \supseteq X_i$, then $w(S_{i_X}^1) - w(S_{i_X}^0) = 1$ and for any subset X that does not contain X_i, the matrices $S_i^1[X]$ and $S_i^0[X]$ are equal up to a column permutation.

Now let $S^0 = [S_1^0 \circ S_2^0 \circ \cdots \circ S_d^0]$ and $S^1 = [S_1^1 \circ S_2^1 \circ \cdots \circ S_d^1]$. We claim that S^0 and S^1 are the basis matrices of a VCS for the access structure $\Gamma_D(G)$.

Let $X \subseteq V$ and $X \in F$. Then X does not contain any X_i, $i = 1, \ldots d$. Hence $S_i^0[X]$ and $S_i^1[X]$ are equal up to column permutation for each i and so $S^0[X]$ and $S^1[X]$ are also equal up to a column permutation. Now let $X \in Q$. Then X contains at least one X_i, and hence $w(S_X^1) - w(S_X^0) \geq w(S_{i_X}^1) - w(S_{i_X}^0) = 1$.

Hence S^0 and S^1 are the basis matrices of a VCS for the access structure $\Gamma_D(G)$ with pixel expansion $m = d2^{\gamma-1}$ and relative contrast $\alpha = \frac{1}{d2^{\gamma-1}}$. □

Corollary 2.9. *For the graph $G = C_{3n}$ there exists a $\Gamma_D(G)$-VCS with $m = 3 \cdot 2^{n-1}$ and $\alpha = \frac{1}{3 \cdot 2^{n-1}}$.*

Proof. Clearly $\gamma(C_{3n}) = n$ and the number of γ-sets in C_{3n} is 3. Hence by Theorem 2.8 there exists a (Γ, m)-VCS for the access structure with $m = 3 \cdot 2^{n-1}$ and $\alpha = \frac{1}{3 \cdot 2^{n-1}}$. □

Remark 2.10. Let X_1, X_2 and X_3 be the γ-sets of C_{3n}. Then any maximal forbidden set for the access structure $\Gamma_D(C_{3n})$ is of the form $(X_1 - \{y_1\}) \cup (X_2 - \{y_2\}) \cup (X_3 - \{y_3\})$, where $y_i \in X_i$. Thus the number of maximal forbidden sets is n^3 and hence the pixel expansions for the VCS constructed by using CA method is 2^{n^3-1}. Also since the sets X_1, X_2, X_3 are disjoint, the pixel expansion M_σ for the VCS obtained by using Theorem 1.4 is given by $M_\sigma = 2^{2n-2} + 2^{n-1} = (2^{n-1}+1)2^{n-1}$. Thus we have a substantial improvement in the pixel expansion.

Example 2.11. For the complete bipartite graph $G = K_{m,n}$, there exists a VCS for the $\Gamma_D(G)$ access structure with $m = 2$ and $\alpha = \frac{1}{2}$. Let X and Y be the bipartition of $K_{m,n}$. Since $\gamma(K_{m,n}) = 2$ and any subset of the form $\{x, y\}$ where $x \in X$ and $y \in Y$ is a γ-set of G, it follows that $S^0 = [\mathbf{1}_{m+n} \circ \mathbf{0}_{m+n}]$ and $S^1 = \begin{bmatrix} \mathbf{1}_m \circ \mathbf{0}_m \\ \mathbf{0}_n \circ \mathbf{1}_n \end{bmatrix}$, where $\mathbf{1}_n(\mathbf{0}_n)$ denotes the $n \times 1$ vector with all entries one (zero) form the basis matrices of a $\Gamma_D(G)$-VCS with $m = 2$ and $\alpha = \frac{1}{2}$.

Theorem 2.12. *For the graph $G = K_n - C_n$ there exists a $\Gamma_D(G)$-VCS with $m = n + 1$ and $\alpha = \frac{1}{n+1}$.*

Proof. Let $V(K_n) = \{1, 2, \ldots, n\}$. Let $G = K_n - E(C_n)$ where C_n is the cycle $(1, 2, \ldots, n, 1)$. Clearly $\gamma(G) = 2$. The collection of maximal forbidden sets Z_M and the basis Γ_0 for the $\Gamma_D(G)$-access structure are given by $Z_M = \{\{1,3\}, \{2,4\}, \ldots, \{n-2, n\}, \{n-1, 1\}, \{n, 2\}\}$ and $\Gamma_0 = E(K_n) - Z_M$. Let $B_1 = \{1,3\}, B_2 = \{2,4\} \ldots, B_{n-2} = \{n-2, n\}, B_{n-1} = \{n-1, 1\}$ and $B_n = \{n, 2\}$. Let $N = (n_{ij})$ be the $n \times n$ matrix defined by

$$n_{ij} = \begin{cases} 0 & \text{if } i \in B_j \\ 1 & \text{otherwise.} \end{cases}$$

Let $M = (m_{ij})$ be the $n \times n$ matrix defined by

$$m_{ij} = \begin{cases} 0 & \text{if } i = j \\ 1 & \text{if } i \neq j. \end{cases}$$

Let $S^0 = [\mathbf{0} \circ M]$ and $S^1 = [\mathbf{1} \circ N]$ where $\mathbf{1}$ and $\mathbf{0}$ are respectively $n \times 1$ matrices with all entries 1 and 0 respectively. Then S^0 and S^1 are $n \times (n+1)$ matrices and every row in S^0 and S^1 has exactly two zeros. We claim that S^0 and S^1 are the basis matrices of a $\Gamma_D(G)$-VCS. Let $X \in Q$. Then $|X| \geq 2$ and there exists a γ-set $Y \subseteq X$. Hence it follows that $S^1[Y]$ has no zero column, so that $w(S^1_X) = n + 1$. Further $w(S^0_X) = n$, and hence $w(S^1_X) - w(S^0_X) = 1$. Now let $X \in F$. If $|X| = 1$, then clearly $S^0[X]$ and $S^1[X]$ are equal up to column permutation. If $|X| = 2$, then $S^0[X]$ has only one zero column and it follows from the definition of N that $S^1[X]$

also has only one zero column. Hence $S^0[X]$ and $S^1[X]$ are equal up to column permutation. □

Remark 2.13. For the access structure $\Gamma_D(G)$ where $G = K_n - C_n$, we have $|Z_M| = n$ and hence the pixel expansion for the VCS constructed by using CA method is given by $m = 2^{n-1}$. Also $|\Gamma_0| = \frac{n(n-1)}{2} - n$ and the union of any two sets in Γ_0 has at least 3 elements. Hence if M_σ is the pixel expansion for the VCS constructed by using Theorem 1.4, then we have $M_\sigma \geq 2\left(\frac{|\Gamma_0|}{2}\right) = \frac{n(n-1)}{2} - n$. Clearly $M_\sigma > n+1$ for all $n \geq 6$ and thus for the VCS given in Theorem 2.12, we have substantial improvement in the pixel expansion.

Theorem 2.14. *Let G be any graph of order n and let $H = G \circ K_1$. Then there exists a $\Gamma_D(H)$-VCS, with optimal pixel expansion $m = 2^{n-1}$.*

Proof. Let $V(G) = \{v_1, v_2, \ldots, v_n\}$ and let $u_1, u_2, \ldots, u_n$ be the vertices adjacent to $v_1, v_2, \ldots, v_n$ respectively. Clearly $\gamma(H) = n$ and $\Gamma_0(H) = \{\{a_1^1, a_2^2, \ldots, a_n^n\} : a_i^i \in \{u_i, v_i\}\}$. Hence $|\Gamma_0| = 2^n$ and

$$Z_M = \{\{v_1, \ldots v_{i-1}, v_{i+1} \ldots v_n\} \cup \{u_1, \ldots u_{i-1}, u_{i+1} \ldots u_n\} : i = 1, 2, \ldots, n\}$$

is the set of maximal forbidden sets. By Theorem 1.3 there exists a VCS with pixel expansion $m = 2^{n-1}$ and contrast $\alpha = 1/2^{n-1}$. We now prove that this pixel expansion m and the relative contrast α are optimum. Let S^0 and S^1 be the basis matrices of a $\Gamma_D(H)$-VCS. Let $X = \{v_1, v_2, \ldots, v_n\}$. Then $X \in Q$. Let $\widehat{S^0} = S^0[X]$ and $\widehat{S^1} = S^1[X]$. Since $X \in Q$, $w(\widehat{S^1}_X) - w(\widehat{S^0}_X) \geq 1$. Let Y be a proper subset X. Then $|Y| < n$, and $Y \in F$. Hence $\widehat{S^0}[Y] = S^0[Y]$ and $\widehat{S^1}[Y] = S^1[Y]$ are equal up to column permutation. Thus $\widehat{S^0}$ and $\widehat{S^1}$ are the basis matrices of a (n, n)-VCS and hence by Theorem 1.2 the pixel expansion m of any $\Gamma_D(H)$-VCS is at least 2^{n-1}. and the relative contrast is at most $1/2^{n-1}$. Hence the above VCS is optimal. □

3 Conclusion

In this paper we have investigated the problem of constructing a VCS for the strong access structure $\Gamma_D(G)$ whose basis is the set of all minimum dominating sets of a given graph G with $\gamma(G) \geq 2$. This problem can be further studied for other families of graphs for which all the γ-sets are known. The problem of constructing a VCS for other access structures arising from a given graph is another direction for further research.

Acknowledgement

The authors are thankful to Liverpool Hope University for its support in the establishment of the Centre for Applicable Mathematics and Systems Science (CAMSS) funded by HIEF4 funding. The first two authors also thank the Department of Science and Technology, New Delhi for its support through the n-CARDMATH Project SR/S4/MS:427/07. We are also thankful to the referee for helpful suggestions.

References

[1] G. Ateniese, C. Blundo, A.D. Santis and D.R. Stinson, Visual Cryptography for General Access Structures, *Inform. and Comput.*, **129**(1996), 86–106.

[2] G. Ateniese, C. Blundo, A.D. Santis and D.R. Stinson, Construction and Bounds for Visual Cryptography, Proc. ICALP 96, *Lecture Notes in Comput. Sci.*, Springer, Berlin, **1099** (1996), 416–428.

[3] Avishek Adhikari, Tridib Kumar Dutta and Bimal Roy, A New Black and White Visual Cryptographic Scheme for General Access Structures, INDOCRYPT, *Lecture Notes in Comput. Sci.*, Springer, Berlin, **3348** (2004), 399–413.

[4] G. Chartrand and L. Lesniak, *Graphs & Digraphs*, Chapman and Hall, CRC, 4^{th} edition, 2005.

[5] S .Droste, *New Results on Visual Cryptography*, CRYPTO 96, Proc. of the 16th Annual International Cryptology Conference, Santa Barbara, CA, August 18-22, 1996, 401–415.

[6] M.H. Dehkordi and A. Cheeragi, Maximal independent sets for the pixel expansion of graph access structures, *IUST International Journal of Science and Engineering*, **19**(1-2) (2008), 13-16.

[7] E.J. Cockayne, S.T. Hedetniemi and D.J. Miller, Properties of hereditary hypergraphs and middle graphs, *Canad. Math. Bull.*, **21** (1978), 461–468.

[8] T.W. Haynes, S.T. Hedetniemi and P.J. Slater, *Fundamentals of Domination in Graphs*, Marcel Dekker Inc., 1998.

[9] M. Naor and A. Shamir, Visual Cryptography, In *Advances in Cryptography-EUROCRYPT' 94*, A. De Santis, Ed., *Lecture Notes in Comput. Sci.* Springer-Verlag, Berlin, **950** (1995), 1–12.