複数の機密画像を埋め込み可能なグラフタイプ視覚復号型秘密分散方式の拡張

須賀祐治[†] 岩村恵市[†]
櫻井幸一[††] 今井秀樹[†††]

(k,n)-しきい値視覚復号型秘密分散法は，復元するための権限としては平等に分散情報が分配されるため，さまざまなアクセス構造が想定される実利用においてはうまく適用できないことが多い．以上の背景のもと，グラフで表現されたアクセス構造を持つ視覚復号型秘密分散法が提案されている．本稿ではこの概念を拡張して，辺の有無ではなく2頂点間の距離に基づいたアクセス構造を持つ視覚復号型秘密分散法を提案する．2枚のシェアを重ねあわせたときに，シェアの距離により復元される機密画像が異なるような視覚復号型秘密分散法を構成することを実現した．また復元画像のコントラストの改善を検討し，より見やすい構成方法についても新たに提案する．

Extended Graph-type Visual Secret Sharing Schemes with Embedded Plural Secret Images

Yuji Suga,[†] Keiichi Iwamura,[†] Kouichi Sakurai[††]
and Hideki Imai[†††]

Visual secret sharing schemes with (k,n)-threshold access structure are not feasible for real world, then the schemes with access sturcture based on graph have been proposed. In this paper, we propose new visual secret sharing schemes with graph access structures based on the distance of 2 vertices instead of the existence of edge, in which reconstructed secret image can be made different on the distance if we stack 2 shares. And we propose new constructions to achieve higher constract of the reconstructed image.

1. はじめに

秘密分散法（Secret Sharing Scheme）の一例である (k,n)-しきい値秘密分散法は，機密情報 S を n 個の分配情報（シェア）w_i $(1 \leq i \leq n)$ に符号化する方式であり，任意の k $(k \leq n)$ 個の分配情報から機密情報 S を復号することは可能であるが，$k-1$ 個以下の分配情報からは機密情報 S に関する情報はまったく得られないという性質を持つ．多項式を用いた (k,n)-しきい値秘密分散法は Shamir により構成された[18]．

新しいタイプの秘密分散方式として，機密情報および分散情報に画像を用いる視覚復号型秘密分散法（Visual Secrect Sharing Scheme，VSSS）[16]が提案されている．機密画像を複数のシェア画像にあらかじめ分散し OHP スライドのように透過性を持ち物理的に重ねあわせが可能なものに印刷しておく．元の機密画像を復元する際にはそれぞれのシェア画像を重ねあわせる操作により，特に計算機のリソースを使うことなく，目の錯覚を利用して機密画像を復元することができる．

VSSS は (k,n)-しきい値秘密分散法に基づく方式（以下 (k,n)-VSSS）が構成[16]され，これまでに

- 復元時のコントラスト（見やすさ）の改善[11),12)]
- グレースケール・カラー画像への適用[14),17)]
- 一般的な復元のためのアクセス構造の検討[1),5)]

などの切り口で研究の進展がなされており，本稿では最後のアクセス構造に着目して新しい方式を提案する．

(k,n)-VSSS は各シェア画像に対して平等に復元のための権限が与えられている．しかし機密情報の分散を目的に実際に VSSS を利用する場合には，復元のための特権を持つメンバーが存在したり，特定のグ

† キヤノン株式会社画像技術研究所
Visual Information Technology Development Laboratory, CANON INC.
†† 九州大学大学院システム情報科学研究院情報工学部門
Graduate School of Information Science and Electrical Engineering, Kyushu University
††† 東京大学生産技術研究所
Institute of Industrial Science, University of Tokyo

ループ内のメンバーだけでは復元が許可されないなどの多様なアクセス構造が必要とされる．以上の背景のもとグラフで表現されたアクセス構造（graph-based access structure）を持つ VSSS [1]であるグラフタイプ VSSS（以下 GVSSS）が提案されている．

GVSSS では，グラフの頂点集合をシェア画像の集合と対応づけ，2 頂点間に辺が存在する場合には（2 頂点に対応する 2 つのシェア画像から）機密画像が復元され，辺がない場合には復元されないというアクセス構造を持つ．$(2,n)$-VSSS は，上記のグラフとして完全グラフを利用した場合に相当するため GVSSS は $(2,n)$-VSSS の拡張と考えることができる．本稿ではさらに GVSSS の概念を拡張して，辺の有無（つまり距離 1 かどうか）ではなく 2 頂点間の距離に基づいたアクセス構造を持つ GVSSS を提案する．既存の GVSSS では 1 つの機密画像のみがシェア画像に埋め込まれていたが，本稿で提案するスキームでは 2 枚のシェア画像を重ねあわせたときに，シェア間の距離に応じて復元される機密画像が異なるような GVSSS を構成することを実現した．このように複数の機密画像を埋め込むことができるため，既存の GVSSS に比べ利用用途が広がると考えられる．また，特に強正則グラフに対して機密画像のコントラストの改善を検討し，既存方式に比べより見やすい構成方法についても新たに提案する．

2. 従来の視覚復号型秘密分散法

2.1 視覚復号型 (k,n)-しきい値秘密分散法

Naor らによる (k,n)-VSSS [16]の構成方法について説明する．機密画像 SI は 2 値（白黒）画像とし各画素成分 $SI(x,y)$ は画素が白（透明）の場合には 0，黒の場合には 1 と表現するものとする．機密画像 SI を構成する各画素は，シェア画像においては m 個の画素で表現される．つまり成分 $SI(x,y)$ はシェア画像において m 画素で構成される (x,y) ブロックに対応し，シェア画像は機密画像の m 倍に拡大される．この m を画像拡大率と呼ぶ．m が平方数であればシェア画像の縦横比を変更しないで構成できるが，非平方の場合には，比率を変える，画素形状を変える，平方数になるように冗長部分を付けるなどの処理が必要となる．

複数枚のシェア画像を重ねあわせた際に各ブロック（m 個の部分画素）における黒画素数の差（コントラスト）によって，白か黒かが視覚的に認識され，機密画像を得ることができる．

シェア画像の構成には後述する生成行列を用いる．以下 (k,n)-VSSS における (1) 生成行列の定義，(2) 分散画像の構成方法，(3) 具体的な生成行列の例を示す．

2.1.1 生成行列の定義

(k,n)-VSSS におけるシェア画像の構成には 2 種類の生成行列（Basis Matrix）S_0 および S_1 を用いる．これらの各生成行列は，ともに $n \times m$ のバイナリ行列（成分が 0 か 1）であり，行列の各行はシェア画像の集合 $W = \{w_i | 1 \le i \le n\}$ により添字付けされる．2 つのしきい値 d_0，d $(1 \le d_0 < d \le m)$ に対して，生成行列 S_0，S_1 は次の 3 つの性質を持つ．

(i) S_0 の任意の異なる k 個の行ベクトルを選択し，OR（論理和）演算を施したベクトルの重みは d_0 以下である．

(ii) S_1 の任意の異なる k 個の行ベクトルを選択し，OR 演算を施したベクトルの重みは d 以上である．

(iii) $1 \le q < k$ を満たす q 個の任意の部分集合 $W' = \{w_{i_1}, \ldots, w_{i_q}\} \subset W$ に対し，S_0，S_1 の行をそれぞれ W' に制限した 2 つの $q \times m$ 行列は，列の入替えにより同じ行列となる．

相対差 α を $\alpha = (d - d_0)/m$ と定義する．相対差は復元する際に白か黒かを判別する際の重要なパラメータであり，できるだけ大きいことが望まれる．また視覚的に復元可能な α の値は 1/25 程度までとされ，それ以上小さくなると機密画像の復元が困難になる．

2.1.2 シェア画像の構成方法

前項の性質を持つ生成行列 S_0，S_1 を用いて機密画像 SI からシェア画像を作成する方法を説明する．機密画像 SI の各成分 $SI(x,y)$ に対して次の処理を行う．

(1) 生成行列として，$SI(x,y) = 0$ の場合は S_0，$SI(x,y) = 1$ の場合は S_1 を選択する．

(2) m 次の置換群から置換 ϕ を任意に選ぶ．

(3) 各シェア画像 w_i $(1 \le i \le n)$ の (x,y) ブロックは，生成行列の w_i 行成分（m 変数のベクトル）に置換 ϕ を施したものとする．

2.1.3 生成行列の例

$(3,3)$-VSSS を構成する生成行列の例をあげておく．この例では $m = 4$，$\alpha = 1/4$ である．

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

2.2 グラフタイプ VSSS

Ateniese ら[1]によるグラフタイプ VSSS（Graph-type VSSS，GVSSS）について説明する．グラフ G

とは，頂点集合 V と，辺（$V \times V$ の元）集合 E とのペアであり，$G = (V, E)$ と記述される．本稿では，多重辺やループを持たない無向グラフと仮定する．

GVSSS [1]は，頂点集合 V を VSSS におけるシェア画像の集合 $W = \{w_i | 1 \leq i \leq n\}$ と同一視し，2 つのシェア画像（2 頂点）間に辺が存在する場合には機密画像が復元され，辺がない場合には復元されないというアクセス構造を持つ．

以上の定義のもと，一般のグラフに対して（グラフを固定したときの）画像拡大率の最小値 m^* に関するいくつかの定理と，頂点数が 4 までのすべての無向グラフに対して m^* と生成行列が分類されている[1]．

2.2.1 スターグラフ分割による構成

一般のグラフに関してシステマティックに GVSSS を構成する方法[1]を紹介する．グラフ G をスターグラフ，つまり 1 頂点（中心）からしか辺が存在しないグラフに分割する．スターグラフは，S_0 の各行を $\{1, 0\}$，S_1 の各行を中心頂点のみ $\{1, 0\}$ それ以外を $\{0, 1\}$ とした画像拡大率 2 の生成行列を持つ GVSSS が構成できる．この画像拡大率 2 の生成行列を利用し，分割されたスターグラフの生成行列を連結（各分割スターグラフの生成行列を横に並べる☆）することでグラフ G に対する生成行列を構成することができる．分割されたスターグラフの個数を β とすると，画像拡大率は $m = 2\beta$ であり，相対差は $\alpha = 1/m = 1/(2\beta)$ である．

図 1（左）のグラフ G_6 をスターグラフ分割する場合には最低 4 つのコンポーネントを必要とする．そのため本構成法では最小で画像拡大率が 8（つまり相対差は最大 1/8）の生成行列を持つ GVSSS しか構成できない．しかし次の生成行列により画像拡大率 3（つまり相対差は 1/3）の GVSSS を構成することが知られている．

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

上記の例は，スターグラフ分割法は必ずしも相対差が最大となる構成方法ではないことを示しており，コントラストを改善する研究の余地が残されている．次章では辺の有無による機密画像の復元の可否というスキームを拡張して，新しいアクセス構造を持つ GVSSS を提案するが，スターグラフ分割法を利用した構成方法よりも相対差を大きくする手法についても検討している．

☆ 生成行列の連結方法については 3.3.1 項における方式に準じる．

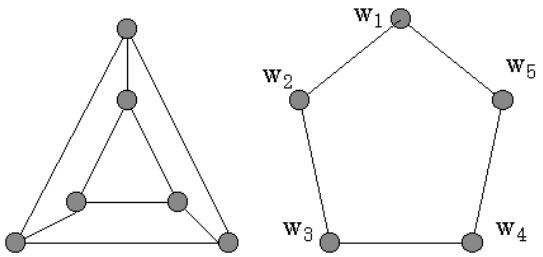

図 1 グラフ $G_6, P(5)$
Fig. 1 The graphs $G_6, P(5)$.

3. GVSSS の拡張

本章にて GVSSS の拡張を行うが，まずいくつかの記号の定義をしておく．n 頂点グラフ $G = (V, E)$ の最大距離を D としたとき，$V \times V$ は 2 点間の距離により $E_0, E_1 (= E), \ldots, E_D$ に分割することができる．つまり $E_i := \{(x, y) \in V \times V | x, y$ の距離が $i\}$ とすると $V \times V = \bigcup_{i=0}^{D} E_i$ となる．さらに E_i に対する $n \times n$ 隣接行列 A_i を次のように定義する．

$$(A_i)_{xy} := \begin{cases} 1 & \text{if } (x, y) \in E_i, \\ 0 & \text{if } (x, y) \notin E_i. \end{cases}$$

$\Gamma := \{1, \ldots, D\}$ を $\Gamma = \bigcup_{i=1}^{l} \Gamma_i$ となるような互いに素な l 個の部分集合 $\Gamma_1, \ldots, \Gamma_l$ に分割する．特に $\Gamma_0 := 0$ とおく．このとき $E_{\Gamma_k} := \bigcup_{j \in \Gamma_k} E_j$ とすると，$V \times V = \bigcup_{k=0}^{l} E_{\Gamma_k}$ となる．

以上の定義のもと 2 頂点の距離に基づき次のような 2 つのスキームを導入することができる．

アクセス構造（1）
特に $l = 2$ つまり $V \times V = E_0 \cup E_{\Gamma_1} \cup E_{\Gamma_2}$ と仮定する．異なる 2 頂点 w_i，w_j を選択したとき $(w_i, w_j) \in E_{\Gamma_1}$ の場合は機密画像が復元されるが，$(w_i, w_j) \in E_{\Gamma_2}$ の場合は復元できない．

アクセス構造（2）
異なる 2 頂点 w_i，w_j を選択したとき $(w_i, w_j) \in E_{\Gamma_k}$ の場合は機密画像 SI_k が復元される．つまり l 個の機密画像 SI_k $(1 \leq k \leq l)$ のうちいずれかが復元される．

以下，それぞれのアクセス構造に対して構成する方

式を検討する．

3.1 アクセス構造（1）

$\Gamma_1 = \{1\}$ すなわち $E_{\Gamma_1} = E$ を満たす場合は，従来型 GVSSS に相当する．つまり，異なる 2 頂点 w_i，w_j を選択したとき $(w_i, w_j) \in E_{\Gamma_1}$ の場合は機密画像が復元されることから，新しいグラフとして $G_1 = (V, E_{\Gamma_1})$ を考えることにより，従来型 GVSSS に帰着することができる．

3.2 アクセス構造（2）

$l \geq 3$ の場合も 2^l 個の拡張生成行列を考えることにより同様に構成可能であるため，本節では特に $l = 2$ の場合についてのみ取り上げる．2 つの機密画像を SI_1，SI_2 としそれぞれの画素成分を $SI_1(x, y)$，$SI_2(x, y)$ とする．また SI_1，SI_2 の画素数は同一であるとする．

3.2.1 拡張生成行列の定義

従来のように 2 つの生成行列を用いるのではなく，$S_{(0,0)}$，$S_{(1,0)}$，$S_{(0,1)}$，$S_{(1,1)}$ の 4 $(= 2^2)$ つの拡張生成行列を利用する．これらの拡張生成行列は次の 3 つの性質を持つように生成する．ただし $W = \{w_i | 1 \leq i \leq n\}$ で添字付けされたバイナリ行列 B に対して，(w_i, w_j) 成分を B の w_i 行目のベクトルと w_j 行目のベクトルの OR 演算を施したベクトルの重みと定義した対称行列を $R(B)$ とおく．

$(i)'$ $R(S_{(1,0)}) - R(S_{(0,0)})$ は $\sum_{i \in \Gamma_1} A_i$ の定数倍である．

$(ii)'$ $R(S_{(0,1)}) - R(S_{(0,0)})$ は $\sum_{i \in \Gamma_2} A_i$ の定数倍である．

$(iii)'$ $R(S_{(1,1)}) - R(S_{(0,0)})$ は $\sum_{i \in \Gamma_1 \cup \Gamma_2} A_i$ の定数倍である．

3.2.2 シェア画像の構成方法

機密画像 SI_1，SI_2 の各成分 $SI_1(x, y)$，$SI_2(x, y)$ に対して，$SI_1(x, y) = a$ かつ $SI_2(x, y) = b$ の場合に生成行列として $S_{(a,b)}$ を選択する．以降の処理は 2.1.2 項と同様である．

3.2.3 生成行列の例

図 1（右）のグラフ $P(5)$ に対して，$\Gamma_1 = \{1\}$，$\Gamma_2 = \{2\}$ となるアクセス構造（2）を構成する $m = 7$ の生成行列は次のとおりである．

$$S_{(0,0)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix},$$

$$S_{(1,0)} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix},$$

$$S_{(0,1)} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$S_{(1,1)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

図 2 はそれぞれ w_i $(1 \leq i \leq 5)$ に対応したシェア画像（ただし $m = 9$ に拡張）と，シェア画像を重ねあわせたときの復元画像として $w_1 + w_2$，$w_1 + w_3$，$w_2 + w_3$ の例を示した．距離 1 の場合には機密画像 SI_1「1」が，距離 2 の場合には機密画像 SI_2「2」が復元される．

3.2.4 既存方式との違い

アクセス構造（2）は複数画像を埋め込むことのできる従来の提案と類似しているようにとらえられるが，提案方式は次を満たし，既存方式とは異なることに留意されたい．

- 複数の画像が埋め込まれている領域が異なる方式[12]ではない．
- 重ねあわせる枚数により異なる復元画像を得る方式[9),11)]ではない．
- シェア画像を 1 画素分ずらすことにより異なる復元画像を得る方式[7]ではない．

3.3 一般的な構成方法と考察

3.3.1 生成行列連結による構成法

従来型 GVSSS からアクセス構造（2）を持つ GVSSS を構成する単純な方式を述べる．グラフ $G_1 = (V, E_{\Gamma_1})$ に基づく GVSSS の生成行列を $S_0(G_1)$，$S_1(G_1)$，画像拡大率を $m(G_1)$ とし，グラフ $G_2 = (V, E_{\Gamma_2})$ においても同様の記号を用いる．このとき $S_{(a,b)} := [S_a(G_1)|S_b(G_2)]$ とする画像拡大率 $m(G_1) + m(G_2)$ の 4 つの生成行列を用いてアクセス構造（2）を持つ GVSSS が構成できる．しかし l が増大するに従い画像拡大率が大きくなる欠点がある．

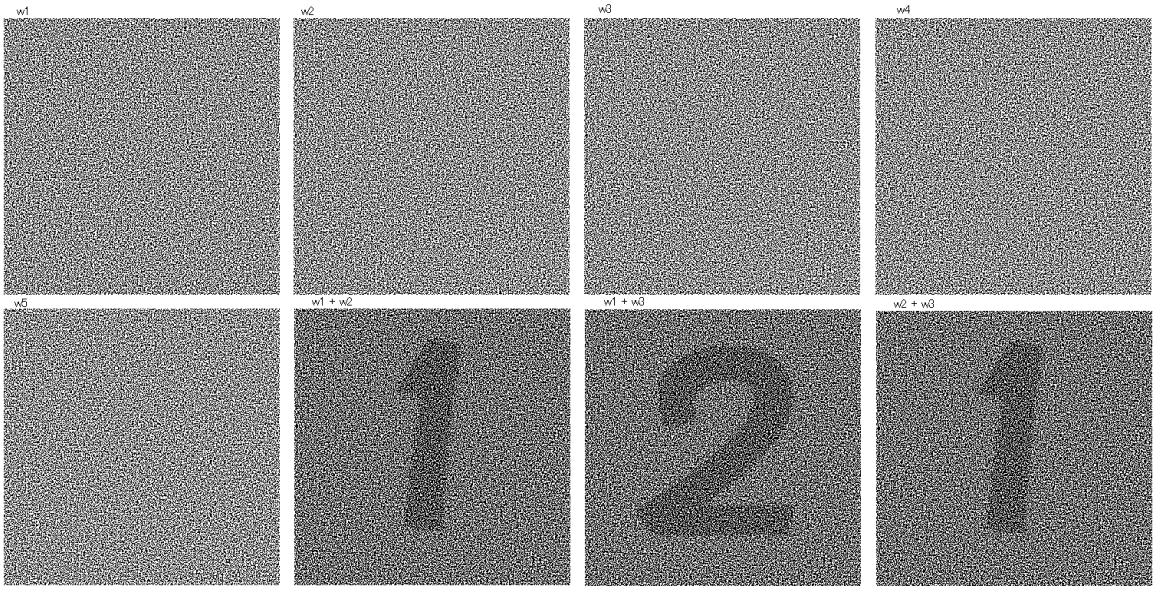

図 2 シェア画像と復元画像
Fig. 2 The share images.

3.3.2 強正則グラフの利用

本節では以下の考察によりグラフに対して強正則という制約を設けたうえで検討を行った．以降において，I は単位行列，J は成分がすべて 1 の行列を表すものとする．一般に，バイナリ行列 B のすべての行ベクトルが同じ重み（ここでは k_B）を持つとき $R(B)$ は

(r1) $R(B) = 2k_B J - BB^T$

と書くことができる．式 (r1) から，$\Gamma' \subset \Gamma$ に対し

(r2) $MM^T = kI + \sum_{i \in \Gamma'} A_i$

となるようなバイナリ行列 M を見つけることにより，本稿で提案するアクセス構造（1）を持つ GVSSS を構成することが可能であることが分かる．

最大距離が 2，頂点数 n のグラフが

(r3) ${A_1}{A_1}^T = kI + \lambda A_1 + \mu A_2$

（ただし $0 < \mu < k < n-1$ とする）

を満たすとき，強正則（Strongly Regular）と呼ぶ．このとき各パラメータ n，k，λ，μ 間には次の関係が成立している[2),15)]．

(r4) $k(k-\lambda-1) = \mu(n-k-1)$.

グラフ P(5) は $(n,k,\lambda,\mu) = (5,2,0,1)$ のパラメータを持つ強正則グラフの例である．以降，式 (r2) と式 (r3) を比較し λ と μ の差を利用して従来型 GVSSS を構成する手法について詳細に述べる．

$Mat\{(A)_a(B)_b\}$ を行列 A を a 回，行列 B を b 回横に並べた行列とする．このとき上式を満たす強正則グラフに対して次が成立する．

(m1) $R(Mat\{(I)_a(1_n)_b\}) = (a+b)J + a(A_1+A_2)$.

(m2) $R(Mat\{(A_1)_1(1_n)_c\}) =$
$(k+c)J + (k-\lambda)A_1 + (k-\mu)A_2$.

ただし 1_n はすべての成分が 1 の $n \times 1$ 行列とする．式 (m1)，(m2) より $\lambda < \mu$ を満たすとき，J の項と A_2 の項の係数が一致するように方程式を解くことにより，$a = k-\mu$，$b = \mu$，$c = 0$ を選択することで従来型 GVSSS が構成できる．さらに，

(m3) $R(Mat\{(A_1+I)_1(1_n)_d\}) =$
$(k+1+d)J + (k-\lambda-1)A_1 + (k-\mu+1)A_2$

と，アダマール行列[3),4)]により構成可能な

(m4) $R(H) = (2p+1)J + (p+1)(A_1+A_2)$

を満たす $4p+3$ 次正方行列 H を用いると，$\mu = \lambda + 1$ が成立する場合にのみアクセス構造（2）を持つ GVSSS が構成できる．このとき $a = p = k-\mu$，$b = a+1$，$d = k-2\mu$，$c = d+1$ を選択すればよい．また，画像拡大率を m とすると相対差は $1/m$ となる．

3.3.3 評　　価

以下の 2 つのアクセス構造（2）を持つ GVSSS の構成方法を相対差の比較により有効性を評価する．

- （既存方式）2.2.1 項のスターグラフ分割法により構成された従来型 GVSSS を用いて 3.3.1 項の生成行列連結法で構成する手法
- （提案方式）3.3.2 項の式 (m3)，(m4) を用いて構成する手法

両方式ともに，画像拡大率を m とすると相対差は $1/m$ で表され，相対差は画像拡大率にのみに依存す

表 1 画像拡大率の比較
Table 1 Comparison of pixel expansions.

グラフ☆	n	k	λ	μ	方式 3.3.1	方式 3.3.2
$L_2(2)$	4	2	0	1	8	7
$P(5)$	5	2	0	1	12	7
$L_2(3)$	9	4	1	2	30	21
Petersen	10	3	0	1	32	23
$P(13)$	13	6	2	3	50	43

る．つまり画像拡大率が小さいほど相対差は大きくなり，よりコントラストを改善することを意味する．

評価対象とするグラフは，頂点数 13 以下のすべての強正則グラフとした．3.3.2 項の手法に適用するためには $\mu = \lambda + 1$ を満たす必要があるが，頂点数が 13 以下の強正則グラフはすべて $\mu = \lambda + 1$ を満たすことが知られている[15]．また，頂点数が 13 を超え，$\mu = \lambda + 1$ を満たす強正則グラフは $P(17)$ などがあげられるが，相対差が現実的ではないため評価対象から除外した．

表 1 は上記の 2 方式を適用したときの画像拡大率を比較したものである．3.3.1 項の生成行列連結法に比べ 3.3.2 項の構成方式は画像拡大率 m を削減していることが分かる．

4. 今後の展開

4.1 提案方式の利用例

VSSS は秘密分散機能を備えた印刷装置への適用ばかりでなく，ユーザの個人認証と同時に（信用できないかもしれない）端末に対する認証が可能[7),10),13)]であり，ヒューマンクリプト[6)]において非常に有効なアプリケーションであると考えられている．

本節では本稿で提案した GVSSS を対面型属性証明に適用した例を示す．各シェア画像は各エンティティに配布され，直接対面を通して互いのシェアを重ねあわせることで相手がどのような属性を保持するか，どのようなグループに属するかを示す用途に用いることができる．このとき従来は同じグループのメンバーかどうかを認識するという目的で利用される方式が想定されるが，本提案の GVSSS を用いることにより各エンティティごとにあるエンティティから見た他エンティティとの関係が異なるという性質を用いて，次のような用途に利用できる．各シェア画像を持つエンティティの年齢がどのくらい離れているかを，グラフ上の 2 エンティティ間の距離で表現しておく．これにより互いの年齢を公開しないで相手の年齢が自分とどのくらい離れているかだけを知る手段に利用できる．

4.2 提案方式の拡張

本稿における GVSSS はさらに次のように拡張可能であると考えられる．

重み付けグラフへの拡張　本稿ではグラフとして無向グラフのみを扱ったが，2 点間の距離を辺の重みに置きかえることで，重み付けグラフを用いる方法への拡張が可能である．

$k \geq 3$ への拡張　本稿では $(2, n)$-VSSS の拡張のみを取り上げたが，$k \geq 3$ においても定義を拡張可能である．その場合 k 個の頂点間のそれぞれの距離から (1) 距離の和，(2) 最小距離，(3) 最大距離を考慮する方式などが考えられる．

5. ま と め

文献 1) で提案されているグラフタイプ視覚復号型秘密分散方式を拡張して，辺の有無ではなく 2 頂点間の距離に基づいたアクセス構造を持つ視覚復号型秘密分散法を提案した．本稿で提案しているスキームの特徴は，複数の機密画像をシェア画像に埋め込むことで，2 枚のシェア画像を重ねあわせたときに，シェア間の距離に応じて復元される機密画像が異なるように構成可能な点にある．特に強正則グラフに対して，よりコントラストを改善した具体的な構成方法を与えた．さらに，このスキームを利用した応用例として対面型属性証明方式について紹介した．

☆ 各グラフの定義を行う．Lattice graph $L_2(m)$ $(m \geq 2)$ は $V = S \times S$（S は位数 m の集合）とし，相異なる直積の元が同じ座標成分を持つときに辺を持つグラフである．Paley graph $P(q)$（q は $q \equiv 1 \pmod 4$ を満たす素数べき）は $V = GF(q)$（位数 q の有限体）とし，相異なる元の差が平方数であるときに辺を持つグラフである．Petersen graph は V を位数 5 の集合における位数 2 の部分集合の集まりとし，相異なる部分集合が互いに素のときに辺を持つグラフである．

参 考 文 献

1) Ateniese, G., Blundo, C., Santis, A.D. and Stinson, D.R.: Visual Cryptography for General Access Structures, *Information and Computation*, Vol.129, pp.86–106 (1996).
2) Brouwer, A.E., Cohen, A.M. and Neumaier, A.: *Distance Regular Graphs*, Springer-Verlag (1989).
3) Bannai, E. and Ito, T.: *Algebraic Combinatorics I: Association Schemes*, Benjamin/Cummings, Menlo Park, CA (1984).
4) Blundo, C., Santis, A.D. and Stinson, D.R.: On the Contrast in Visual Cryptography Schemes, *Journal of Cryptology*, Vol.12, pp.261–289 (1999).
5) Choi, C., Park, J. and Kohno, R.: Con-

trast Analysis According to Hierarchical Access Structure on VCS, *SITA97*, Vol.20, No.1, pp.217–220 (1997).
6) 今井，古原，渡辺：ヒューマンクリプトとは，ISEC 2000-17 (2000).
7) 加藤：視覚復号型秘密分散法とその応用方式の検討，博士論文 (1996).
8) 加藤，今井：視覚復号型秘密分散法の拡張構成方法，電子情報通信学会論文誌（A），Vol.J79-A, No.8, pp.1344–1351 (1996).
9) 加藤，今井：複数の画像を隠すことのできる視覚復号型秘密分散法の個人認証方式への適用，*SITA96*, pp.661–664 (1996).
10) 加藤，今井：覗き見攻撃を考慮した視覚復号型秘密分散法を用いた個人認証方式，*SCIS97*, 25C (1997).
11) Kim, M., Park, J., Park, S. and Kim, K.: A Study on Secret Sharing Scheme Using Visual Cryptography, *SCIS97*, 25B (1997).
12) Kim, M., Shin, S. and Park, J.: New Construction for Multiple Visual Secret Sharing, *SCIS2000*, B44 (2000).
13) Kobara, K. and Imai, H.: Limiting the Visible Space Visual Secret Sharing Schemes and their Application to Human Identification, *ASIACRYPT'96*, pp.185–195 (1996).
14) Koga, H. and Yamamoto, H.: Proposal of a Lattice-Based VSSS for Color and Glay-scale Images, *IEICE Trans. Fundamentals*, Vol.E81-A, No.6, pp.1262–1269 (1998).
15) van Lint, J.H. and Wilson, R.M.: *A Course in Combinatorics*, Cambridge Univ. Press (1992).
16) Naor, M. and Shamir, A.: Visual Cryptography, *EUROCRYPT'94*, pp.1–12 (1994).
17) Naor, M. and Shamir, A.: Visual Cryptography 2, Lecture Notes in Computer Science, Vol.1189, pp.179–202 (1997).
18) Shamir, A.: How to Share a Secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).

(平成 12 年 12 月 1 日受付)
(平成 13 年 6 月 19 日採録)

須賀　祐治（正会員）

平成 7 年九州大学理学部数学科卒業．平成 9 年同大学院数理学研究科数理学専攻修士課程修了．同年財団法人九州システム情報技術研究所第 2 研究室研究員として出向．平成 11 年キヤノン（株）入社．現在，情報セキュリティの研究開発に従事．

岩村　恵市（正会員）

昭和 55 年九州大学工学部情報工学科卒業．昭和 57 年同大学院修士課程修了．同年キヤノン（株）入社．平成 6 年東京大学工学博士．現在，主に符号理論，並列処理，情報セキュリティ，電子透かしの研究に従事．電子情報通信学会，情報理論とその応用学会各会員．

櫻井　幸一（正会員）

昭和 61 年九州大学理学部数学科卒業．昭和 63 年同大学院工学研究科応用物理専攻修了．同年三菱電機（株）入社．現在，九州大学大学院システム情報科学研究院助教授．平成 9 年 9 月より 1 年間コロンビア大学計算機科学科客員として在籍．暗号理論と情報セキュリティの研究に従事．情報処理学会平成 11 年度坂井記念特別賞，平成 11 年度論文賞受賞．「暗号理論の基礎」（平成 8 年共立出版，監訳），「数論アルゴリズムと楕円暗号理論入門」（平成 9 年シュプリンガー東京，訳），工学博士．電子情報通信学会，日本数学会各会員．情報規格調査会 SC27（セキュリティ技術）WG2（暗号技術）国内委員会主査．

今井 秀樹（正会員）

昭和 41 年東京大学工学部電子工学科卒業．昭和 46 年同大学院博士課程修了．工学博士．同年横浜国立大学講師（工学部電気工学科）．昭和 47 年同助教授．昭和 59 年同教授（工学部電子情報工学科）．平成 4 年東京大学教授（生産技術研究所）．郵政省通信総合研究所客員研究官等を兼任．現在に至る．この間，符号理論とその応用，暗号と情報セキュリティ，スペクトル拡散方式，データ圧縮，移動通信等の研究に従事．昭和 50 年度，平成 2 年度電子情報通信学会著述賞，平成 3 年度同論文賞，米澤ファウンダーズ・メダル，平成 6 年度情報通信月間推進協議会情報通信功績賞，電気通信普及財団テレコムシステム技術賞，電子情報通信学会業績賞，平成 10 年 IEEE シャノン 50 周年記念論文賞，平成 11 年韓国順天郷大学名誉博士号等を受賞．著書「符号理論」（昭晃堂），「情報数学」（昭晃堂），「情報と符号の理論」（岩波書店），「情報理論」（昭晃堂），「符号理論」（電子情報通信学会），「暗号のおはなし」（日本規格協会），「明るい暗号の話」（裳華房），「Essentials of Error-Control Coding Techniques」（Academic Press）等．電子情報通信学会理事，監事，電子情報通信学会「基礎・境界ソサイエティ」会長，IEEE 情報理論ソサイエティ理事，国際暗号研究学会（IACR）理事，情報理論とその応用学会会長，日本学術振興会未来開拓学術研究推進事業マルチメディアのための高度情報セキュリティ技術研究プロジェクトリーダー等を歴任．IEEE Fellow．