FACTA UNIVERSITATIS (NIŠ)
Ser. Math. Inform. Vol. 38, No 5 (2023), 905 - 917
https://doi.org/10.22190/FUMI230904058C
Original Scientific Paper

VISUAL CRYPTOGRAPHY SCHEME ON GRAPH ACCESS STRUCTURES WITH OPTIMAL PIXEL EXPANSION FOUR

Abbas Cheraghi[1] and Mahmood Davarzani[2]

[1]**Department of Mathematics, Khansar Campus, University of Isfahan, Iran**
[2]**Faculty of Mathematics and Computer Science, Kharazmi University, Iran**

Abstract. The strong access structure obtained from graph G is $\Gamma(G)$ if $G = (V, E)$ is a connected graph. A visual cryptography scheme (VCS) is a specific technique for encoding a secret image that typically changes any pixel in the image to m subpixels for a group of active participants. Within each VCS, only qualified sets can retrieve the secret picture by stacking their preferred shares. The pixel expansion value is traditionally called m, and the minimum pixel expansion value of a VCS for $\Gamma(G)$ is referred to as $m^*(G)$. The principal aim of this paper is to identify all connected graphs G with $m^*(G) = 4$ and $\omega(G) = 6$, which realistically is the clique number of graph G.
Keywords: Visual cryptography scheme, Graph access structure, Access structure.

1. Introduction

A secret sharing scheme represents an efficient method for sharing a sensitive secret among a specific group of people to ensure that only qualified people can accurately reconstruct the valuable secret from their outstanding shares. Moreover, proper subsets that are unqualified cannot extract some information regarding the secret. Naor and Shamir [8] introduced the Visual Cryptography Scheme (VCS) as an effective method of sharing well-kept secrets. They are investigating the case of $((k, n) - VCS)$ where $2 \leq k \leq n$, in which the secret image is visible if and only if k or more participants stack their shares. In addition, any independent set of less than k participants have no access to information on the secret image. In

Received September 04, 2023. accepted September 19, 2023.
Communicated by Mojtaba Bahramian, Amirhossein Nokhodkar, Predrag Stanimirović
Corresponding Author: Abbas Cheraghi, Department of Mathematics, Khansar Campus, University of Isfahan, Iran | E-mail: a.cheraghi@khc.ui.ac.ir
2010 *Mathematics Subject Classification.* Primary 94A62 ; Secondary 05C90

a VCS, a decoder is a human visual system, and a group of qualified people can see th image without knowing cryptography. Ateniese et al. [3, 4] extended this scheme to general access structures. P is the term used to describe the set of all participants in this standard model. The access structure for $\Gamma = (Q, F)$ is that $Q \subseteq 2^P$ represents the collection of qualified sets and $F \subseteq 2^P$ involves the collection of forbidden set. It is our assumption that the secret picture is a collection of pixels in black and white. In a VCS, any pixel of this image is replaced by m subpixels and given to each share. The amount of m is known as the pixel expansion. The optimal pixel expansion is the minimum value of m for a given general access structure Γ, indicated by $m^*(\Gamma)$. Let the vertex set V in a graph $G = (V, E)$ be the set of participants and any element of Γ be the subset of V which contains at least one edge. $\Gamma(G)$ is used to denote this access structure and $m^*(G)$ is used to denote the optimal expansion. Atenies et al. in [3, 4] studied the construction of VCSs that obtained from graphs and have proven that $m^*(\Gamma)$ =2 if and only if $\Gamma = \Gamma(G)$ where G is a complete bipartite graph.They have also proved that $m^*(K_n)$ is the smallest m which $n \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$. So $m^*(K_2) = 2$ and $m^*(K_3) = 3$. In addition they proved that $m^*(H) \leq m^*(G)$ where H is induced subgraph G. Since $m^*(K_6) = 4$ and $m^*(K_7) = 5$, if $m^*(G) = 4$ and H be the induced subgraph G then the biggest induced complete subgraph G is K_6.

The characterization of all connected graphs G for which $m^*(G) = 2$ and 3 was obtained by Arumugam et al. in [1, 2]. In this paper, we study the graphs with $m^*(G) = 4$. We describe the characterization of every connected graph G that has $m^*(G) = 4$ and $\omega(G) = 6$, which is the clique number of graph G.

2. Preliminaries

Suppose that $P = \{1, 2, \cdots, n\}$ is a collection of participants and 2^P is the collection of all subsets of P. If $Q \subseteq 2^P$ and $F \subseteq 2^P$ so that $Q \cap F = \emptyset$, then the pair $\Gamma = (Q, F)$ is referred to as an access structure over P. We refer to items valued at Q as qualified items and items valued at F as prohibited items. When Q is monotonously increasing and F is monotonously decreasing, we call Γ a strong access structure, and $Q \cup F = 2^P$. The focus of this paper is on strong access structures only. Define Γ_0 to consist of all the minimal qualify sets : $\Gamma_0 = \{A \in Q : A' \notin Q \text{ for all } A' \subsetneq A\}$.

Let S be a boolean matrix with a value of $n \times m$. If $X \subseteq P = \{1, 2, \cdots, n\}$, then $S[X]$ denotes the $|X| \times m$ matrix obtained from S by considering its restriction to rows corresponding to the elements of X. Furthermore, S_X is the vector obtained using the boolean OR operation on the rows of $S[X]$, and $w(S_X)$ is the hamming weight of S_X.

Definition 2.1. [3]. Let $\Gamma = (Q, F)$ be a strong access structure on a set of n participants. Two $n \times m$ boolean matrices S^0 and S^1 construct a VCS if there exist a positive real number α and the set $\{t_X | X \in Q\}$ satisfying the following conditions:

1. The shared image can be recovered by stacking the transparency of any qualified set $X = \{i_1, i_2, \dots, i_q\} \in Q$. Formally $w(S^0_X) \leq t_X - \alpha \cdot m$, whereas $w(S^1_X) \geq t_X$.
2. The forbidden set $X = \{i_1, i_2, \dots, i_q\} \in F$ does not contain any information about the shared image. Formally the two $q \times m$ matrices $S^0[X]$ and $S^1[X]$ are equal up to a column permutation.

Image contrast is traditionally associated with the first property, while safety is linked to the second property. It is common for us to believe that the message consists of a collection of black and white pixels. Let π be a random permutation of $\{1, 2, \dots, m\}$. The following is the process of using a VCS to encrypt an image. In the case that 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 make up the share of ith participant. Therefore, each share is a collection of m black and white subpixels. The pixel expansion value is called m, and the relative contrast value is called α, which measures the clarity of a reconstructed image. One problem with a VCS is minimising pixel expansion and maximizing relative contrast. Several results on these two concepts can be found in [9, 10]. $m^*(\Gamma)$ is used to denote the minimum value of the pixel expansion m of a VCS for $\Gamma = (Q, F)$.

Definition 2.2. Let $\Gamma = (Q, F)$ be an access structure on a set P of participants. Then $\Gamma' = (Q', F')$ is the induced access structure on $P' \subseteq P$ by $Q' = Q \cap 2^{P'}$ and $F' = F \cap 2^{P'}$.

Let $G = (V, E)$ be a graph, then we can define a VCS on G such that a subset X of V is qualified if and only if the induced subgraph $G[X]$ contains at least one edge of G. The access structure based on graph G is denoted by $\Gamma(G)$ and $m^*(G)$ is the minimum value of pixel expansion m a VCS that $\Gamma(G)$ is the access structures.

Theorem 2.1. *[3]. Let $\Gamma = (Q, F)$ be an access structure on a set P of participants and let $\Gamma' = (Q[P'], F[P']))$ be the induced access structure on the subset of participants P'. Then $m^*(\Gamma') \leq m(\Gamma)$.*

Remark 2.1. If $H = (V', E')$ be an induced subgraph of $G = (V, E)$, then $\Gamma(H)$ is an induced access structure of $\Gamma(G)$ and by Theorem 2.1, $m^*(H) \leq m^*(G)$.

Ateniese et al. [3, 4] studied the construction of VCSs on general access structures and graph access structures. They showed in [3] that how can obtain basis matrices S^0 and S^1 of a VCS on a complete graph.

Theorem 2.2. *[3]. Let $\Gamma = (Q, F)$ be an access structure on a set P of participants. Let $X, Y \subseteq P$ be two nonempty subsets of participants such that $X \cap Y = \emptyset$, $X \in F$ and $X \cup Y \in Q$. Then in any $(\Gamma, m) - VCS$ for this access structure, we have $w(S^1_{X \cup Y}) - w(S^1_X) \geq \alpha \cdot m$ where S^0 and S^1 are basis matrices, m is the pixel expansion and α is the relative contrast.*

Remark 2.2. [2]. In particular, if $Y = \{y\}$, then $S^1[X \cup \{y\}]$ has at least one column with 1 in the row corresponding to y and with zero in all other entries. An *unavoidable pattern* refers to a column in $S^1[X \cup \{y\}]$.

For complete graph K_n and complete bipartite graph, we have the following theorems.

Theorem 2.3. *[3]. Let $G = K_n$ be complete graph. Then the value $m^*(K_n)$ is the smallest integer m such that $n \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$.*

Theorem 2.4. *[3]. Create a strong access structure called Γ for a set of participants P. $m^*(\Gamma) = 2$, If and only if $\Gamma = \Gamma(G)$ where G is a complete bipartite graph with $V(G) = P$.*

A *clique*, C, is a subset of the vertices in a graph $G = (V, E)$ where every two distinct vertices are adjacent. This is equivalent to the requirement for the $G[C]$ sub-graph to be complete. A clique with the most vertices in a graph G is called a maximum clique. In the graph G, the *clique number* $\omega(G)$ is the number of vertices in a maximum clique in G. An *independent set*, I, in a graph is a subset of vertices such that no two vertices in I are adjacent. A *maximal independent set* is an independent set containing the largest possible number of vertices in graph. The following theorem gives a relation between $m^*(G)$ and number of maximal independent sets in G that proved by Dehkordi and Cheraghi in [6].

Theorem 2.5. *[6]. Let G be a graph with the number of maximal independent sets l, then $m^*(G) \geq t$ where t is the smallest integer such that $l \leq \binom{t}{\lfloor \frac{t}{2} \rfloor}$.*

3. Main results

Let $G = (V, E)$ be a connected graph with $m^*(G) = 4$. Then by Remark 2.1 for any induced subgraph H of G having no isolated vertices, we have $m^*(H) \leq 4$. we have from Theorem 2.5 that the number of maximal independent sets in H is at most 6. Further by Theorem 2.3, we have $\omega(G) \leq 6$. If $\omega(G) = 6$ then K_6 is induced subgraph of graph G. We first obtain the basis matrices of S^0 and S^1 a VCS that $\Gamma = \Gamma(K_6)$ is access structure.

Proposition 3.1. *Let $G = K_6$ be a complete graph and $V = \{v_1, v_2, \ldots, v_6\}$ is vertices set. Then basis matrices a VCS for $\Gamma(G)$ are*

$$S^1[V] \sim \begin{bmatrix} 1&1&0&0 \\ 1&0&1&0 \\ 1&0&0&1 \\ 0&1&1&0 \\ 0&1&0&1 \\ 0&0&1&1 \end{bmatrix}, \; S^0[V] \sim \begin{bmatrix} 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \end{bmatrix}.$$

Proof. By Theorem 2.3, $m^*(K_6) = 4$. From Theorem 6.6 and Corollary 6.7 in [3], a $(\Gamma(K_6), 4)$-VCS implies the existence of a Sperner family of size 6 over a ground set of size 4. Let ground set is $P = \{a_1, a_2, a_3, a_4\}$, since only Sperner family of size 6 over P is $B_1 = \{a_1, a_2\}$, $B_2 = \{a_1, a_3\}$, $B_3 = \{a_1, a_4\}$, $B_4 = \{a_2, a_3\}$, $B_5 = \{a_2, a_4\}$, $B_6 = \{a_3, a_4\}$, from Theorem 7.2 in [3], we obtain basis matrices for a VCS with strong access structure $\Gamma(K_6)$ from following definitions:

$$S^1(i,j) = \left\{ \begin{array}{ll} 1 & a_j \in B_i \\ 0 & a_j \notin B_i \end{array} \right., S^0(i,j) = \left\{ \begin{array}{ll} 1 & 1 \leq j \leq |B_i| \\ 0 & |B_i| + 1 \leq j \leq 4 \end{array} \right. .$$

Hence $S^1[V] \sim \begin{bmatrix} 1&1&0&0\\1&0&1&0\\1&0&0&1\\0&1&1&0\\0&1&0&1\\0&0&1&1 \end{bmatrix}$ and $S^0[V] \sim \begin{bmatrix} 1&1&0&0\\1&1&0&0\\1&1&0&0\\1&1&0&0\\1&1&0&0\\1&1&0&0 \end{bmatrix}$. □

Lemma 3.1. *Let G be a connected graph with $m^*(G) = 4$. If $\omega(G) = 6$ where $\omega(G)$ is the clique number of graph G, then G is $(K_6 \cup K_1)$-free.*

Proof. Assume that G is not $(K_6 \cup K_1)$-free, thus G contains $K_6 \cup K_1$ as an induced subgraph. So if $Z = V(K_6) = \{v_1, v_2, \ldots, v_6\}$ and $V(K_1) = \{x\}$, then the vertex x is not connected to any of the vertices of the Z. Given that $G[Z] = K_6$ and by using Proposition 3.1, we have $S^1[Z] \sim \begin{bmatrix} 1&1&0&0\\1&0&1&0\\1&0&0&1\\0&1&1&0\\0&1&0&1\\0&0&1&1 \end{bmatrix}$. Without loss of generality assume that the rows of $S^1[Z]$ corresponds to $v_1, v_2, \ldots, v_6$ respectively. Using Remark 2.2 with $X = \{x, v_4\}$ and $Y = \{v_1\}$, which $X \in F$ and $X \cup Y \in Q$, then $S^1[X \cup Y]$ has at least one column with 1 in the row corresponding to v_1 and with zero in all other entries. Therefore, the row corresponding to x in $S^1[Z \cup \{x\}]$ must be $[0 \quad ? \quad ? \quad ?]$ where ? represents the presence of either 0 or 1. So the first entry is zero and the following table shows that other entries of the row corresponding to x are also zero.

X	Y	row of x in $S^1[Z \cup \{x\}]$
x, v_4	v_1	$[0 \quad ? \quad ? \quad ?]$
x, v_2	v_1	$[0 \quad 0 \quad ? \quad ?]$
x, v_3	v_2	$[0 \quad 0 \quad 0 \quad ?]$
x, v_4	v_5	$[0 \quad 0 \quad 0 \quad 0]$

Thus $S^1[Z \bigcup \{x\}] \sim \begin{bmatrix} 1&1&0&0\\1&0&1&0\\1&0&0&1\\0&1&1&0\\0&1&0&1\\0&0&1&1\\0&0&0&0 \end{bmatrix}$. This gives a contradiction since no row of S^1 can have weight zero. Hence G is $(K_6 \cup K_1)$-free. □

Because of the G is $(K_6 \cup K_1)$-free, then for any vertex of $x \in G$, we have $N(x) \cap Z \neq \emptyset$, where $Z = \{v_1, v_2, \ldots, v_6\}$ is a clique of G and $N(x)$ is the open neighborhood of x consisting of all vertices which are adjacent to x. Since $\omega(G) = 6$, we have $1 \leq |\, N(x) \cap Z| \leq 5$. Now for $1 \leq i < j < k < r < s \leq 6$, we define:

$$\begin{aligned}
V_i &:= \bigl\{x \in V - Z \bigm| N(x) \cap Z = \{v_i\}\bigr\},\\
V_{ij} &:= \bigl\{x \in V - Z \bigm| N(x) \cap Z = \{v_i, v_j\}\bigr\},\\
V_{ijk} &:= \bigl\{x \in V - Z \bigm| N(x) \cap Z = \{v_i, v_j, v_k\}\bigr\},\\
V_{ijkr} &:= \bigl\{x \in V - Z \bigm| N(x) \cap Z = \{v_i, v_j, v_k, v_r\}\bigr\},\\
V_{ijkrs} &:= \bigl\{x \in V - Z \bigm| N(x) \cap Z = \{v_i, v_j, v_k, v_r, v_s\}\bigr\}.
\end{aligned}$$

We now proceed to characterize connected graphs G such that $m^*(G) = 4$ and $\omega(G) = 6$.

Lemma 3.2. *Let G be a connected graph with $m^*(G) = 4$ and $\omega(G) = 6$. Then with above definitions,we have*

1. *$V_i = \emptyset$, for all $1 \le i \le 6$,*
2. *$V_{ij} = \emptyset$, for all $1 \le i < j \le 6$,*
3. *$V_{ijk} = \emptyset$, for all $1 \le i < j < k \le 6$ possibly expected of $V_{124}, V_{135}, V_{236}$ and V_{456},*
4. *$V_{ijkr} = \emptyset$, for all $1 \le i < j < k < r \le 6$,*
5. *The V_{ijkrs} can be nonempty for all $1 \le i < j < k < r < s \le 6$.*

Proof. Let $G[Z] = K_6$ and $Z = \{v_1, v_2, \ldots, v_6\}$. By Lemma 3.1, we have $S^1[Z] \sim \begin{bmatrix} 1&1&0&0\\ 1&0&1&0\\ 1&0&0&1\\ 0&1&1&0\\ 0&1&0&1\\ 0&0&1&1 \end{bmatrix}$. Without loss of generality assume that the rows of $S^1[Z]$ corresponds to $v_1, v_2, \ldots, v_6$ respectively.

proof of (1): Suppose $V_1 \neq \emptyset$ and let $x \in V_1$. Using Remark 2.2, we have the following table:

X	Y	row of x in $S^1[Z \cup \{x\}]$
x, v_4	v_1	$[0 \quad ? \quad ? \quad ?]$
x, v_2	v_1	$[0 \quad 0 \quad ? \quad ?]$
x, v_3	v_2	$[0 \quad 0 \quad 0 \quad ?]$
x, v_4	v_5	$[0 \quad 0 \quad 0 \quad 0]$

Therefore row of x in $S^1[Z \cup \{x\}]$ is $[0 \quad 0 \quad 0 \quad 0]$. This gives a contradiction, hence $V_1 = \emptyset$. A similar proof show that other V_i's are empty.

proof of (2): For V_{ij}'s, we have two non-isomorphic form V_{12} and V_{34}, Because columns v_1 and v_2 in $S^1[Z]$ are $\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right], \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]$ and columns of v_3 and v_4 are $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right], \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$. If V_{12} and V_{34} be nonempty, let $x \in V_{12}$ and $y \in V_{34}$. Using Remark 2.2, we have the following tables:

X	Y	row of x in $S^1[Z \cup \{x\}]$
x, v_4	v_1	$[0 \quad ? \quad ? \quad ?]$
x, v_3	v_1	$[0 \quad 0 \quad ? \quad ?]$
x, v_3	v_2	$[0 \quad 0 \quad 0 \quad ?]$
x, v_4	v_5	$[0 \quad 0 \quad 0 \quad 0]$

X	Y	row of y in $S^1[Z \cup \{y\}]$
y, v_5	v_1	$[0 \quad ? \quad ? \quad ?]$
y, v_6	v_4	$[0 \quad 0 \quad ? \quad ?]$
y, v_5	v_4	$[0 \quad 0 \quad 0 \quad ?]$
y, v_2	v_6	$[0 \quad 0 \quad 0 \quad 0]$

Therefore rows of x and y in $S^1[Z \bigcup \{x, y\}]$ are $[0 \quad 0 \quad 0 \quad 0]$. This gives a contradiction, hence V_{12} and V_{34} are empty.

proof of (3): If $V_{456} \neq \emptyset$, let $x \in V_{456}$. Using Remark 2.2, row of x in $S^1[Z \cup \{x\}]$ obtain from the following table:

X	Y	row of x in $S^1[Z \cup \{x\}]$
x, v_2	v_1	$[? \quad 0 \quad ? \quad ?]$
x, v_3	v_2	$[? \quad 0 \quad 0 \quad ?]$
x, v_2	v_3	$[? \quad 0 \quad 0 \quad 0]$
v_4	x	$[1 \quad 0 \quad 0 \quad 0]$

Hence row of x in $S^1[Z \cup \{x\}]$ has entry of nonzero in first place to linked that v_4, v_5 and v_6 are zero only in first column of $S^1[Z]$.
If $x \in V_{456}$, we have $xv_1 \in F$, so columns of x and v_1 in $S^1[Z \cup \{x\}]$ and $S^0[Z \cup \{x\}]$ are same, thus row of x in $S^0[Z \cup \{x\}]$ is $[? \quad ? \quad 0 \quad 0]$ and since $w(S^0_{\{x\}}) = 1$, row of x in $S^0[Z \cup \{x\}]$ is $[0 \quad 1 \quad 0 \quad 0]$ or $[1 \quad 0 \quad 0 \quad 0]$. Similarly if $y \in V_{236}, z \in V_{135}$ and $w \in V_{124}$, then rows of y, z and w in $S^1[Z \cup \{y\}], S^1[Z \cup \{z\}]$ and $S^1[Z \cup \{w\}]$ are $[0 \quad 1 \quad 0 \quad 0], [0 \quad 0 \quad 1 \quad 0]$ and $[0 \quad 0 \quad 0 \quad 1]$.
we have $\binom{6}{3} = 20$ type of V_{ijk}, where $1 \leq i, j, k \leq 6$ and i, j, k are different. It is simple work to show all of V_{ijk}'s are empty expected of $V_{124}, V_{135}, V_{236}$ and V_{456}. For example, if $V_{123} \neq \emptyset$, Let $x \in V_{123}$. Using Remark 2.2 and following table, row of x in $S^1[Z \cup \{x\}]$ is $[0 \quad 0 \quad 0 \quad 0]$.

X	Y	row of x in $S^1[Z \cup \{x\}]$
x, v_4	v_1	$[0 \quad ? \quad ? \quad ?]$
x, v_6	v_4	$[0 \quad 0 \quad ? \quad ?]$
x, v_5	v_2	$[0 \quad 0 \quad 0 \quad ?]$
x, v_4	v_5	$[0 \quad 0 \quad 0 \quad 0]$

Hence $V_{123} = \emptyset$.

proof of (4): By the (3), graph G can contains $V_{456}, V_{236}, V_{135}$ and V_{124}. From each one, we can make three V_{ijkr}, where $1 \leq i < j < k < r \leq 6$ and i, j, k, r are different as follows:

V_{ijk}	V_{124}	V_{135}	V_{236}	V_{456}
V_{ijkr}	V_{1234}	V_{1235}	V_{1236}	V_{1456}
	V_{1245}	V_{1345}	V_{2346}	V_{2456}
	V_{1246}	V_{1356}	V_{2356}	V_{3456}

These V_{ijkr}'s are different. Let V_{1456} that obtained from V_{456} is not empty and let $x \in V_{1456}$. To considering table of provided in (3), row of x in $S^1[Z \cup \{x\}]$

is $[1\quad 0\quad 0\quad 0]$. Using Remark 2.2 with $X = \{v_1\}$ and $Y = \{x\}$, we have that $S^1[\{x, v_1\}]$ has the unavoidable pattern $[\begin{smallmatrix}1\\0\end{smallmatrix}]$, while this pattern dont exist. Hence $V_{1456} = \emptyset$. Similarly all of V_{ijkr}'s above table are empty. Now it is sufficient that show V_{1256}, V_{2345} and V_{1346} are empty. Let $x \in V_{1256}, y \in V_{2345}$ and $z \in V_{1346}$. Using Lemma 2.2, we have the following tables:

X	Y	row of x in $S^1[Z \cup \{x\}]$
x, v_4	v_1	$[0\quad ?\quad ?\quad ?]$
x, v_3	v_1	$[0\quad 0\quad ?\quad ?]$
x, v_3	v_2	$[0\quad 0\quad 0\quad ?]$
x, v_4	v_5	$[0\quad 0\quad 0\quad 0]$

X	Y	row of y in $S^1[Z \cup \{y\}]$
y, v_6	v_2	$[0\quad ?\quad ?\quad ?]$
y, v_6	v_5	$[0\quad 0\quad ?\quad ?]$
y, v_1	v_2	$[0\quad 0\quad 0\quad ?]$
y, v_1	v_3	$[0\quad 0\quad 0\quad 0]$

X	Y	row of z in $S^1[Z \cup \{z\}]$
z, v_5	v_1	$[0\quad ?\quad ?\quad ?]$
z, v_2	v_4	$[0\quad 0\quad ?\quad ?]$
z, v_5	v_4	$[0\quad 0\quad 0\quad ?]$
z, v_2	v_3	$[0\quad 0\quad 0\quad 0]$

Hence V_{1256}, V_{2345} and V_{1346} are empty.

proof of (5): Let $x \in V_{12345}$, then $xv_6 \in F$. Now by Lemma 2.2, row of x in $S^1[Z \cup \{x\}]$ obtain from the following table.

X	Y	row of x in $S^1[Z \cup \{x\}]$
x, v_6	v_1	$[0\quad ?\quad ?\quad ?]$
x, v_6	v_4	$[0\quad 0\quad ?\quad ?]$
v_2	x	$[0\quad 0\quad ?\quad 1]$
v_3	x	$[0\quad 0\quad 1\quad 1]$

Note that $\{x, v_6\} \in F$ and row of x is the same to row of v_6 in $S^1[Z \cup \{x\}]$. Similarly, graph G can be contain other V_{ijkrs}'s. □

Lemma 3.3. *Let G be a connected graph with $m^*(G) = 4$ and $\omega(G) = 6$. If V_{mnp}'s and V_{ijkrs}'s be not empty, then they are independent.*

Proof. Let $G[Z] = K_6$ and $Z = \{v_1, v_2, \ldots, v_6\}$. Let $x, y \in V_{124}$. If $\{x, y\} \in Q$, then we have 9 maximal independent sets as follows:

$$\{x, v_3\}, \{x, v_5\}, \{x, v_6\}, \{y, v_3\}, \{y, v_5\},$$

$$\{y, v_6\}, \{v_1\}, \{v_2\}, \{v_4\},$$

and by Thorem 2.5, this gives a contradiction, since G has at most 6 maximal independent sets. Similarly, The sets of V_{456}, V_{135} and V_{236} are independent. Now, Let $x, y \in V_{12345}$. If $\{x, y\} \in Q$, Then we have 7 maximal independent sets as follows:

$$\{x, v_6\}, \{y, v_6\}, \{v_1\}, \{v_2\}, \{v_3\}, \{v_4\}, \{v_5\},$$

by Theorem 2.5, this gives a contradiction, hence V_{12345} is a independent set. Similarly, each other V_{ijkrs}'s are independent sets. □

Lemma 3.4. *Let G be a connected graph with $m^*(G) = 4$ and $\omega(G) = 6$. If V_{ijk}'s and V_{ijkrs}'s be not empty , then*

1. *The sets of V_{ijk} are mutually independent from each other,*
2. *The sets of V_{ijkrs} are mutually complete bipartite graphs.*

proof of (1): Let $G[Z] = K_6$ and $Z = \{v_1, v_2, \ldots, v_6\}$. By Lemma 3.2, we know that the sets of $V_{456}, V_{236}, V_{135}$ and V_{124} may be not empty. Let $x \in V_{124}$ and $y \in V_{135}$. If $\{x, y\} \in Q$, we have 7 maximal independent sets as follows:

$$\{x, v_3\}, \{x, v_5\}, \{x, v_6\}, \{y, v_2\}, \{y, v_4\}, \{y, v_6\}, \{v_1\},$$

by Theorem 2.5, this gives a contradiction, hence $\{x, y\} \in F$. Similarly the sets of $V_{456} \cup V_{236}$, $V_{456} \cup V_{135}$, $V_{456} \cup V_{124}$, $V_{236} \cup V_{135}$ and $V_{236} \cup V_{124}$ are independent sets.
proof of (2): Let $x \in V_{12345}$ and $y \in V_{23456}$, By Lemma 3.2, we have

$$S^1[Z \cup \{x, y\}] \sim \begin{bmatrix} 1&1&0&0 \\ 1&0&1&0 \\ 1&0&0&1 \\ 0&1&1&0 \\ 0&1&0&1 \\ 0&0&1&1 \\ 0&0&1&1 \\ 1&1&0&0 \end{bmatrix}.$$

Since $\{x, v_6\}$, $\{y, v_1\}$ are forbidden sets and $w(S^1_{\{x\}}) = w(S^1_{\{y\}}) = 2$, we have $S^0[Z \cup \{x, y\}] \sim \begin{bmatrix} 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \end{bmatrix}$. Hence $w(S^1_{\{x,y\}}) = 4$ and $w(S^0_{\{x,y\}}) = 2$. Thus $\{x, y\}$ is qualified set and x , y are adjacent. Similarly the sets of $V_{ijkrs} \cup V_{i'j'k'r's'}$ are complete bipartite graphs.

Remark 3.3. If $V_{mnp}, V_{ijkrs} \neq \emptyset$,

for $1 \leq m < n < p < i < j < k < r < s \leq 6$ and $t := | \{i, j, k, r, s\} \cap \{m, n, p\}|$, then $t = 2$ or $t = 3$.

Lemma 3.5. *Let G be a connected graph with $m^*(G) = 4$ and $\omega(G) = 6$. If $V_{mnp}, V_{ijkrs} \neq \emptyset$*

where $1 \leq m < n < p < i < j < k < r < s \leq 6$, then

$$G\big[V_{mnp} \cup V_{ijkrs}\big] = \begin{cases} K_{3,5} & ; \quad t = 2 \\ \\ \overline{K_8} & ; \quad t = 3 \end{cases}$$

Proof. Let $t = 2$. If $x \in V_{124}$ and $y \in V_{13456}$, then by Lemma 3.2, we have

$$S^1[Z \cup \{x, y\}] \sim \begin{bmatrix} 1&1&0&0 \\ 1&0&1&0 \\ 1&0&0&1 \\ 0&1&1&0 \\ 0&1&0&1 \\ 0&0&1&1 \\ 0&0&0&1 \\ 1&0&1&0 \end{bmatrix},$$

$$S^0[Z \cup \{x, y\}] \sim \begin{bmatrix} 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 0&1&0&0 \\ 1&1&0&0 \end{bmatrix} \text{ or } \begin{bmatrix} 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&0&0&0 \\ 1&1&0&0 \end{bmatrix}.$$

Hence $w(S^1_{\{x,y\}}) = 3$ and $w(S^0_{\{x,y\}}) = 2$. Thus $\{x, y\}$ is a qualified set and x and y are adjacent.

Let $t = 3$. If $x \in V_{124}, y \in V_{12345}$ and $\{x, y\} \in Q$, then we have 7 maximal independent sets as follows:

$$\{x, v_3\}, \{x, v_5\}, \{x, v_6\}, \{y, v_6\}, \{v_1\}, \{v_2\}, \{v_4\},$$

by Theorem 2.5, this gives a contradiction, hence $\{x, y\} \in F$. □

Lemma 3.6. *Let G be contain two sets from four sets $V_{124}, V_{135}, V_{236}$ and V_{456}. Then other sets are empty.*

Proof. Let $x \in V_{124}$ and $y \in V_{135}$. If $V_{236} \neq \emptyset$, Let $z \in V_{236}$. By Lemma 3.2, we have

$$S^1[Z \cup \{x, y, z\}] \sim \begin{bmatrix} 1&1&0&0 \\ 1&0&1&0 \\ 1&0&0&1 \\ 0&1&1&0 \\ 0&1&0&1 \\ 0&0&1&1 \\ 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \end{bmatrix},$$

$$S^0[Z \cup \{x, y, z\}] \sim \begin{bmatrix} 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ ?&?&0&0 \\ ?&?&0&0 \\ ?&?&0&0 \end{bmatrix},$$

which $w(S^0_{\{x\}}) = w(S^0_{\{y\}}) = w(S^0_{\{z\}}) = 1$. Thus $w(S^1_{\{x,y,z\}}) = 3$ and $w(S^0_{\{x,y,z\}}) = 2$, hence $\{x, y, z\}$ is a qualified set. However $\{x, y\}$, $\{x, z\}$ and $\{y, z\}$ are forbidden, hence we have a contradiction. Thus $V_{236} = \emptyset$. Similarly $V_{456} = \emptyset$. □

We are now performing the characterization of the G connected graphs so that $m^*(G) = 4$ and $\omega(G) = 6$. Let $\mathcal{F}$ be the family of graphs that obtained from complete graph K_6 with $V(K_6) = \{v_1, v_2, \dots, v_6\}$ by adding four independent sets $V_{124}, V_{456}, V_{135}, V_{236}$ and six independent sets V_{ijkrs}, which $1 \leq i < j < k < r < s \leq 6$ and i, j, k, r, s are different and these sets satisfy in Lemma 3.3 to Lemma 3.8. A few graphs in the family $\mathcal{F}$ are given in Figure 3.1.

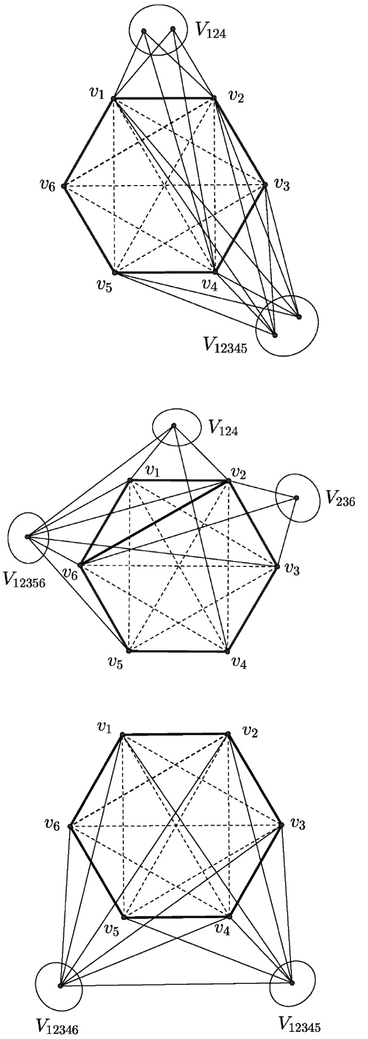

FIG. 3.1: Graphs in family $\mathcal{F}$

Theorem 3.1. *Let G be a connected graph with $\omega(G) = 6$. Then $m^*(G) = 4$ if and only if G is isomorphic to a graph H in $\mathcal{F}$.*

Proof. Let $m^*(G) = 4$. By Lemma 3.2 to Lemma 3.6, G is isomorphic to a graph in

$\mathcal{F}$. For prove the converse, let $H \in \mathcal{F}$ and V_{ijkrs}'s are nonempty, which $1 \le i < j < k < r < s \le 6$ and i, j, k, r, s are different. By Lemma 3.6, we assume V_{124} and V_{456} are nonempty. If $|V_{124}| = n_1$, $|V_{456}| = n_2$, $|V_{12345}| = m_1$, $|V_{23456}| = m_2$, $|V_{13456}| = m_3$, $|V_{12456}| = m_4$, $|V_{12356}| = m_5$ and $|V_{12346}| = m_6$, then the basis matrices for VCS of the access structure $\Gamma(H)$ are:

$$S^1 \sim \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0_{n_1} & 0_{n_1} & 0_{n_1} & 1_{n_1} \\ 1_{n_2} & 0_{n_2} & 0_{n_2} & 0_{n_2} \\ 0_{m_1} & 0_{m_1} & 1_{m_1} & 1_{m_1} \\ 1_{m_2} & 1_{m_2} & 0_{m_2} & 0_{m_2} \\ 1_{m_3} & 0_{m_3} & 1_{m_3} & 0_{m_3} \\ 1_{m_4} & 0_{m_4} & 0_{m_4} & 1_{m_4} \\ 0_{m_5} & 1_{m_5} & 1_{m_5} & 0_{m_5} \\ 0_{m_6} & 1_{m_6} & 0_{m_6} & 1_{m_6} \end{bmatrix}$$

and

$$S^0 \sim \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1_{n_1} & 0_{n_1} & 0_{n_1} & 0_{n_1} \\ 1_{n_2} & 0_{n_2} & 0_{n_2} & 0_{n_2} \\ 1_{m_1} & 1_{m_1} & 0_{m_1} & 0_{m_1} \\ 1_{m_2} & 1_{m_2} & 0_{m_2} & 0_{m_2} \\ 1_{m_3} & 1_{m_3} & 0_{m_3} & 0_{m_3} \\ 1_{m_4} & 1_{m_4} & 0_{m_4} & 0_{m_4} \\ 1_{m_5} & 1_{m_5} & 0_{m_5} & 0_{m_5} \\ 1_{m_6} & 1_{m_6} & 0_{m_6} & 0_{m_6} \end{bmatrix}$$

where 1_n (0_n) denotes the $n \times 1$ column matrix with all entries one (zero). It is simple work that S^0 and S^1 are basis matrices for a VCS of the access structure $\Gamma(H)$. Hence $m^*(H) \le 4$. However H contains K_6, thus $m^*(H) = 4$. Now if $G \in \mathcal{F}$, then G is an induced subgraph of H and since G contains K_6 as a subgraph, we have $m^*(G) = 4$. □

4. Conclusion

Ateniese et al. [3] have proved that $m^*(\Gamma) = 2$ if and only if $\Gamma = \Gamma(G)$ where G is a complete bipartite graph. Also Arumugam et al. [2] have obtained a characterization of all connected graphs G where $m^*(G) = 3$. If $m^*(G) = 4$, then $\omega(G) \leq 6$. In this paper, we obtained a characterization of all connected graphs G for which $\omega(G) = 6$. The next challenge is to categorize all graphs where $m^*(G) = 4$ and $\omega(G) \leq 5$.

REFERENCES

1. S. Arumugam, R. Lakshmanan, Atulya K. Nagar, Visual cryptography scheme for graphs with vertex covering number two *Nat. Acad. Sci. Lett.*, **36 (6)** 575-579 (2013).
2. S. Arumugam, R. Lakshmanan, Atulya K. Nagar, Graph access structure with optimal pixel expansion three, *Inform. and Comput.*, **230** 67-75 (2013).
3. G. Ateniese, C. Blundo, A.D. Santis, D.R. Stinson, Visual cryptography for general access structures, *Inform. and Comput*, **129** 86-106 (1996).
4. G. Ateniese, C. Blundo, A.D. Santis, D.R. Stinson, *Construction and bounds for visual cryptography*, in: Proc. ICALP 96, Springer, Berlin, 1996, pp. 416-428.
5. G. Chartrand, L. Lesniak, *Graphs and Digraphs*, fourth ed., Chapman and Hall, CRC, 2005.
6. M.H. Dehkordi, A. Cheraghi, Maximal independent sets for the pixel expansion of graph access structures, *IUST Int. J. Sci. Eng.*, **19 (1–2)** 13-16 (2008).
7. H. Hajiabolhassan, A. Cheraghi, Bounds for visual cryptography schemes, *Discret Appl. Math.*, **158(6)** 659-665 (2010).
8. M. Naor, A. Shamir, Visual cryptography, in: A. De Santis (Ed.), Advances in Cryptography, EUROCRYPT '94, in: Lecture Notes in Comput. Sci., *Springer-Verlag*, **950** 1-12 (1995).
9. 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** 179-196 (1997).
10. T. Hofmeister, M. Krause , H.U. Simon, Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography, *Computing and combinatorics*, **240** 471-485 (2000).