www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 8 No. 2 (2019), pp. 53-66.

www.ui.ac.ir

VISUAL CRYPTOGRAPHY SCHEME ON GRAPHS WITH $m^*(G) = 4$

MAHMOOD DAVARZANI

Communicated by Hamidreza Maimani

ABSTRACT. Let $G = (V, E)$ be a connected graph and $\Gamma(G)$ be the strong access structure where obtained from graph G. A visual cryptography scheme (VCS) for a set P of participants is a method to encode a secret image such that any pixel of this image change to m subpixels and only qualified sets can recover the secret image by stacking their shares. The value of m is called the pixel expansion and the minimum value of the pixel expansion of a VCS for $\Gamma(G)$ is denoted by $m^*(G)$. In this paper we obtain a characterization of all connected graphs G with $m^*(G) = 4$ and $\omega(G) = 5$ which $\omega(G)$ is the clique number of graph G.

1. Introduction

A secret sharing scheme is a method to share a secret among a set of participants such that only qualified subsets can reconstruct the secret from their shares, in addition non-qualified subsets can not obtain any information about the secret.

Visual cruptography scheme, (VCS), is a kind of secret sharing scheme, was introduced by Naor and Shamir [9]. They investigate 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, whereas any set of less than k participants have no information on the secret image. In a VCS, decoder is human visual system and participants in a qualified set can see secret image without knowledge of cryptographic. Ateniese et al. [3, 4] extended this scheme to general access structures. In this model, P is set of participants and $\Gamma = (Q, F)$ is access structure such that $Q \subseteq 2^P$ is the collection of qualified sets and $F \subseteq 2^P$ is the

MSC(2010): Primary: 94A60; Secondary: 14G50, 94A15.
Keywords: Secret sharing schemes, Visual cryptography scheme, Graph access structure, Pixel expansion.
Received: 28 October 2018, Accepted: 04 February 2019.

DOI: http://dx.doi.org/10.22108/toc.2019.113671.1599

.

collection of forbidden sets. We assume that image secret is collection of black and white pixels. Now in a VCS any pixel of this image is replaced by m subpixels and give to each shares. The number of m is called the pixel expansion and for a given general access structure Γ, the minimum value of m is denoted by $m^*(\Gamma)$, and is called the optimal pixel exapansion.

If 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, then this access structure is denoted by $\Gamma(G)$ and the optimal expansion is denoted by $m^*(G)$. Atenies et al. in [3, 4] studied the construction of VCSs that obtained from graphs and proved 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 $m^*(K_7) = 5$ thus if $m^*(G) = 4$ and H be the induced subgraph G then the biggest induced complete subgraph G is K_6.

Arumugam et al. in [1, 2] obtained a characterization of all connected graphs G for which $m^*(G) = 2$ and 3. In this paper, we study the graphs with $m^*(G) = 4$. We give a characterization of all connected graphs G which $m^*(G) = 4$ and $\omega(G) = 5$ that $\omega(G)$ is the clique number of graph G.

2. **Preliminaries**

Let $P = \{1, 2, \ldots, n\}$ be a set of participants and let 2^P denote the set of of all subsets of P. If $Q \subseteq 2^P$ and $F \subseteq 2^P$ such that $Q \cap F = \emptyset$, then the pair $\Gamma = (Q, F)$ is called an access structure on P. We refer elements of Q as qualified sets and to elements of F as forbidden sets. We say Γ is strong access structure whenever Q is monotone increasing and F is monotone decreasing and $Q \cup F = 2^P$. Throughout this paper we consider only strong access structures. 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 an $n \times m$ boolean matrix. If $X \subseteq P = \{1, 2, \ldots, n\}$ then $S[X]$ denotes the $|X| \times m$ matrix obtained from S by considering its restriction to rows corrresponding to the elements in X, further S_X denotes the vector obtained by applying the boolean OR operation to the rows of $S[X]$ and $w(S_X)$ is Hamming weight of S_X.

Definition 2.1. [3] *Let $\Gamma = (Q, F)$ be a strong access 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 follwing conditions:*

(1) *Any qualified set $X = \{i_1, i_2, \ldots, i_q\} \in Q$ can recover the shared 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 $X = \{i_1, i_2, \ldots, i_q\} \in F$ 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.*

The first property is attributed to the contrast of the image and the second property is related to security. We assume that the message consist of a collection of black and white pixels. Let π be a random permutation of $\{1, 2, \ldots, m\}$. Now a VCS is used to encrypt an image as follows. 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 is the share of ith participant. Therefore each share is a collection of m black and white subpixels. The value of m is called the *pixel expansion* and the value of α is called *relative contrast* that measure clarity of reconstructed image.

One problem in a VCS is to minimize the pixel expansion and maximize the relative contrast. Several results on these two concepts can be found in [10, 11]. The minimum value of the pixel expansion m of a VCS for $\Gamma = (Q, F)$ is denoted by $m^*(\Gamma)$.

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 $P' \subseteq P$ that $Q' = Q \cap 2^{P'}$ 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 2.3. [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 2.4. *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 Theoram 2.3, $m^*(H) \leq m^*(G)$.*

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 2.5. [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 $w(S^1_{X\cup Y}) - w(S^1_X) \geq \alpha.m$ where S^0 and S^1 are basis matrices, m is the pixel expansion and α is the relative contrast.*

Remark 2.6. [2] *By Theorem 2.5, 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. such a column in $S^1[X \cup \{y\}]$ is called an unavoidable pattern.*

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

Theorem 2.7. [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 2.8. [3] *Let Γ be a strong access structure on a set of participants P. Then $m^*(\Gamma) = 2$ if and only if $\Gamma = \Gamma(G)$ where G is a complete bipartite graph with $V(G) = P$.*

An *clique*, C, in a graph $G = (V, E)$ is a subset of the vertices such that every two distinct vertices are adjacent. This is equivalent to the condition that the induced subgraph $G[C]$ is complete. A maximum clique of a graph G is a clique such that there is no clique with more vertices. The *clique* *number* $\omega(G)$ of a graph 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 [7].

Theorem 2.9. [7] *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 2.4 for any induced subgraph H of G having no isolated vertices, we have $m^*(H) \leq 4$. We have from Theorem 2.9 that the number of maximal independent sets in H is at most 6. Further by Theorem 2.7, we have $\omega(G) \leq 6$. In [6] we charecterized all of graphs which $m^*(G) = 4$ and $\omega(G) = 6$. In this paper, we consider case of $\omega(G) = 5$. If $\omega(G) = 5$, then K_5 is induced subgraph of graph G. We first prove the following lemma.

Proposition 3.1. *Let $G = K_5$ be a complete graph and $V = \{v_1, v_2, \ldots, v_5\}$ is vertices set. Then one of the pairs of base matrices a VCS for $\Gamma(G)$ is*

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

Proof. By Theorem 2.7, $m^*(K_5) = 4$. From Theorem 6.6 and corollary 6.7 in [3], a $(\Gamma(K_5), 4)$-VCS implies the existence of a sperner family of size 5 over a ground set of size 4. Let ground set is $P = \{a_1, a_2, a_3, a_4\}$, now only sperner family of size 5 over P is $B_1 = \{a_1, a_2\}$, $B_2 = \{a_2, a_3\}$, $B_3 = \{a_3, a_4\}$,$B_4 = \{a_1, a_4\}$, $B_5 = \{a_1, a_3\}$. From Theorem 7.2 in [3], we obtain basis matrices for a VCS with strong access structure $\Gamma(K_5)$ from following definitions.

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

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

Lemma 3.2. *Let G be a connected graph with $m^*(G) = 4$. If $\omega(G) = 5$ where $\omega(G)$ is the clique number of graph G, then G is $(K_5 \cup K_1)$-free.*

Proof. Assume that G is not $(K_5 \cup K_1)$-free, thus G contains $K_5 \cup K_1$ as an induced subgraph. So if $Z = V(K_5) = \{v_1, \ldots, v_5\}$ and $V(K_1) = \{x\}$, then the vertex x is not connected to any of the vertices of the Z. Given that $G[Z] = K_5$ and by using Proposition 3.1, we have $S^1[Z] \sim \begin{bmatrix} 1&1&0&0 \\ 0&1&1&0 \\ 0&0&1&1 \\ 1&0&0&1 \\ 1&0&1&0 \end{bmatrix}$. Without loss of generality assume that the rows of $S^1[Z]$ corresponds to $v_1, v_2, \ldots, v_5$ respectively. Using Remark 2.6 with $X = \{x, v_2\}$ 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_2	v_1	$[0 \quad ? \quad ? \quad ?]$
x, v_3	v_2	$[0 \quad 0 \quad ? \quad ?]$
x, v_4	v_3	$[0 \quad 0 \quad 0 \quad ?]$
x, v_5	v_4	$[0 \quad 0 \quad 0 \quad 0]$

Thus $S^1[Z \bigcup \{x\}] \sim \begin{bmatrix} 1&1&0&0 \\ 0&1&1&0 \\ 0&0&1&1 \\ 1&0&0&1 \\ 1&0&1&0 \\ 0&0&0&0 \end{bmatrix}$. This gives a contradiction since no row of S^1 can have weight zero. Hence G is $(K_5 \cup K_1)$-free. □

Since graph G is $(K_5 \cup K_1)$-free, then for any vertex of $x \in G$, we have $N(x) \cap Z \neq \emptyset$, where $N(x)$ is the open neighborhood of x consisting of all vertices which are adjacent to x. Also, since $\omega(G) = 5$, it follows that $1 \leq \left|N(x) \cap Z\right| \leq 4$. For any nonempty proper subset $X \subseteq \{1, 2, \ldots, 5\}$, we define the set V_X as follows:

$$V_X := \left\{x \in V \backslash Z, N(x) \cap Z = \{v_i : i \in X\}\right\}$$

We now determine the properties of above sets in following lemmas.

Lemma 3.3. *Let G be a connected graph with $m^*(G) = 4$ and $\omega(G) = 5$. Then with above definition, we have*

(i) *If $|X| = 1$, then $V_X = \emptyset$,*
(ii) *If $|X| = 2$, then $V_X = \emptyset$ except probably V_{14} and V_{23},*
(iii) *If $|X| = 3$, then $V_X = \emptyset$ except probably V_{125} and V_{345},*
(iv) *If $|X| = 4$, then V_X can be available.*

Proof. Let $G[Z] = K_5$ and $Z = \{v_1, v_2, \ldots, v_5\}$. By Lemma 3.1, $S^1[Z \bigcup \{x\}] \sim \begin{bmatrix} 1&1&0&0 \\ 0&1&1&0 \\ 0&0&1&1 \\ 1&0&0&1 \\ 1&0&1&0 \end{bmatrix}$. Without loss of generality we assume that rows of $S^1[Z]$ corresponds to $v_1, v_2, \ldots, v_5$ respectively.

(i). Suppose $V_1 \neq \emptyset$ and let $x \in V_1$. Using Remark 2.6, we have the following table:

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

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 shows that other V_i's are empty.

(ii). According to $S^1[Z]$, v_2 and v_3 are zero in first column and other entries in this column are nonzero, so $V_{23} \neq \emptyset$ and if $x \in V_{23}$ then we have

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

Similarly if $y \in V_{14}$ then we have

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

The other V_{ij}'s are empty. For example let $x \in V_{12}$, then by Remark 2.6, we have the following table:

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

Therefore row of x in $S^1[Z \cup \{x\}]$ is $[0 \quad 0 \quad 0 \quad 0]$. This gives a contradiction, hence $V_{12} = \emptyset$. A similar proof shows that other V_{ij}'s are empty.

(iii). In $S^1[Z]$, v_1, v_2 and v_5 are zero in last column and other entries in this column are nonzero, so $V_{125} \neq \emptyset$. If $x \in V_{125}$, then we have

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

Similarly if $y \in V_{345}$, then we have

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

By the (ii), graph G can contains V_{14} and V_{23}. From each one, we can make three V_{ijk}, where $1 \leq i, j, k \leq 5$ and i, j, k are different as follows:

V_{ij}	V_{23}	V_{14}
	V_{123}	V_{124}
V_{ijk}	V_{234}	V_{134}
	V_{235}	V_{145}

All of V_{ijk}'s in above table are $\emptyset$. Let V_{123} that is obtained from V_{23} is not empty and let $x \in V_{123}$. Then by (ii) row of x in $S^1[Z \cup \{x\}]$ is $[1 \quad 0 \quad 0 \quad 0]$. However $\{x, v_1\} \in F$, Thus in $S^1[Z \cup \{x\}]$ we must have the unavoidable patterns of $[\begin{smallmatrix}1\\0\end{smallmatrix}]$ and $[\begin{smallmatrix}0\\1\end{smallmatrix}]$ while the first pattern doesn't exist. Hence $V_{123} = \emptyset$. Similarly all of V_{ijk}'s in above table are empty. Now, it is sufficient that we show V_{135} and V_{245} are empty. Let V_{135} and V_{245} are not empty and $x \in V_{245}, y \in V_{135}$. Using Remark 2.6, we have the following tables:

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

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

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_{245} and V_{135} are empty.

(iv). Let $x \in V_{1234}$. By Remark 2.6, we have the following table:

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

.

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

Also, since $\{x, v_5\}$ is forbidden set and $w(S^1_{\{x\}}) = 2$, then $S^0[Z \cup \{x\}] \sim \begin{bmatrix} 1&1&0&0\\1&1&0&0\\1&1&0&0\\1&1&0&0\\1&1&0&0\\1&1&0&0 \end{bmatrix}$. Let $y \in V_{1235}$. By Remark 2.6, we have the following table:

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

.

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

Also, since $\{y, v_4\}$ is forbidden set and $w(S^1_{\{y\}}) = 2$, then $S^0[Z\cup\{y\}] \sim \begin{bmatrix} 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0 \end{bmatrix}$. Let $z \in V_{1245}$. By Remark 2.6, we have the following table:

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

.

Hence $S^1[Z\cup\{z\}] \sim \begin{bmatrix} 1&1&0&0\\ 0&1&1&0\\ 0&0&1&1\\ 1&0&0&1\\ 1&0&1&0\\ 0&0&1&1 \end{bmatrix}$.

Also, since $\{z, v_3\}$ is forbidden set and $w(S^1_{\{z\}}) = 2$, then $S^0[Z\cup\{z\}] \sim \begin{bmatrix} 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0 \end{bmatrix}$. Let $s \in V_{1345}$. By Remark 2.6, we have the following table:

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

.

Hence $S^1[Z\cup\{s\}] \sim \begin{bmatrix} 1&1&0&0\\ 0&1&1&0\\ 0&0&1&1\\ 1&0&0&1\\ 1&0&1&0\\ 0&1&1&0 \end{bmatrix}$.

Also, since $\{s, v_2\}$ is forbidden set and $w(S^1_{\{s\}}) = 2$, then $S^0[Z\cup\{s\}] \sim \begin{bmatrix} 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0 \end{bmatrix}$. Let $t \in V_{2345}$. By Remark 2.6, we have the following table:

http://dx.doi.org/10.22108/toc.2019.113671.1599

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

Hence $S^1[Z \cup \{t\}] \sim \begin{bmatrix} 1&1&0&0\\ 0&1&1&0\\ 0&0&1&1\\ 1&0&0&1\\ 1&0&1&0\\ 1&1&0&0 \end{bmatrix}$.

Also, since $\{t, v_1\}$ is forbidden set and $w(S^1_{\{t\}}) = 2$, then $S^0[Z \cup \{t\}] \sim \begin{bmatrix} 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0 \end{bmatrix}$. □

Lemma 3.4. *Let G be a connected graph with $m^*(G) = 4$ and $\omega(G) = 5$. Also, suppose that $Z = \{v_1, v_2, \ldots, v_5\}$ is a clique of G. Then V_X is an independent set for any $X \subseteq \{1, 2, \ldots, 5\}$ with $2 \le |X| \le 4$.*

Proof. Let $|X| = 2$. Then by Lemma 3.3, we consider the cases $X = \{1, 4\}$ and $X = \{2, 3\}$. Let $x, y \in V_{14}$. If $\{x, y\} \in Q$, then we have 8 maximal independent sets as follows: $\{x, v_2\}$, $\{x, v_3\}$, $\{x, v_5\}$, $\{y, v_2\}$, $\{y, v_3\}$, $\{y, v_5\}$, $\{v_1\}$,$\{v_4\}$. By Thorem 2.9, G has at most 6 maximal independent sets, thus this gives a contradiction. Hence V_{14} is a independent set. Similarly, the set of V_{23} is independent. Now let $x, y \in V_{125}$. If $\{x, y\} \in Q$, then we have 7 maximal independent sets as follows: $\{x, v_3\}$, $\{x, v_4\}$, $\{y, v_3\}$, $\{y, v_4\}$, $\{v_1\}$, $\{v_2\}$, $\{v_5\}$ and $\{v_5\}$. By Theorem 2.9, this gives a contradiction, hence V_{125} is a independent set. Similarly, the set of V_{345} is independent.
Now we show that $V_{1234} = \emptyset$. If $V_{1234} \neq \emptyset$, let $x, y \in V_{1234}$. Then by Lemma 3.3, we have

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

So $w(S^1_{\{x,y\}}) = w(S^0_{\{x,y\}}) = 2$, thus $\{x, y\} \in F$. Hence V_{1234} is a independent set and this complete proof. □

Lemma 3.5. *Let G be a connected graph with $m^*(G) = 4$ and $\omega(G) = 5$. Then $V_{14} \cup V_{23}$ is an independent set.*

Proof. From lemma 3.3, we have

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

http://dx.doi.org/10.22108/toc.2019.113671.1599

If $S^0[Z \cup \{x,y\}] \sim \begin{bmatrix} 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&0&0&0\\ 1&0&0&0 \end{bmatrix}$ then $w(S^1_{\{x,y\}}) > w(S^0_{\{x,y\}})$, thus $\{x,y\} \in Q$. However $w(S^1_{\{xyv_5\}}) = w(S^0_{\{xyv_5\}})$, which is contradiction since $\Gamma(G)$ is strong access structure. Hence $S^0[Z \cup \{x,y\}] \sim \begin{bmatrix} 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&0&0&0\\ 0&1&0&0 \end{bmatrix}$. In this case $w(S^1_{\{x,y\}}) = w(S^0_{\{x,y\}})$ and this show that $\{x,y\} \in F$. Hence x and y are nonadjacent. Thus $V_{14} \cup V_{23}$ is an independent set. □

Remark 3.6. *Suppose that $V_{125}, V_{345} \neq \emptyset$. Let $x \in V_{125}$, $y \in V_{345}$. From Lemma 3.3, we have*

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

In first form of $S^0[Z \cup \{x,y\}]$, we have $w(S^1_{\{x,y\}}) > w(S^0_{\{x,y\}})$, hence $\{x,y\}$ is qualified set and this show that x and y are adjacent. In second form of $S^0[Z \cup \{x,y\}]$, we have $w(S^1_{\{x,y\}}) = w(S^0_{\{x,y\}})$, hence $\{x,y\}$ is forbidden set, thus x and y are nonadjacent.

Lemma 3.7. *Let G be a connected graph with $m^*(G) = 4$ and $\omega(G) = 5$. Also, X, Y and W be nonempty proper subsets of $\{1,2,\ldots,5\}$. If $|X| = 2$, $|Y| = 3$ and $|W| = 4$, then with previous definitions,*

(i) *The sets of $V_X \cup V_Y$ are independent sets,*
(ii) *The sets of $V_X \cup V_W$ are independent sets,*
(iii) *The induced subgraphs $G[V_Y \cup V_W]$ are complete bipartite graphs.*

Proof. (i). Let $V_{14}, V_{125} \neq \emptyset$. If $x \in V_{14}$ and $y \in V_{125}$, then by Lemma 3.3, we have

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

Hence $w(S^1_{\{x,y\}}) > w(S^0_{\{x,y\}})$, thus $\{x,y\} \in Q$. However $w(S^1_{\{x,y\,v_3\}}) = w(S^0_{\{x,y,v_3\}})$, which is contradiction since $\Gamma(G)$ is strong access structure. So $\{x,y\} \in F$ and hence $V_{14} \cup V_{125}$ is independent set. A similar proof shows that $V_{14} \cup V_{345}, V_{23} \cup V_{125}$ and $V_{23} \cup V_{345}$ are independent sets.

(ii). Let $V_{14}, V_{1234} \neq \emptyset$. If $x \in V_{14}$ and $y \in V_{1234}$, then by Lemma 3.3, we have

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

Hence $w(S^1_{\{x,y\}}) = w(S^0_{\{x,y\}})$, thus $\{x,y\} \in F$. A similar proof shows that $V_X \cup V_W$ is an independent set.

(iii). Let $V_{125}, V_{1234} \neq \emptyset$. If $x \in V_{125}$ and $y \in V_{1234}$, then by Lemma 3.3, we have

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

Hence $w(S^1_{\{x,y\}}) > w(S^0_{\{x,y\}})$, thus $\{x,y\} \in Q$. A similar proof shows that the induced subgraph $G[V_Y \cup V_W]$ is a complete bipartite graph. □

Lemma 3.8. *Let G be a connected graph with $m^*(G) = 4$ and $\omega(G) = 5$. If V_{ij}'s are not empty, then V_{ijk}'s are empty.*

Proof. Let V_{ij}'s are not empty and $x \in V_{23}$ and $y \in V_{14}$. If $V_{125} \neq \emptyset$, then by Lemma 3.3 we have

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

Hence $w(S^1_{\{x,y,z\}}) > w(S^0_{\{x,y,z\}})$, therefore $\{x,y\} \in Q$ and this is contradiction with Lemma 3.5. □

We now proceed to characterize connected graphs G such that $m^*(G) = 4$ and $\omega(G) = 5$. Let $\mathcal{F}$ be the family of graphs that obtained from complete graph K_5 with $V(K_5) = \{v_1, v_2, \ldots, v_5\}$ by adding nine independent sets V_{14}, $V_{23}, V_{125}, V_{345}, V_{1234}, V_{1235}, V_{1245}, V_{1345}$ and V_{2345} where $|V_{14}| = n_1$, $|V_{23}| = n_2$, $|V_{125}| = n_3$, $|V_{345}| = n_4$, $|V_{1234}| = n_5$, $|V_{1235}| = n_6$, $|V_{1245}| = n_7$, $|V_{1345}| = n_8$, $|V_{2345}| = n_9$ and these sets satisfy in Lemma 3.4 to Lemma 3.8. According to the definition of V_{1234}, if $x \in V_{1234}$, then $\{x, v_5\}$ is independent, so we can replace set of v_5 with a set of independent vertices, with the name V'_5, instead of set V_{1234}. Similarly, the vertices v_1, v_2, v_3 and v_4 can replace by independent sets V'_1, V'_2, V'_3 and V'_4. A few graphs in the family $\mathcal{F}$ are given in Figure 1.

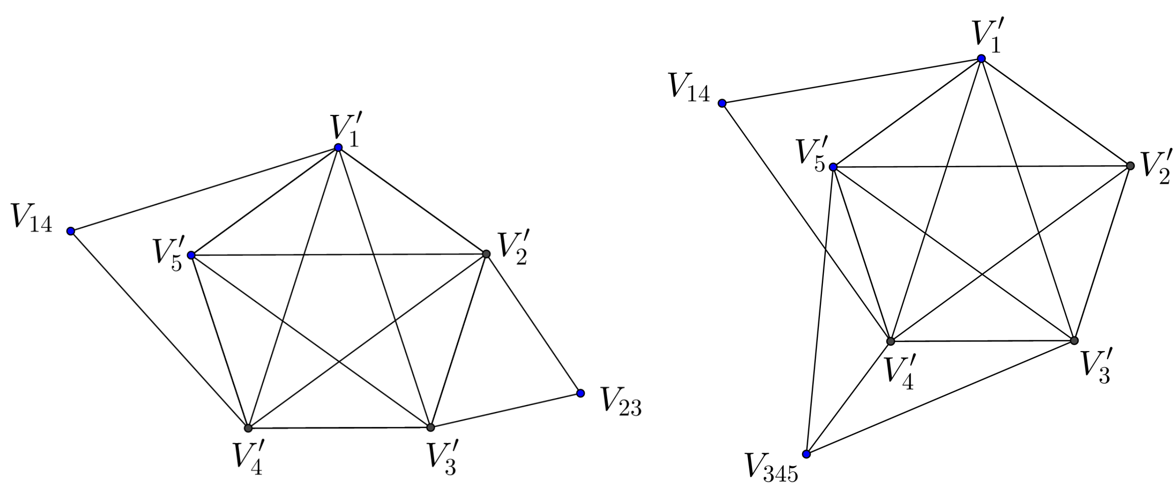

FIGURE 1. Graphs in family $\mathcal{F}$

Theorem 3.9. *Let G be a connected graph with $\omega(G) = 5$. Then $m^*(G) = 4$ if and only if for specified values $n_1, n_2, \ldots, n_9$, G is isomorphic to a graph H in $\mathcal{F}$.*

Proof. Let $G = (V, E)$ be a connected graph containing the complete graph $V(K_5) = \{v_1, v_2, \ldots, v_5\}$ and $m^*(G) = 4$. Let $Z = \{v_1, v_2, \ldots, v_5\}$. It follows from Lemma 3.2 that every vertex $u \in V - Z$ is adjacent to at least one vertex in Z. Further since G is K_6 free, u is adjacent to at most four vertices in Z. Therefore by Lemma 3.3 to Lemma 3.8, we conclude that $G \in \mathcal{F}$. To prove the converse, consider $H \in \mathcal{F}$. By Lemma 3.8, if $|V_{14}| = n_1$ and $|V_{23}| = n_2$, then V_{125} and V_{345} are empty sets. Given that $|V_{1234}| = n_5, |V_{1235}| = n_6, |V_{1245}| = n_7, |V_{1345}| = n_8$ and $|V_{2345}| = n_9$, then the basis matrices for VCS of the access structure $\Gamma(H)$ are:

$$S^1 \sim \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0_{n_1} & 0_{n_1} & 1_{n_1} & 0_{n_1} \\ 1_{n_2} & 0_{n_2} & 0_{n_2} & 0_{n_2} \\ 1_{n_5} & 0_{n_5} & 1_{n_5} & 0_{n_5} \\ 1_{n_6} & 0_{n_6} & 0_{n_6} & 1_{n_6} \\ 0_{n_7} & 0_{n_7} & 1_{n_7} & 1_{n_7} \\ 0_{n_8} & 1_{n_8} & 1_{n_8} & 0_{n_8} \\ 1_{n_9} & 1_{n_9} & 0_{n_9} & 0_{n_9} \end{bmatrix} \text{ and } S^0 \sim \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1_{n_1} & 0_{n_1} & 0_{n_1} & 0_{n_1} \\ 0_{n_2} & 1_{n_2} & 0_{n_2} & 0_{n_2} \\ 1_{n_5} & 1_{n_5} & 0_{n_5} & 0_{n_5} \\ 1_{n_6} & 1_{n_6} & 0_{n_6} & 0_{n_6} \\ 1_{n_7} & 1_{n_7} & 0_{n_7} & 0_{n_7} \\ 1_{n_8} & 1_{n_8} & 0_{n_8} & 0_{n_8} \\ 1_{n_9} & 1_{n_9} & 0_{n_9} & 0_{n_9} \end{bmatrix},$$

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 $m^*(H) \leq 4$. However H contains K_5, thus $m^*(H) = 4$. Now if $G \in \mathcal{F}$, then G is an induced subgraph of H and since G contains K_5 as a subgraph, we have $m^*(G) = 4$.

Further if V_{125} and V_{345} are not empty and $|V_{125}| = n_3$ and $|V_{345}| = n_4$, then by Lemma 3.8 dont exist V_{14} and V_{23} simultaneously. Let $V_{14} \neq \emptyset$, in this case the basis matrices for VCS of the access structure $\Gamma(H)$ are:

$$S^1 \sim \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0_{n_1} & 0_{n_1} & 1_{n_1} & 0_{n_1} \\ 0_{n_3} & 0_{n_3} & 0_{n_3} & 1_{n_3} \\ 0_{n_4} & 1_{n_4} & 0_{n_4} & 0_{n_4} \\ 1_{n_5} & 0_{n_5} & 1_{n_5} & 0_{n_5} \\ 1_{n_6} & 0_{n_6} & 0_{n_6} & 1_{n_6} \\ 0_{n_7} & 0_{n_7} & 1_{n_7} & 1_{n_7} \\ 0_{n_8} & 1_{n_8} & 1_{n_8} & 0_{n_8} \\ 1_{n_9} & 1_{n_9} & 0_{n_9} & 0_{n_9} \end{bmatrix} \text{ and } S^0 \sim \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1_{n_1} & 0_{n_1} & 0_{n_1} & 0_{n_1} \\ 1_{n_3} & 0_{n_3} & 0_{n_3} & 0_{n_3} \\ 1_{n_4} & 0_{n_4} & 0_{n_4} & 0_{n_4} \\ 1_{n_5} & 1_{n_5} & 0_{n_5} & 0_{n_5} \\ 1_{n_6} & 1_{n_6} & 0_{n_6} & 0_{n_6} \\ 1_{n_7} & 1_{n_7} & 0_{n_7} & 0_{n_7} \\ 1_{n_8} & 1_{n_8} & 0_{n_8} & 0_{n_8} \\ 1_{n_9} & 1_{n_9} & 0_{n_9} & 0_{n_9} \end{bmatrix}.$$

In this case, similar to discussion of above, 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. [1] have obtained a characterization of all connected graphs G where $m^*(G) = 3$. If $m^*(G) = 4$ then $\omega(G) \leq 6$. We have obtained previously in [6] a characterization of all connected graphs G for which $\omega(G) = 6$. In this paper, we obtained a characterization of all connected graphs G for which $\omega(G) = 5$. The next problem is to characterize all graphs where $m^*(G) = 4$ and $\omega(G) \leq 4$.

Acknowledgments

The author would like to thank the referee for his/her helpful remarks which have contributed to improve the presentation of the article.

References

[1] S. Arumugam, R. Lakshmanan and A. K. Nagar, Graph access structure with optimal pixel expansion three, *Inform. and Comput.*, **230** (2013) 67–75.

[2] S. Arumugam, R. Lakshmanan and A. K. Nagar, Visual cryptography scheme for graphs with vertex covering number two *Nat. Acad. Sci. Lett.*, **36** (2013) 575–579.

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

[4] G. Ateniese, C. Blundo, A. D. Santis and D. R. Stinson, *Construction and bounds for visual cryptography*, in: Proc. ICALP 96, Springer, Berlin, 1996 416–428.

[5] G. Chartrand and L. Lesniak, *Graphs and Digraphs*, fourth ed., Chapman and Hall, CRC, 2005.

[6] M. Davarzani, Visual cryptography scheme for graphs with pixel expansion four and clique number six, *Journal of Mathematical Cryptology*, (to appear).

[7] M. H. Dehkordi and A. Cheraghi, Maximal independent sets for the pixel expansion of graph access structures, *IUST Int. J. Sci. Eng.*, **19** (2008) 13–16.

[8] H. Hajiabolhassan and A. Cheraghi, Bounds for visual cryptography schemes, *Discret Appl. Math.*, **158** (2010) 659–665.

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

[10] E. R. Verheul and H. C. A. Van Tilborg, Constructions and Properties of k out of n Visual Secret Sharing Schemes, *Des. Codes Cryptogr.*, **11** (1997) 179–196.

[11] 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), *Theoret. Comput. Sci.*, **240** (2000) 471–485

M. Davarzani

Faculty of Mathematics and Computer Science, Kharazmi University, P.O.Box 1561836314, Tehran, Iran

Email: mahmood.davarzani@gmail.com

http://dx.doi.org/10.22108/toc.2019.113671.1599