組合せデザインを用いた視覚復号型秘密分散法

東京理科大学 創域理工学部 情報計算科学科 教授 宮本（みやもと） 暢子（のぶこ）

はじめに

デジタル化が進む現代社会において，情報の保護やセキュリティはより重要な課題となっています．個人情報，機密データ，著作権保護など様々な分野で情報漏洩のリスクが存在します．これらのリスクに対処するためには，高度な暗号技術やセキュリティ対策が求められますが，これらの対策が複雑であることも少なくありません．秘密分散法（Secret Sharing Scheme）は，1979 年に Adleman，Blakley，Shamir らによって提案された，秘密情報を複数のシェアに分割し，一定数のシェアが揃うことで元の情報を復元できるようにする方法です．特に，クラウドサーバーやデジタルストレージの利用が拡大する中で，秘密分散法は，信頼性とセキュリティを兼ね備えたデータの保護手段として広く利用されています．本稿では，秘密の画像を複数のシェアに分割し，複雑な計算をすることなく物理的に重ね合わせることで元の画像を復元する視覚復号型秘密分散法（Visual Cryptography Scheme，VCS）について紹介します．

VCS の仕組み

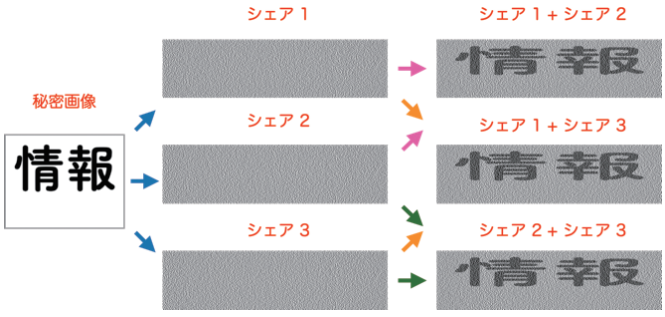
VCS の基本的なアイデアは 1994 年に Naor と Shamir によって提案されました．まず例をみてみましょう．**【図 1】**は「情報」と黒文字で書かれた秘密画像を 3 つのシェアに分割し，各シェアを OHP シートのような透明なシートに印刷したとき，そのうちの 2 枚を物理的に重ね合わせると元画像が復元される仕組みを表しています．このように白黒の秘密画像を n 個のシェアに分割し，そのうちの任意の k 個が集まれば復元できる方法を (k,n)-VCS といいます．これを実現するため，元の秘密画像の各ピクセルを白と黒の特定のパターンに基づいて拡張します．**【図 2】**は $(2,2)$-VCS で用いる一つのパターンを表しています．白（黒）ピクセルを 2 倍に拡張し，シェア 1 とシェア 2 にそれぞれ分けます．2 つのシェアを重ね合わせたとき，白の場合は 2 個のうち 1 つが黒，黒の場合は 2 つとも黒のようになり，この白と黒のギャップで元の画像が復元されます．ただし，1 つのシェアを見ただけでは，元が白と黒のどちらのピクセルであったかは判断できません．例では 1 ピクセルを 2 倍に拡張しましたが，シェア数を増やすためには拡張数も増やす必要があります．

白（黒）ピクセルの拡張パターンを表すために基底行列と呼ばれる行列 $M_0(M_1)$ を用います．黒を “1”，白を “0” で表現すると，【図 2】は

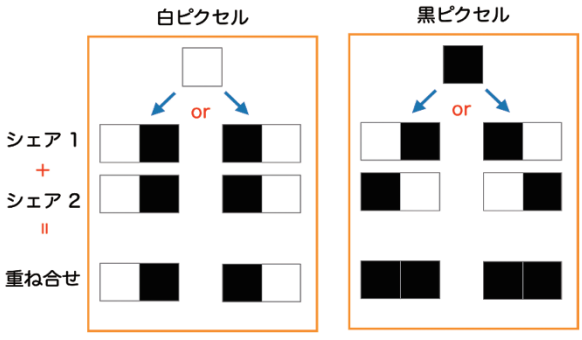
$$M_0 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

と表され，各行がシェアに対応します．拡張するシェアのパターンが規則性をもたないように，ピクセルごとに基底行列をランダムに列置換して用います．

$(2,n)$-VCS において $n \times m$ の基底行列 $M_0(M_1)$ が満たすべき条件を考えます．行列 M_h の第 i 行目を $M_h[i](i=1,\ldots,n,h=0,1)$，2 進ベクトル x のハミング重み（x に含まれる 1 の個数）を $w(x)$ と表します．各シェアからいかなる情報も漏れないためには，



【図 1】(2,3)-VCS



【図 2】(2,2)-VCS のピクセルの拡張例

$$w(M_0[i])=w(M_1[i])\quad(i=1,\ldots,n)$$

である必要があります．さらに 2 個のシェアの重ね合わせは，ビットごとの論理和（or）を

$$w(M_h[i]\mathrm{or}M_h[j])\quad(i,j=1,\ldots,n,i\neq j)$$

で表すと，重ね合わせたときの白と黒の明度に差が生じるためには少なくとも

$$w(M_1[i]\mathrm{or}M_1[j])\geq w(M_0[i]\mathrm{or}M_0[j])+1$$

である必要があります．ピクセル拡張数 m に対する白と黒の明度の差を相対コントラスト γ といい，γ はすべての $i,j=1,\ldots,n,i\neq j$ に対して

$$\frac{w(M_1[i]\mathrm{or}M_1[j])-w(M_0[i]\mathrm{or}M_0[j])}{m}\geq\gamma$$

を満たすものとして定義されます．【図 2】の (2,2)-VCS の相対コントラストは，$\gamma=1/2$ となります．

最適コントラストをもつ (2,*n*)-VCS の構成

(2,n)-VCS の相対コントラスト γ には，次の上限が存在し，上限値に達するとき最適コントラストをもつといいます．

$$\gamma\leq\frac{\lceil\frac{n}{2}\rceil\lfloor\frac{n}{2}\rfloor}{n(n-1)}$$

ただし，$\lceil x\rceil$ は x 以上の最小の整数，$\lfloor x\rfloor$ は x 以下の最大の整数を表すものとします．実際，シェア数 n に対する最適コントラスト γ^* は次のようになります．

$$\gamma^*(n)=\begin{cases}\dfrac{n}{4(n-1)} & (n\text{ が偶数の場合})\\ \dfrac{n+1}{4n} & (n\text{ が奇数の場合})\end{cases}$$

【例 1】 ピクセル拡張数 $m=3$，最適コントラスト $\gamma^*=1/3$ である (2,3)-VCS の基底行列

$$M_0=\begin{pmatrix}1&0&0\\1&0&0\\1&0&0\end{pmatrix},M_1=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

【例 2】 ピクセル拡張数 $m=6$，最適コントラスト $\gamma^*=1/3$ である (2,4)-VCS の基底行列

$$M_0=\begin{pmatrix}1&1&1&0&0&0\\1&1&1&0&0&0\\1&1&1&0&0&0\\1&1&1&0&0&0\end{pmatrix}$$

$$M_1=\begin{pmatrix}1&1&1&0&0&0\\1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&0&1&1\end{pmatrix}$$

基底行列を整数計画法で求める方法もありますが，ここでは，BIBD（balanced incomplete block design）と呼ばれる組合せデザインを用いて求める方法について解説します．

X を v 個の要素（点と呼ぶ）からなる集合，$\mathcal{B}$ を X の部分集合（ブロックと呼ぶ）の集まりとし，ペア $(X,\mathcal{B})$ が次の 2 つの条件を満たすとき，(v,k,λ)-BIBD といいます．

(1) どのブロックも k 個の点を含む

(2) 異なる 2 点を含むブロックはちょうど λ 個存在する

このとき，各点はちょうど $r=\lambda(v-1)/(k-1)$ 個のブロックに含まれ，ブロックの総数は $b=vr/k=\lambda(v^2-v)/(k^2-k)$ となります．また，BIBD のブロックのサイズに関する条件（1）を緩和し，条件（2）のみを課した構造を (v,K,λ)-PBD（pairwise balanced design）といいます．ただし，K はブロックのサイズの集合を表します．組合せデザインは，$v\times b$ の (0,1)-行列 $H=(h_{x,B})$（結合行列と呼ぶ）で表すこともできます．ただし，$x\in X,B\in\mathcal{B}$ に対して

$$h_{x,B}=\begin{cases}1\ (x\in B\text{ の場合})\\ 0\ (x\notin B\text{ の場合})\end{cases}$$

とします．また各ブロック $B\in\mathcal{B}$ に対してその補集合を集めたものを

$$\mathcal{A}=\{X\setminus B:B\in\mathcal{B}\}$$

とすると，$(X,\mathcal{A})$ は，$(v,v-k,b-2r+\lambda)$-BIBD となり補デザインと呼ばれます．また $b=v$ の対称型 BIBD において任意の $B_0\in\mathcal{B}$ に対して，

$$(B_0,\{B\cap B_0:B\in\mathcal{B},B\neq B_0\})$$

は，$(k,\lambda,\lambda-1)$-BIBD となり派生デザインと呼ばれます．さらに，

$$(X\setminus B_0,\{B\setminus B_0:B\in\mathcal{B},B\neq B_0\})$$

は，$(v-k,k-\lambda,\lambda)$-BIBD となり剰余デザインと呼ばれます．

【例 3】 (11,5,2)-BIBD$(X,\mathcal{B})$ とその結合行列

$$X=\{0,1,\ldots,10\}=\mathbb{Z}_{11}$$

$$\mathcal{B}=\{\{0,2,3,4,8\}+i(\mathrm{mod}\ 11),i\in X\}$$

$$H=\begin{pmatrix}1&0&0&1&0&0&0&1&1&1&0\\0&1&0&0&1&0&0&0&1&1&1\\1&0&1&0&0&1&0&0&0&1&1\\1&1&0&1&0&0&1&0&0&0&1\\1&1&1&0&1&0&0&1&0&0&0\\0&1&1&1&0&1&0&0&1&0&0\\0&0&1&1&1&0&1&0&0&1&0\\0&0&0&1&1&1&0&1&0&0&1\\1&0&0&0&1&1&1&0&1&0&0\\0&1&0&0&0&1&1&1&0&1&0\\0&0&1&0&0&0&1&1&1&0&1\end{pmatrix}$$

【例 4】(11,5,2)-BIBD の補デザイン，派生デザイン，剰余デザイン

補デザイン (11,6,3)-BIBD　$(X,\mathcal{A})$
$\mathcal{A}=\{\{1,5,6,7,9,10\}+i(\mathrm{mod}\ 11), i\in X\}$

派生デザイン (5,2,1)-BIBD　$(B_0,\mathcal{A}')$
$B_0=\{0,2,3,4,8\}$
$\mathcal{A}'=\{\{3,4\},\{2,4\},\{0,3\},\{4,8\},\{2,8\},$
$\{3,8\},\{0,4\},\{0,8\},\{0,2\},\{2,3\}\}$

剰余デザイン (6,3,2)-BIBD　$(X\setminus B_0,\mathcal{A}'')$
$X\setminus B_0=\{1,5,6,7,9,10\}$
$\mathcal{A}''=\{\{1,5,9\},\{5,6,10\},\{5,6,7\},\{1,6,7\},\{5,7,9\},$
$\{6,9,10\},\{7,9,10\},\{1,5,10\},\{1,6,9\},\{1,7,10\}\}$

(n,k,λ)-BIBD が存在すると仮定します．黒の基底行列 M_1 を BIBD の $n\times b$ の結合行列，白の基底行列 M_0 を 1 の個数が r 個，残りが 0 の同一の行ベクトルが並んだものと考えます．このとき，次のように最適コントラストをもつピクセル拡張数 m の $(2,n)$-VCS を構成することができます．

【構成法 1】（n が偶数の場合）
$(n,n/2,n/2-1)$-BIBD が存在すれば，ピクセル拡張数 $m=2n-2$ の最適コントラストをもつ $(2,n)$-VCS を構成できる．

【例 5】 例 4 の剰余デザイン (6,3,2)-BIBD を用いた $m=10,\gamma^*=3/10$ の (2,6)-VCS の構成．ただし，基底行列は次のように与えられる．

$$M_0=\begin{pmatrix}1&1&1&1&1&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0\end{pmatrix}$$

$$M_1=\begin{pmatrix}1&0&0&1&0&0&0&1&1&1\\1&1&1&0&1&0&0&1&0&0\\0&1&1&1&0&1&0&0&1&0\\0&0&1&1&1&0&1&0&0&1\\1&0&0&0&1&1&1&0&1&0\\0&1&0&0&0&1&1&1&0&1\end{pmatrix}$$

【構成法 2】（$n\equiv 3(\mathrm{mod}\ 4)$ の場合）
$(n,(n-1)/2,(n-3)/4)$-BIBD が存在すれば，ピクセル拡張数 $m=n$ の最適コントラストをもつ $(2,n)$-VCS を構成できる．

【例 6】 例 3 の (11,5,2)-BIBD を用いた $m=11,\gamma^*=3/11$ の (2,11)-VCS の構成

【構成法 3】（$n\equiv 1(\mathrm{mod}\ 4)$ の場合）
$(n,(n-1)/2,(n-3)/2)$-BIBD が存在すれば，ピクセル拡張数 $m=2n$ の最適コントラストをもつ $(2,n)$-VCS を構成できる．

【例 7】 例 4 の派生デザイン (5,2,1)-BIBD を用いた $m=10,\gamma^*=3/10$ の (2,5)-VCS の構成

位数 n のアダマール行列とは，$HH^T=nI_n$（I_n は n 次の単位行列）を満たす成分が ± 1 の行列 H をいいます．n が 4 の倍数のとき，アダマール行列が存在するというアダマール予想は未解決問題ですが，$4t-1$ が素数の場合や，$2t-1$ が素数かつ t が奇数の場合は，位数 $4t$ のアダマール行列が存在することなど多くの結果が知られています．構成法 1 から 3 で用いた BIBD はいずれもアダマール行列と関連しています．位数 $4t$ のアダマール行列の存在が仮定されると，$(4t-1,2t-1,t-1)$-BIBD（構成法 2）やその剰余デザイン $(2t,t,t-1)$-BIBD が存在します（構成法 1）．また位数 $8t+4$ のアダマール行列の存在が仮定されると，$(8t+3,4t+1,2t)$-BIBD やその派生デザイン $(4t+1,2t,2t-1)$-BIBD が存在します（構成法 3）．

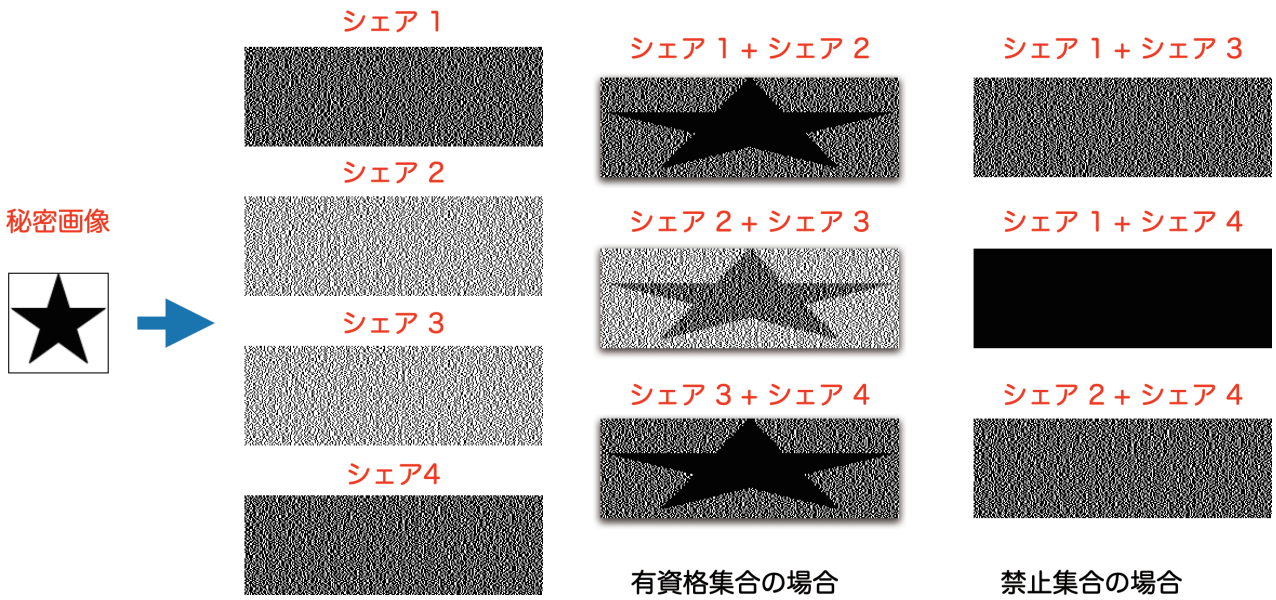
(k,n)-VCS についても $k=2$ の場合と同様に，組合せデザインや直交配列を用いた構成法や，重ね合わせる枚数によって黒白の明度の差があるプログレッシブ型などが研究されています．

アクセス構造型 VCS

(k,n)-VCS は，秘密画像を n 個のシェアに分割し，そのうちの任意の k 個が集まれば復元できるというしきい値型の方法でしたが，特定のシェアの組合せのみが復元できるというアクセス構造型秘密分散法と呼ばれる方法があります．まずアクセス構造について説明します．$\mathcal{P}=\{1,2,\ldots,n\}$ を参加者の集合，$2^{\mathcal{P}}$ を $\mathcal{P}$ のべき集合とします．$\Gamma_{Qual}\subseteq 2^{\mathcal{P}}$ をシェアから秘密画像を復元できる参加者集合の集合（有資格集合），$\Gamma_{Forb}\subseteq 2^{\mathcal{P}}$ をシェアから一切の情報を得られない参加者集合の集合（禁止集合）とおくとき，$(\Gamma_{Qual},\Gamma_{Forb})$ をアクセス構造といいます．Γ_{Qual} に単調増加性

$$A\in\Gamma_{Qual},\ A\subset B\Rightarrow B\in\Gamma_{Qual}$$

を，Γ_{Forb} に単調減少性



【図 3】例 8 のアクセス構造型 VCS

$$A\in\Gamma_{Forb},\ B\subset A \Rightarrow B\in\Gamma_{Forb}$$

をさらに

$$\Gamma_{Qual}\cup\Gamma_{Forb}=2^{\mathcal{P}}$$

である $(\Gamma_{Qual},\Gamma_{Forb})$ を強アクセス構造といいます．
また

$$\Gamma_0=\{A\in\Gamma_{Qual}:B\notin\Gamma_{Qual}\ for\ all\ B\subseteq A,B\neq A\}$$

を極小有資格集合といい，$\Gamma_0=\Gamma_{Qual}$ である $(\Gamma_{Qual},\Gamma_{Forb})$ を弱アクセス構造といいます．

アクセス構造型 VCS を実現するためには，白と黒の各ピクセルを拡張するための基底行列が次の 2 つの条件を満たす必要があります．

(1) すべての $S\in\Gamma_{Qual}$ に対して，

$$w(OR(M_0[S]))+\alpha\cdot m=w(OR(M_1[S]))$$

を満たすある定数 $\alpha>0$ が存在する．ただし，$M_h[S]$ は M_h の行を S に制限して得られる行列であり，OR は列ごとの論理和（or）をとる操作を表すものとする．

(2) すべての $S\in\Gamma_{Forb}$ に対して，$M_0[S]$ と $M_1[S]$ は適当な列置換により等しくできる．

【例 8】 $n=4,\mathcal{P}=\{1,2,3,4\}$

$$\Gamma_{Qual}=\{\{1,2\},\{2,3\},\{3,4\},\{1,2,3\}\},$$
$$\Gamma_{Forb}=\{\{1\},\{2\},\{3\},\{4\},\{1,3\},\{1,4\},\{2,4\}\}$$

とする．このとき，$\Gamma_0=\{\{1,2\},\{2,3\},\{3,4\}\}$ である．またアクセス構造 $(\Gamma_{Qual},\Gamma_{Forb})$ の VCS を実現するための基底行列は，

$$M_0=\begin{pmatrix}1&0&1\\1&0&0\\1&0&0\\1&1&0\end{pmatrix},\ M_1=\begin{pmatrix}0&1&1\\1&0&0\\0&0&1\\1&1&0\end{pmatrix}$$

であり，$\alpha=1/3$ となる．【図 3】をみると Γ_{Forb} の要素では何も情報が得られないことが分かります．

アクセス構造型 VCS は，(n,n)-VCS の基底行列を適切に配置することで実現する方法が一般的ですが，BIBD とは異なる制約条件をもつ GDD（group divisible design）や nested BIBD といった組合せデザインを用いることで様々なタイプのアクセス構造型 VCS を与えることができます．

さいごに

本稿で紹介した VCS 以外にも，シェア単体でも何らかの意味のある画像となるように元画像を分散させる拡張 VCS，複数の秘密画像やカラー画像に対応した VCS もあります．筆者は，代数や有限射影幾何を用いた組合せデザインの構成問題，符号・暗号理論や多重通信などへの組合せデザインの応用を研究してきました．現在は深層学習への応用についての研究も進めています．

[参考文献]

- Ateniese et al.,“Visual cryptography for general access structures.” *Information and computation* 129.2 (1996) : 86–106.
- Blundo et al.,.“On the contrast in visual cryptography schemes.” *Journal of Cryptology* 12.4 (1999) : 261–289.