NEW PARADIGM IN GRAPH-BASED VISUAL SECRET SHARING SCHEME BY ACCEPTING REVERSAL IN BLACK-WHITE IMAGES

Yuji SUGA
Canon Inc., PF Technology Development Center, 30-2, Shimomaruko 3-Chome, Ohta-ku, Tokyo 146-8501, Japan

Abstract: The visual secret sharing scheme (for short the VSS scheme) with access structure based on graph has been proposed as one of the (2,n)-threshold visual secret sharing schemes. Ateniese et al.[1] showed a decomposition method into star graphs from a given graph which edges are specified by qualified sets, that is, two different participants (two vertices in the graph) have a common edge if and only if they can decrypt the secret image by stacking each share images. In this paper, we expand the definition of black-white visual secret sharing scheme and propose new decomposition methods by splitting complete n-partite graphs. These methods improve contrast of the decoded secret image. Moreover, we obtain several optimal examples and evaluate on graph-based VSS schemes.

Key words: visual secret sharing scheme; n-partite graph; complete n-partite graph

1. INTRODUCTION

The visual secret sharing scheme (abbreviated as VSS scheme) proposed by Naor and Shamir[11] is a method to distribute secret image S into n shadow images w_i ($1 <= i <= n$) called shares. Shares are printed to materials with permeability that can be stacked physically like OHP sheets and each participant receives one share in secret. Any qualified participants can reconstruct the secret image visually by stacking shares, but forbidden participants cannot obtain any information about secret image. In the (k, n)-

threshold VSS scheme, any k out of n participants can decrypt the secret image, but any k-1 or fewer participants cannot decode.

The VSS schemes with various access structures (which differs from threshold schemes) for reconstruction have proposed. Ateniese et al.[11] proposed graph-based access structure, that is, vertices on a given graph are identified as participants with the following property. Two vertices have a common edge if and only if participants can decrypt the secret image by stacking shares. Graph-based access structure scheme with a complete graph, which any different two vertices have a common edge, is as same as (2, n) -threshold VSS scheme, so this implies that graph-based VSS scheme can be considered as an extension of (2, n) -threshold VSS scheme.

Ateniese et al. proposed "star graph decomposition method", this method means that given graph is divided into a collection of star graphs. This method has advantage that one can construct graph-based VSS scheme systematically for arbitrary given graph, but also has disadvantage of inefficient pixel expansion (a measure for contrast of reconstructed image).

One of approach is improving graph decomposition of their method, but we introduce new paradigm of VSS schemes as follows; we can accept "reversal image" which every pixel color is opposite in decoded image. In ordinary case, we use black-color in the object and white-color in the background, so we decrypt by stacking shares and understand secret image by recognizing more black as object in pre-image. In our new paradigm, we can accept reversal image, that is, we can understand the secret image by recognizing white areas as the object in pre-image. To introduce the weaker definition than ordinary definition of VSS schemes leads to get efficient constructions.

The rest of the paper is organized as follows. Section 2 mentions previous construction and defines our new definition of VSS schemes. Section 3 gives various efficient constructions in our new paradigm. Section 4 gives evaluation of our schemes and implies efficiency. Section 5 concludes this paper.

2. THE VSS SCHEME FOR GRAPH ACCESS STRUCTURE

2.1 Preliminaries

In this section, now we recall some terminologies on graph theory. A graph is a pair G = (V,E) consisting of a set V, referred to as the vertex set of G and a set E of 2-subsets of V, referred to as the edge set of G. Assume that our graph does not contain loops, undirected edges and multiple edges. For given G, we define the adjacency matrix (a_{ij}) (whose rows and columns are indexed by the elements of V) where the (i,j)-th entry a_{ij} = 1 if and only if (x_i,x_j) is a vertex in E.

We say that G'= (V',E') is a subgraph of G = (V,E) if V' is a subset of V and E' is a subset of E. Furthermore, subgraph G'=(V',E') is called induced subgraph of G if it satisfies that E' consists of E that have both vertices in V'. Let Ind(G) be the collection of induced subgraphs of G, we define that Ind(G) include G, but Ind(G) does not contain an empty graph (a graph with no edge). A complete graph is a graph in which each pair of distinct vertices is joined by an edge, and the complete graph on n vertices is denoted by K_n. For any graphs G, a complete subgraph of G is called a clique of G. The number of vertices in a largest clique of G is denoted by c(G).

A graph G is called n-partite if the vertex set V can be partitioned into k nonempty sets V_1, V_2, ... ,V_n such that every edge of G joins vertices from different subsets. The n-partite graph G is called complete n-partite if, for each i, j (i does not equal j), every vertex of V_i is adjacent to every vertex of V_j, and the complete n-partite graph is denoted by $K_{a1,a2,\ldots,an}$ where $|V_i|=a_i$ for each i. Especially, G is called complete bipartite graph if k=2. The n-partite graph for G = (V(G),E(G)) (denoted by $K_{a1,a2,\ldots,an}(G)$) is a subgraph of $K_{a1,a2,\ldots,an}$ if every vertex of V_i is adjacent to every vertex of V_j such that (v_i, v_j) in E(G) where a vertex set V(G) = {v_1, v_2, ... , v_n} is correspond with a partitioned subsets {V_1, V_2, ... , V_n}.

2.2 The model

We assume that a secret image is a black-white image which is encoded to n images w_i (1 <= i <= n). Each pixel (in an original image) expands to m subpixels (in distributed images) and parameter m is called pixel expansion. In expression of images, we denote white pixel and black pixel by 0 and 1 respectively, this notation is used for both of a secret image and shares. By

stacking two shares, we can decode a secret image visually because of the difference of the number of black pixel in the OR-operated subpixels.

We introduce basis matrices containing two matrices denoted by S0 and S1 written how to share shadow images.

2.2.1 Basis matrices

When we generate shares, we use basis matrices which row vectors are indexed by a set of shares $W = \{w_i \mid 1 <= i <= n\}$. These matrices are expressed in n by m binary matrices where m is pixel expansion. We denote graph-based VSS scheme with graph G and pixel expansion m by GVSSS-(G, m).

For any vector v, w(v) is the Hamming weight of v, that is, the number of "1" in v. For any binary matrix B which the i-th row vector of B denotes b_i, we define symmetric matrix R(B) which the (i,j)-th element equals $w(b_i) + w(b_j)$. For any matrix A, we define normalized matrix norm(A) such that $(\mathrm{norm}(A))_{xy} := 0$ if $A_{xy}=0$, $(\mathrm{norm}(A))_{xy} := 1$ if A_{xy} does not equal to 0.

Definition 1 [Basis matrices of GVSSS-(G, m)]

|V(G)| by m basis matrices S0, S1 with respect to GVSSS-(G, m) satisfies that norm(R(S1) - R(S0)) = Adj(G) where Adj(G) is an adjacency matrix of G.

Example 2

$$Adj(G) = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}, \quad S_0 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad S_1 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

$$R(S_0) = \begin{bmatrix} 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 1 & 1 & 1 \\ 2 & 2 & 2 & 1 & 1 & 1 \\ 2 & 2 & 2 & 1 & 1 & 1 \end{bmatrix}, \quad R(S_1) = \begin{bmatrix} 2 & 3 & 3 & 3 & 2 & 2 \\ 3 & 2 & 3 & 2 & 3 & 2 \\ 3 & 3 & 2 & 2 & 2 & 3 \\ 3 & 2 & 2 & 1 & 2 & 2 \\ 2 & 3 & 2 & 2 & 1 & 2 \\ 2 & 2 & 3 & 2 & 2 & 1 \end{bmatrix}.$$

Restriction of Definition 1 is "weaker" than original difinition[1] because of the following viewpoints; 1) We do NOT consider the case of three or more shares and 2) We can allow "reversal image" (which every pixel color

is opposite) in decoded image. Due to above two restrictions, we can reduce an increase of pixel expansion and obtain higher contrast in the reconstructed image. Please keep in mind that theorem 7 mentioned latter does not match previous result (Th 5.2 in Ateniese paper[1]) because of the difference of definitions.

2.2.2 The minimum pixel expansion

For given graph G, let m*(G) be the minimum of m if GVSSS-(G, m) exists. We call GVSSS-(G, m) is optimal if m=m*(G). The following results are known on m*(G).

Theorem 3 [Th 7.3 in Ateniese paper[1]] $m^*(K_n) = \min \{ m \mid n <= {}_mC_{[m/2]} \}$.

Theorem 4 [Th 7.4 in Ateniese paper[1]] $m^*(G) >= m^*(K_{c(G)})$.

Theorem 4 gives a lower bound of m*(G), however problem to calculate the greatest clique for given graph G is known as a NP problem.

2.2.3 Independent graph-based VSS schemes

In some case of choosing basis matrices, we see the next boring example, which has same row vectors in basis matrices. This means that different participants have same shares.

Example 5

$$Adj(G) = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \; S_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}, \; S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

Now we define new concept because we would like to exclude the above case.

Definition 6 [Independent]

The GVSSS-(G, m) is called independent if all shadow images are different each other, strictly speaking, i, j does not exist such that w_i-th vector in S0 equal w_j-th vector in S0 and w_i-th vector in S1 equal w_j-th vector in S1.

Note that example 2 is independent, but example 5 is not independent. We discuss independent graph-based VSS schemes and some results are obtained.

Theorem 7

If there exists an independent GVSSS-(G, 2), G is included in Ind(K_{22}).

[Proof]

(=>) In case of m=2, we enumerates all possible row vectors of S0, S1as follows:

$$\tilde{S_0} = \begin{matrix} w_1) \\ w_2) \\ w_3) \\ w_4) \\ w_5) \\ w_6) \end{matrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \tilde{S_1} = \begin{matrix} w_1) \\ w_2) \\ w_3) \\ w_4) \\ w_5) \\ w_6) \end{matrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

So we can calculate R(˜S1) - R(˜S0) as follows;

$$R(\tilde{S_1}) - R(\tilde{S_0}) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

We consider norm(R(˜S1) - R(˜S0)), and omit rows and columns which each elements are all 0 (w_1) and w_6)). So we can obtain an adjacent matrix of $K_{2,2}$.

(<=) It is enough that we show an example of GVSSS-($K_{2,2}$, 2) (See example 8). Q.E.D.

Example 8

$$Adj(G) = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad S_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}, \quad S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Corollary 9

If there exists an independent GVSSS-(G, 3) such that G is not included in Ind(K_{22}), GVSSS-(G, 3) is optimal.

We can see that example 8 is optimal. Moreover, we obtain the following theorem and corollary straightforwardly.

Theorem 10

If there exists a GVSSS-(G, 2), G is included in Ind($K_{a1,a2, \ldots ,a4}(K_{2,2})$).

Corollary 11

If there exists a GVSSS-(G, 3) such that G is not included in Ind($K_{a1,a2, \ldots ,a4}(K_{2,?})$), GVSSS-(G, 3) is optimal.

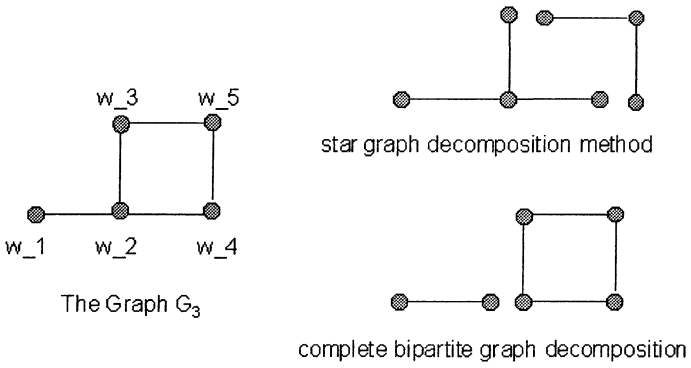
3. CONSTRUCTIONS BY GRAPH DECOMPOSITION

In this section, we treat some graph decomposition methods as constructions of basis matrices. First, we recall star graph decomposition method as a previous construction with no efficiency. Next, we propose new methods and show that our methods have usefulness at a point of view "whether to be optimal or not".

3.1 The star graph decomposition method

The star graph decomposition method is proposed in Ateniese paper[1], this method means that we divide given graph G into star graph $K_{1,a}$ which edges are joined to only one vertex (called the center vertex). We can construct GVSSS-($K_{1,a}$, 2) with basis matrices S0, S1 such that each row vector in S0 have {1,0} , a row vector with related to the center vertex in S1 has {1,0} and the others have {0,1}. Finally we concatenate basis (sub)matrices of all star graphs side by side, so we can construct GVSSS-(G, 2 b(G)) for any given graphs where b(G) is the number of decomposed star graphs.

Figure 1 [Difference of decomposition methods]



Example12 [The star graph decomposition method]
The star graph decomposition for graph G_3 in Blundo's paper[2] at figure 1(left) causes GVSSS-(G_3, 4) because of decomposition expressed at figure 1 (upper right) which basis matrices are as follows:

$$S_0 = \begin{matrix} w_1) \\ w_2) \\ w_3) \\ w_4) \\ w_5) \end{matrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad S_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

3.2 The complete n-partite graph decomposition method

We propose new extended method that we decompose complete n-partite graphs instead of star graphs, that is, we treat GVSSS-($K_{a1,a2,\ldots,an}$, m*(K_n)). Actually, we use basis matrices derived from GVSSS-(K_n, m*(K_n)) which row vectors are iterate a_i times for each i.

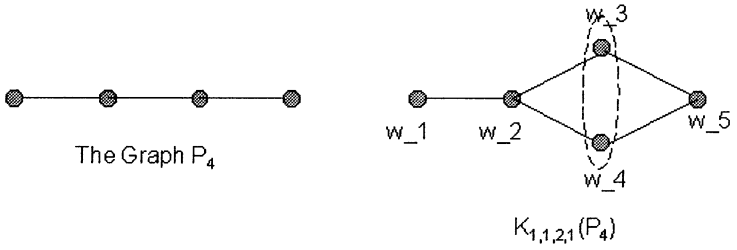
Example 13 [The complete n-partite graph decomposition method]
The decomposition for graph G_3 causes GVSSS-(G_3, 4) because of decomposition expressed at figure 1 (lower right) which basis matrices are as follows:

$$S_0 = \begin{matrix} w_1) \\ w_2) \\ w_3) \\ w_4) \\ w_5) \end{matrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad S_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

3.3 The n-partite graph decomposition method

We propose new extended method with decomposed graph which we consider the n-partite graph $K_{a1,a2,\ldots,an}(G)$ (for given graph) instead of star graph, that is, we treat GVSSS-($K_{a1,a2,\ldots,an}$, m*(G)). Actually, we use basis matrices derived from GVSSS-(K_n, m*(G)) which rows are iterate a_i times for each i.

Figure 2 [n-partite graph decomposition method]



Example 14 [The n-partite graph decomposition method]
Note that P_n is a path with n vertices. There is a GVSSS-(P_4, 3) which basis matrices are as follows:

$$S_0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \; S_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

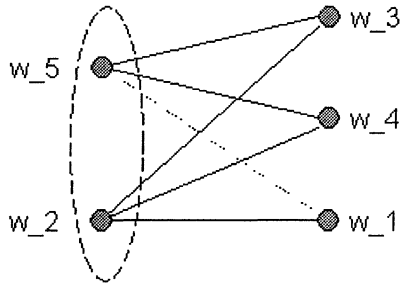
So, we can extend basis matrices by using our proposed method mentioned above, w_3 and w_4 have same share image each other.

$$S_0 = \begin{matrix} w_1) \\ w_2) \\ w_3) \\ w_4) \\ w_5) \end{matrix} \left[\begin{array}{c|cc} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{array}\right], \; S_1 = \left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right].$$

3.4 The edge-deletion method

This method means that we represent edge set (of given graph) as edge sets of $K_{a1,a2,\ldots,an}$ and $K_{a1,a2,\ldots,an}(G)$ with "difference for set", then we realize by exchange S0, S1 each other in "difference".

Figure 3 [The Graph $K_{2,3}$ - $K_{1,1}$]



Example 15 [The edge-deletion method]

In figure 2, we can describe that $E(G_3)=E(K_{2,3})$ - (w_1, w_5) $=E(K_{2,3})$ - $E(K_{1,1})$. When we obtain basis matrices from concatenation of GVSSS-($K_{2,3}$, 2) and GVSSS-($K_{1,1}$, 2), we do the following process beforehand. The above process is the deletion of an edge (w_1, w_5), that is, exchange of S0, S1 in GVSSS-($K_{1,1}$, 2).

$$S_0 = \begin{matrix} w_1) \\ w_2) \\ w_3) \\ w_4) \\ w_5) \end{matrix} \left[\begin{array}{c|cc} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{array}\right], \; S_1 = \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{array}\right].$$

Remark 16

Note that example 14,15 are optimal from corollary 11, because G_3 is not included in $\mathrm{Ind}(K_{a1,a2,\ldots,a4}(K_{2,2}))$ for any a_i's. Furthermore we can see that $\mathrm{Ind}(K_{2,2}) = \{P_2, P_3, C_4 (=K_{2,2})\}$ where graph C_n is a cycle with n vertices.

4. EVALUATION AND VARIATION

We already see that some optimal examples exist, so it is natural to have been renewal of interest in clarification of optimal graph-based VSS schemes. Several studies have been made on classification of optimal case in ordinary (non visual) secret sharing schemes, Blundo et al.[2] restricted the number of participants and classified at small order. On the other hand, we choose the pixel-expansion-fix approach because this approach is more suitable than participant-fix approach.

4.1 Classification in the case of m* is at most 3

Theorem 7 means that classification of optimal graph-based VSS scheme GVSSS-(G, 2) have already finished, now we consider the case of $m^* = 3$ as same as theorem 7. So, we obtain C_6, P_5 as optimal cases and the basis matrices of GVSSS-(C_6 ,3) are the following example.

Example 17 [GVSSS-(C_6 ,3)]

$$S_0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad S_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Note that P_5 is subgraph of C_6, so the basis matrices of GVSSS-(P_5 ,3) is derived from the basis matrices of GVSSS-(C_6 ,3) by using only some 5 rows.

4.2 Evaluation on Graph-type VSS scheme

An extended scheme called by the Graph-type VSS scheme has been introduced[14], this scheme focuses on the distance of two vertices instead of the existence of edge. In the Hamming graph $L_2(3)$ with 9 vertices, we can

reduce the parameter of pixel expansion from 21 to 6. Note that if we use star graph decomposition method, we need 30 as pixel expansion.

4.3 Reuse for the color/gray-scale images

We show the ability to reuse basis matrices of optimal graph-based VSS scheme for the black-white image and extend into the color/gray-scale images similarly. Assume that a secret image has different t colors ($\{c_1,c_2, \ldots ,c_t\}$) and one of them (denoted by 1) is the strongest color which can cover other colors by stacking shares. For example, color sets are R(red), G(green), B(blue) and 1(black).

Our proposal method is as follows: 1) we change 0 and 1 in basis matrices of the black-white image into 1 and c_i (some color) for all non-black colors, then 2) we concatenate new basis matrices similarly mentioned above. In this case, the pixel expansion equals mt when we apply GVSSS-(G ,m).

5. CONCLUSION

We proposed optimal constructions of graph-based VSS scheme over the new definition that brings higher constant of reconstructed secret image. In new definition, we obtain optimal GVSSS-(G ,m) such that m = 2,3 and suggested an extended construction for color images by re-using basis matrices of the black-white images.

REFERENCES

1. G.Ateniese, C.Blundo, A.D. Santis, D.R. Stinson, Visual Cryptography for General Access Structures, Information and Computation 129, 86-106, 1996.
2. C.Blundo, A.D.Santis, D.R.Stinson, U.Vaccaro, Graph decompositions and secret sharing schemes, EUROCRYPT'92, pp.1-24, 1992.
3. E. Bannai and T. Ito, Algebraic Combinatorics I :Association schemes, Benjamin / Cummings, Menlo Park, California, 1984.
4. C.Blundo, A.D.Santis, D.R.Stinson, On the Contrast in Visual Cryptography Schemes, Journal of Cryptology 12, 261-289, 1999.
5. J.Clark, D.A.Holton, A First Look at Graph Theory, World Scientific Publishing, 1991.
6. New results on visual cryptography, CRYPTO'96, pp.401-415, 1996
7. M.Iwamoto, H.Ymamamoto, A visual secret sharing scheme for plural images (in Japanese), SITA2001, pp.565-568, 2001.

8. T.Kato, H.Imai, An extended construction method of visual secret sharing scheme (in Japanese), IEICE Trans., vol. J79-A, no.8, pp.1344-1351, 1996.
9. H.Koga, H.Yamamoto, Proposal of a Lattice-Based VSSS for Color and Gray-scale Images, IEICE Trans. on Fundmentals, vol. E81-A, no.6, pp.1262-1269, 1998.
10. H.Kuwakado, H.Tanaka, Polynomial representation of visual secret sharing scheme for black-white images, 2001 Symposium on Cryptography and Information Security, pp.417-422, 2001.
11. M.Naor, A.Shamir, Visual Cryptography, EUROCRYPT'94, pp.1-12, 1994.
12. M.Naor, A.Shamir, Visual Cryptography 2, Lecture Notes in Computer Science 1189, pp.179-202, 1997.
13. A.Shamir, "How to Share a Secret", Commun.of ACM, Vol.22, No.11, pp.612-613, 1979.
14. Y.Suga, K.Iwamura, K.Sakurai, H.Imai, Extended Graph-type Visual Secret Sharing Schemes with Embedded Plural Secret Images (in Japanese), IPSJ JOURNAL Vol.42 No.08, pp.2106-2113, 2001.
15. E.R.Verheul, H.C.A.van Tilborg, Constructions and properties of k out of n visual secret sharing scheme, Designs, Codes, and Cryptography, vol.1, no.2, pp.179-196, 1997.