

ボトムアップ型視覚暗号の 数理計画法による構成

渡辺 宏太郎, 大塚 志成, 丹羽 弘樹

視覚暗号, Visual Cryptography Sharing Schemes (VCSS) は 1994 年に Naor と Shamir により提案されたデジタル画像に対する秘密分散法の一つである. ある秘密情報に対してこれを画像化し, 複数枚の画像として分散する. 秘密情報の復元は, 特別な装置を必要とせず, 分散された画像を重ねていくことによりなされる. 本稿では, 秘密を分散する画像の構成に数理計画法を用いる方法を紹介する.

キーワード: 視覚暗号, 秘密分散法, 数理計画法

1. はじめに

視覚暗号は Naor and Shamir [1] による創始以来, カラー画像への適用 [2], 連続諧調画像の拡張視覚暗号化 (秘密画像を分散した画像自体も自然画像となる) [3] など, さまざまな拡張がなされてきている. 本稿では, 最も基本的な秘密画像とその秘密分散化画像が共に 2 値の場合, そして, その構成法も数理計画法を用いた場合に限って報告したい¹.

2. 秘密分散共有法

ある秘密を紛失から守るためには, そのコピーをたくさん作って複数の場所に保管しておくといよい. しかし, これでは秘密の漏えいの危険性も増す. そこで, 秘密をいくつかの場所に分散しても, それ自体からは秘密の漏えいがない, そしていくつかの分散情報の保管場所が利用不可能となっても元の秘密が復元できるという性質をもつ手法があれば, 都合がよい. (t, n) 閾値秘密分散法とは, 次の性質を満たす, ある秘密情報を n 個の情報 (シェアと呼ばれる) $s_1, \dots, s_n$ に分散する方法である.

- (1) $s_1, \dots, s_n$ のうち, 任意の t 個のシェアから秘密が復元できる.
- (2) しかし, $t-1$ 個以下のシェアからは秘密について何もわからない.

紛失については $n-t$ 個までを許し, 情報の漏えいについては $t-1$ 個までは守られるので, おおもとの要求を満たしていることがわかる. 秘密情報が, ある整数であるならば, 黒澤 [4] (p. 136) のようにラグランジュ補間を用いて (t, n) 閾値秘密分散法を実現できる.

2.1 視覚暗号

視覚暗号 (Visual Cryptography Sharing Schemes, VCSS) は, 1994 年に Naor と Shamir により提案された (t, n) 閾値秘密分散法である [1]. この方法はシェアからの秘密情報の復元法に特徴をもつ. この方法の場合, 秘密情報もシェアも画像となる. 通常, n 枚のシェアは透過性のあるシート (OHP シート!) に印刷され, これらのシェアを重ね合わせることで秘密の復元がなされる. このことからわかるように, 特別な装置を必要としないので, 復元に何らかの不正が入り込むことを避けることができる.

具体例で示そう. $(t, n) = (2, 2)$ の場合を考える. 秘密画像は 2 値画像である.

$$X_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad X_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (1)$$

X_0 は秘密画像の値 “0” (白色) に対する符号化に用いる行列, X_1 は秘密画像の値 “1” (黒色) に対する符号化に用いる行列である. また, それぞれの行列の第 1 行はシェア 1 に対する符号化, 第 2 行はシェア 2 に対する符号化となる. したがって秘密画像のあるピクセルが 0 だったときは, シェア 1, シェア 2 とも $(1, 0)$ を配布, 秘密画像のあるピクセルが 1 だったときはシェア 1 には $(1, 0)$, 一方シェア 2 には $(0, 1)$ を配布する. シェア 1, シェア 2 単独では 1 と 0 の個

¹ 包括的な報告は, 筆者の力量ではできないため, ご容赦ください.

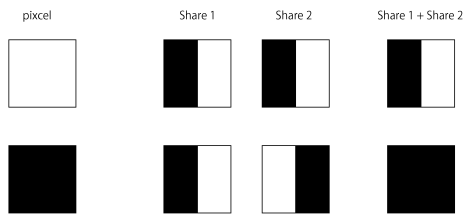


図 1 $(t, n) = (2, 2)$ の場合の各シェアとその重ね合わせ

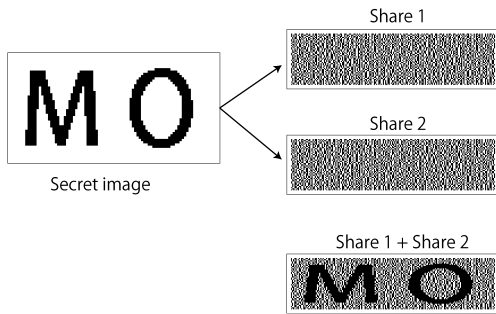


図 2 $(t, n) = (2, 2)$ の場合の具体例

数が同数だから、秘密画像のピクセルについて何の情報も得ていないことを注意する。図 1 からわかるようにシェア 1 とシェア 2 を重ねたとき、秘密画像のピクセルが“1”だったときは、“0”のときに比べて黒がはっきりとする。画像全体では図 2 のようになる。以上のように比較的簡単に $(t, n) = (2, 2)$ の場合は秘密分散することができる。ただし、次のことに注意する必要がある。図 2 の各シェアの作成の際には、式 (1) と式 (1) の第 1 列と第 2 列を交換した行列

$$X'_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \quad X'_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (2)$$

をランダムに選ばなくてはならない。仮に式 (1) の符号化ばかりを用いると、図 3 のように、シェア 1 とシェア 2 を重ねなくてもシェア 2 だけから秘密が漏えいしてしまう。 $(t, n) = (2, 2)$ の場合には行列 X_0 と X_1 は周知だから、それらの列の交換の順序が漏えいすると秘密を守ることはできないということに注意が必要である。

3. 最適な視覚暗号

次に $n \geq 3$ の場合の VCSS を考える。 $G = \{1, 2, \dots, n\}$ をシェアのインデックスとする。 $n = 2$ の場合と同様、秘密画像のピクセル値 0 用の符号化行列 X_0 と 1 用の行列 X_1 を用意する。

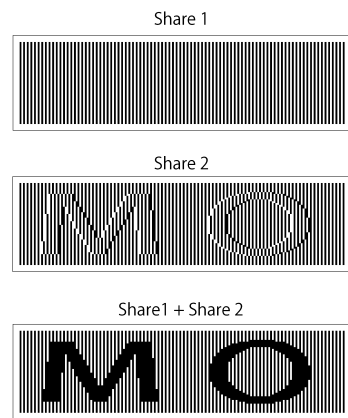


図 3 $(t, n) = (2, 2)$ の場合の失敗例

定義 1. $n \times m$ のブール (バイナリ) 行列 X_0, X_1 が次の条件を満たすとき、 X_0, X_1 は (t, n) -VCSS の基本行列という。

- (1) 正の定数 α が存在して、任意の $|S| = t$ を満たす $S \subset G$ に対して

$$h(X_0[S]) + \alpha m \leq h(X_1[S]). \quad (3)$$

ここで $h(X_i[S])$ ($i = 0, 1$) は X_i を S に制限した行列の各行の論理 OR をとった結果のハミング重みである。

- (2) 任意の $|S| \leq t - 1$ を満たす $S \subset G$ に対しては

$$h(X_0[S]) = h(X_1[S]) \quad (4)$$

が成立する。

条件 (2) は $t - 1$ 枚以下のシェアの重ね合わせでは、秘密画像の“0”に対する符号化と“1”に対する符号化で濃淡に差がないことを表す。一方、条件 (1) は、どのような t 枚のシェアを重ねても濃淡の差が、秘密画像の“0”、“1”に対応して最低 $m\alpha$ は出ることを意味する。上記の α は相対差と呼ばれる。より正確には

$$\alpha := \min_{S \subset G: |S|=t} \frac{h(X_1[S]) - h(X_0[S])}{m} \quad (5)$$

とかけることを注意する。

$$X_0 = \begin{bmatrix} 00000000000000011100001110 \\ 00000000000000011010100011 \\ 00000000000000001100010011 \\ 00000000000000010101110010 \\ 0000000000000001101101001 \\ 00000000000000011011011001 \\ 0000000000000000111000111 \\ 00000000000000000111111 \end{bmatrix} \quad (6)$$

$$X_1 = \begin{bmatrix} 1110000000000000000000111 \\ 00011000000000010000000111 \\ 0000011000000000000000111 \\ 0000000111000000000000111 \\ 0000000000110001000000111 \\ 0000000000001111000000111 \\ 0000000000000000111000111 \\ 000000000000000000111111 \end{bmatrix} \quad (7)$$

m は、秘密画像の 1 ピクセルを m ピクセルに置き換えることを意味し、画素拡大 (pixel expansion) と呼ばれている。上記の X_0 と X_1 は $m = 25$ の $(t, n) = (3, 8)$ の VCSS を与える。 $S = \{1, 2\}$ としよう。このとき、 $h(X_0[S]) = 9, h(X_1[S]) = 9$ が成り立ち、条件 (2) が成立している。一方、 $S = \{1, 2, 3\}$ とすると、 $h(X_0[S]) = 10, h(X_1[S]) = 11$ となり、わずかながら秘密画像のピクセルごとの符号化に濃淡差が生じる。 $(t, n) = (2, 2)$ の場合で述べたようにこの場合も、秘密画像のピクセルごとの符号化を行うたびにランダムに X_0 と X_1 の列の置換を行う必要がある。

式 (5) は、シェア t 枚を重ねたときの濃淡差の最小値を表したが、 t 枚以上のシェアを重ねたときの濃淡差を考える場合もある [5]。 l ($l \geq t$) 枚のシェアを重ねたときの濃淡差の最小値を α_l で表す。すなわち、

$$\alpha_l := \min_{S \subset G: |S|=l} \frac{h(X_1[S]) - h(X_0[S])}{m} \quad (8)$$

とする。 α_{t+1} から α_{n-1} までの個々の相対差の最大化について理論的な結果を得ることは難しそうであるが、 α_t, α_n の最大化については、結果が得られている。

3.1 最適な α_t

α_t の最大化については次が得られている。

(i) (n, n) -VCSS のとき [1] :

$$\alpha_t = \frac{1}{2^{n-1}}.$$

(ii) $(n-1, n)$ -VCSS のとき [6] :

$$\alpha_t = \begin{cases} \left(\frac{n}{4} \binom{n}{n/2}\right)^{-1} & \text{if } n \text{ is even} \\ \left(\frac{n}{2} \binom{n-1}{(n-1)/2}\right)^{-1} & \text{if } n \text{ is odd.} \end{cases}$$

(iii) $(2, n)$ -VCSS のとき [1] :

$$\alpha_t = \frac{n}{4(n-1)}.$$

(iv) $(3, n)$ -VCSS, ただし $n \equiv 0 \pmod{4}$ のとき [7] :

$$\alpha_t = \frac{n^2}{16(n-1)(n-2)}.$$

Hofmeister et al. [7], また Blundo et al. [6] は相対差 α_t の最大化を数理計画法で定式化して求めている (Case (i), (ii) の場合も扱っている)。この際、キーとなるのは、符号化行列 X_0 と X_1 の各列のハミング重みが等しいならば、その出現頻度も等しい (totally symmetric と呼んでいる) 行列に限ってよいという事実である。これにより、符号化行列の列数 m は非常に大きくなるが、 α_t の最大値を表現する際には都合がよい。

上記の数理計画法を用いた、 α_t の最大値の表現では、たとえば Case (iii) の場合、符号化行列の列サイズは、 n が偶数のとき $m = \binom{n}{n/2}$ といった非常に大きな値となってしまふ。(高解像度のプリンタを使用すれば、符号化行列の列サイズが大きくなっても各シェアの印刷はできるのかもしれないが、 t 枚を重ねたときの位置合わせが難しいので、 m はできれば小さい値に抑えたい。)

最適な α_t を達成するためには、 m は大きくならざるを得ないのであろうか? このことは、必ずしも正しくはない。実際、Hofmeister et al. [7] の Theorem 5 は Hadamard 行列を用いて $n = 2^k, k \geq 1$ の場合には、 $m = 2n - 2$ で Case (iii) の α_t が達成されることを示している。議論中、最適性を示す部分では、符号理論における Plotkin 限界式を用いており、これも興味深いのではなからうか。

文献 [7] や文献 [6] は数理計画法を用いる方法であったが、これとは異なるアプローチとして Koga [8] がある。Koga [8] では (t, n) -VCSS にある線型偏微分方程式の多項式解を対応させ、構成する。次の行列を考えよう。

$$M_3(0,0,1) = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

これは列ベクトル $[0, 0, 1]^\top$ ($\top$ は転置を表す) に $3!$ 個の成分の置換を施してできる列ベクトルをすべて並べた行列となっている. 各列は 2 個の 0 と 1 個の 1 で構成されているからこの行列に単項式 a^2z を対応させる. (一般には k 個の 1 と $n-k$ の 0 から成る列ベクトルの $n!$ 個の成分の置換を行ってできる列ベクトルすべてを並べた $n \times n!$ 行列に単項式 $a^{n-k}z^k$ を対応させる.) この単項式に微分作用素

$$D := \frac{\partial}{\partial a} + \frac{\partial}{\partial z}$$

を作用させてみると $D(a^2z) = 2az + a^2$ となる. これを $[0, 0]^\top$ の 2 成分を置換したものと二つの $[0, 1]^\top$ の 2 成分を置換したものの接続と解釈すると対応する行列は

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

となり, $M_3(0,0,1)$ の第 3 行を削除した行列になっている. すなわち D を多項式へ作用させることは, 対応する行列の 1 行を削除することに相当する. 今, X_1 に対応する多項式を $f^+(a, z)$, X_0 に対応する多項式を $f^-(a, z)$ としよう. X_1, X_0 が (t, n) -VCSS を実現するならば, それらを $n-t+1$ 行以上削除して得られる行列には差異がないが, ちょうど $n-t$ 行削除して得られる行列には全零列の個数に差異が生じるはずである. すなわち

$$\begin{cases} D^{(n-t+1)}(f^+)(a, b) = D^{(n-t+1)}(f^-)(a, b) \\ D^{(n-t)}(f^+)(a, b) = D^{(n-t)}(f^-)(a, b) + Ca^t \end{cases} \quad (9)$$

が成り立つ. ここで C は正整数. 文献 [8] は方程式 (9) の解を用いて Case (i), (ii), (iii) の α_t の値を求めている. 視覚暗号の構成に偏微分方程式が利用できるという点が大変興味深く思われる.

3.2 最適な α_n

この節では Iwamoto [9], Shyu and Chen [10], Okada and Koga [11] に従って最適な α_n を数理計画法により求めてみよう (定式化は文献 [1, 2] と異なる). その前にプログレッシブ型 VCSS (PVCSS) の定義をしておく.

定義 2. (X_0, X_1) を (t, n) -VCSS の符号化行列とする. このとき

$$\alpha_t < \alpha_{t+1} < \cdots < \alpha_n \quad (10)$$

が満たされるならば, VCSS はプログレッシブ型 VCSS (PVCSS) であるという.

定式化のためにいくつか記号を導入する. $D \subset G$ に対して次の列ベクトル E_D を定義する.

$$E_D := [b_1, b_2, \dots, b_n]^\top, \quad b_i = \begin{cases} 1, & \text{if } i \in D \\ 0, & \text{else.} \end{cases}$$

また, $D \subset G$ に対して, 関数 $f: 2^G \rightarrow \{0, 1, \dots, 2^n - 1\}$ を

$$f(D) := \begin{cases} 0, & \text{if } D = \emptyset, \\ \sum_{i \in D} 2^{i-1} \end{cases}$$

と定義する. 符号化行列 X_i に現れる列 E_D の出現回数を $x_{f(D)}^i$ で表す. i 番目のシェアを考える. $i \in D$ ならば, シェア i が重ねられたとき, E_D に対応する画素は値 1 (黒) となり, そうでないときは, 0 (白) となる. したがって, 重ね合わせるシェアの集合を $S \subset G$ としたとき, $S \cap D \neq \emptyset$ ならば, E_D に対応する画素は値 1 となり, $S \cap D = \emptyset$ ならば, 0 となる. α_n の最大値を得るため, 次の線形計画問題を考える.

maximize: (11)

$$\frac{1}{M} \left(\sum_{S \subset G: S \cap G \neq \emptyset} (y_{f(S)}^1 - y_{f(S)}^0) \right)$$

subject to:

$$\begin{aligned} y_{f(S)}^i &\in \mathbb{R}, y_{f(S)}^i \geq 0, i \in \{0, 1\}, S \subset G, \\ \sum_{S \subset G} y_{f(S)}^1 &= \sum_{S \subset G} y_{f(S)}^0 = M, \\ \sum_{S \subset G: S \cap D \neq \emptyset} (y_{f(S)}^1 - y_{f(S)}^0) &= 0, \end{aligned}$$

$$\begin{aligned} D \subset G: |D| < t, \\ 1 + \sum_{S \subset G: S \cap D \neq \emptyset} y_{f(S)}^0 &\leq \sum_{S \subset G: S \cap D \neq \emptyset} y_{f(S)}^1, \\ D \subset G: |D| \geq t \end{aligned}$$

ここで M は 2 以上の整数である. 式 (11) の解は明らかに有理数で表される. したがって $\{y_{f(S)}^i\}$ ($i \in \{0, 1\}$) たちの分母の最小公倍数 d をとって $\{y_{f(S)}^i\}$ たちにかけてやれば, α_n を最大化する VCSS が実現されることになる. この際, 画素拡大のサイズは dM になって

しまうが, α_n の最大値を求めるという観点では式 (11) を解けば十分ということになる. 後で式 (11) を数値計画ソルバー (Gurobi5.0) を用いて α_n の値を具体的に求めるが, その出力は実数型のため, Mathematica などの数式処理システムを用いて有理数表現にする必要がある (画素拡大が小さい場合は, 数式処理システムで直接扱ったほうがよいかもしれない).

画素拡大は, やはり小さいほうが望ましいので, α_n の最大値を達成する画素拡大のうち最小のものを求めることにする. 文献 [11] に従い, 次の整数計画問題を解けばよい. α_n は式 (11) で得られた値とする.

$$\begin{aligned} & \text{minimize:} \\ & \sum_{S \subset G} x_{f(S)}^0 \\ & \text{subject to:} \\ & x_{f(S)}^i \in \mathbb{Z}, x_{f(S)}^i \geq 0, i \in \{0, 1\}, S \subset G, \\ & \sum_{S \subset G} x_{f(S)}^1 = \sum_{S \subset G} x_{f(S)}^0 \\ & \sum_{S \subset G: S \cap D \neq \emptyset} (x_{f(S)}^1 - x_{f(S)}^0) = 0, \\ & D \subset G: |D| < t, \\ & 1 + \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^0 \leq \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^1, \\ & D \subset G: |D| \geq t, \\ & \sum_{S \subset G: S \cap D \neq \emptyset} (x_{f(S)}^1 - x_{f(S)}^0) = \alpha_n \sum_{S \subset G} x_{f(S)}^0. \end{aligned} \quad (12)$$

最後の拘束条件は, α_n の分母を両辺にかけた形で実際は適用するが, わかりやすさの点から上記の記述とした. $|D| < t$ の場合の拘束条件は $t-1$ 以下のシェアの重ね合わせでは, 秘密画像のピクセル 1 の符号化と 0 の符号化で濃淡に差が出ないことを表している. $|D| \geq t$ の場合の拘束条件は, t 枚以上のシェアの重ね合わせで上記の差が生じることを意味する.

表 1 は, 式 (11) を各 (t, n) について実行した結果である (文献 [10] の表 1 も参照のこと). 表 2 は, 表 1 を実現する画素拡大の最小値を式 (12) で求めたものである. 表 2 より n が大きくかつ t も大きな値をとるとき, 画素拡大はかなり大きな値になってしまう (たとえば, $(t, n) = (7, 10)$ のとき, 画素拡大の最小値は $m = 1155$ にもなってしまふ. 一方, $t \leq 3$ のときは, n が大きくても画素拡大は急激な増大とはならないことがわかる. そこで, (t, n) で t が 4 以下の範囲で α_t , α_n の最大化を考える. ただし, 画素拡大 m は平方数となる比較的小さい数に制限するものとする. これは, 前に述べたようにあまり m が大きいと重ねたシェアの位置合わせが困難となるためである.

3.3 画素拡大数制限下での α_t と α_n の最適値

画素拡大数制限下での α_t の最適値を求めるには次のようにすればよい.

$$\begin{aligned} & [\max \alpha_t] \\ & \text{maximize: } X \\ & \text{subject to:} \\ & x_{f(S)}^i, X \in \mathbb{Z}, x_{f(S)}^i \geq 0, i \in \{0, 1\}, S \subset G, \\ & \sum_{S \subset G} x_{f(S)}^1 = \sum_{S \subset G} x_{f(S)}^0 = m, \\ & \sum_{S \subset G: S \cap D \neq \emptyset} (x_{f(S)}^1 - x_{f(S)}^0) = 0, \\ & D \subset G: |D| < t, \\ & X + \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^0 \leq \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^1, \\ & D \subset G: |D| = t \\ & 1 + \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^0 \leq \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^1, \\ & D \subset G: |D| \geq t + 1 \end{aligned} \quad (13)$$

式 (13) の最後の拘束条件ではプログレッシブ型という拘束条件になっていないが, 実際は表 3 のようにプログレッシブ型となることがほとんどのである (意図的にそうでないものを作成することはできるが). 次に画素拡大数制限下での α_n の最適値の定式化について述べる. これは, ほとんど式 (11) と同じで次のように記述できる.

$$\begin{aligned} & [\max \alpha_n] \\ & \text{maximize:} \\ & \sum_{S \subset G: S \cap D \neq \emptyset} (x_{f(S)}^1 - x_{f(S)}^0) \\ & \text{subject to:} \\ & x_{f(S)}^i \in \mathbb{Z}, x_{f(S)}^i \geq 0, i \in \{0, 1\}, S \subset G, \\ & \sum_{S \subset G} x_{f(S)}^1 = \sum_{S \subset G} x_{f(S)}^0 = m, \\ & \sum_{S \subset G: S \cap D \neq \emptyset} (x_{f(S)}^1 - x_{f(S)}^0) = 0, \\ & D \subset G: |D| < t, \\ & 1 + \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^0 \leq \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^1, \\ & D \subset G: |D| \geq t \end{aligned} \quad (14)$$

表 3 の左の欄は α_t , 右の欄は α_n についての最適化の結果を示す. $\beta_i = m\alpha_i$ ($i = 1, \dots, n$) とする. また, * は α_n の最適化に必要な画素拡大の最小サイズ以下の m である場合を示す. たとえば, $(n, t, m) = (8, 3, 64)$ の場合, α_n についての最適化を行うと $\beta_8 = 38$ となり, α_t についての最適化を行った結果 $\beta_8 = 12$ に比べて 3 倍近い視認性を示す. 一方, β_3 の値を比べると

表 1 最適な α_n

$n \setminus t$	2	3	4	5	6	7	8	9	10
2	1/2								
3	2/3	1/4							
4	3/4	1/3	1/8						
5	4/5	4/9	1/5	1/16					
6	5/6	1/2	1/4	1/10	1/32				
7	6/7	9/16	2/7	5/33	2/35	1/64			
8	7/8	3/5	7/20	9/49	5/64	1/35	1/128		
9	8/9	16/25	32/81	7/32	1/9	4/85	1/63	1/256	
10	9/10	2/3	3/7	8/33	9/65	2/33	7/295	1/126	1/512

表 2 最適な α_n を達成する最小画素拡大

$n \setminus t$	2	3	4	5	6	7	8	9	10
2	2								
3	3	4							
4	4	6	8						
5	5	18	15	16					
6	6	14	24	30	32				
7	7	16	35	99	70	64			
8	8	35	100	196	128	140	128		
9	9	50	162	576	315	510	315	256	
10	10	33	245	363	650	1155	590	630	512

表 3 画素拡大数制限下での α_t と α_n の最適値 ($\beta_i = m\alpha_i$)

(n, t, m)	α_t	β_1	β_2	β_3	β_4	β_5	β_6	β_7	β_8	α_n	β_1	β_2	β_3	β_4	β_5	β_6	β_7	β_8
(8,2,9)		0	2	2	3	4	4	5	5		0	1	2	3	4	5	6	7
(8,2,25)		0	7	9	11	12	13	13	13		0	3	6	9	12	15	18	21
(8,2,36)		0	10	14	15	17	18	18	18		0	1	6	11	16	21	26	31
(8,2,49)		0	13	17	21	22	24	25	25		0	6	12	18	24	30	36	42
(8,3,16)*		0	0	1	1	2	3	3	4		0	0	1	2	3	4	5	7
(8,3,25)*		0	0	2	4	5	6	7	8		0	0	1	3	5	8	11	14
(8,3,36)		0	0	3	6	8	10	11	11		0	0	2	5	9	13	17	21
(8,3,49)		0	0	4	7	9	11	12	15		0	0	2	6	11	17	23	29
(8,3,64)		0	0	5	8	10	11	12	12		0	0	2	8	15	22	29	38
(8,3,81)		0	0	7	13	18	21	23	26		0	0	3	10	19	28	38	48
(8,4,36)*		0	0	0	1	2	4	5	8		0	0	0	1	3	5	7	9
(8,4,49)*		0	0	0	1	3	5	7	9		0	0	0	1	3	6	9	15
(8,4,64)*		0	0	0	2	5	9	13	17		0	0	0	1	4	9	14	20
(8,4,81)*		0	0	0	2	5	10	15	21		0	0	0	1	6	13	20	27
(8,4,100)*		0	0	0	3	7	12	18	24		0	0	0	3	9	17	26	35
(8,4,121)		0	0	0	4	9	13	15	15		0	0	0	3	9	17	26	41
(8,4,144)		0	0	0	5	13	22	31	41		0	0	0	2	9	20	33	48

α_n についての最適化は $\beta_3 = 2$ なのに対して α_t についての最適化は $\beta_2 = 5$ となり、視認性が 0.4 倍となってしまう。そのほかの場合においてもこの傾向がほぼ当てはまることが見て取れるだろう。(t,n)-VCSS を考える場合、やはり t 枚付近の重ね合わせの視認性の向上が望まれる性質と考えられる。しかしながら、単純に α_t を最大にしても、上で見たように最大枚数 n 枚を重ね合わせた場合の視認性は確保されない。そこ

で、次節では α_t を最大にしながら、それより多くのシェアを重ねたときの視認性も向上させる方法を検討してみる。

4. ボトムアップアプローチ

α_t を最大にしながら、それより多くのシェアを重ねたときの視認性も向上させる方法として、この節では二つの方法を考える。 $t \leq n-1$ を仮定する。

表 4 画素拡大数制限下での BUP1 と BUP2 の最適値 ($\beta_i = m\alpha_i$)

(n, t, m)	BU1	β_1	β_2	β_3	β_4	β_5	β_6	β_7	β_8	BU2	β_1	β_2	β_3	β_4	β_5	β_6	β_7	β_8
(8,2,9)		0	2	3	4	5	5	6	6		0	2	3	4	4	5	6	6
(8,2,25)		0	7	10	12	12	13	13	13		0	7	9	11	12	13	13	13
(8,2,36)		0	10	15	18	19	20	20	20		0	10	14	16	18	20	20	20
(8,2,49)		0	13	21	26	29	30	30	30		0	13	20	24	26	29	30	30
(8,3,16)*		0	0	1	2	3	4	5	7		0	0	1	2	3	4	5	7
(8,3,25)*		0	0	2	4	6	7	8	8		0	0	2	3	5	6	7	8
(8,3,36)		0	0	3	6	9	11	12	13		0	0	3	6	8	9	10	14
(8,3,49)		0	0	4	9	13	16	18	19		0	0	4	8	12	16	20	24
(8,3,64)		0	0	5	11	17	23	29	35		0	0	5	11	17	23	29	35
(8,3,81)		0	0	7	15	21	25	28	30		0	0	7	13	19	25	30	34
(8,4,36)*		0	0	0	1	3	5	7	9		0	0	0	1	3	5	7	9
(8,4,49)*		0	0	0	1	4	7	10	13		0	0	0	1	3	6	10	15
(8,4,64)*		0	0	0	2	6	10	14	18		0	0	0	2	5	10	15	20
(8,4,81)*		0	0	0	2	7	13	19	25		0	0	0	2	5	11	18	27
(8,4,100)*		0	0	0	3	9	17	26	35		0	0	0	3	9	17	26	35
(8,4,121)		0	0	0	4	11	20	30	40		0	0	0	4	11	20	30	40
(8,4,144)		0	0	0	5	13	22	31	41		0	0	0	5	12	21	32	42

[ボトムアップアプローチ 1 (BU1)]

α_t の最適化 (13) を $MP(t)$ と定義する (実行可能とする)。

- (1) $MP(t)$ 実行する。
- (2) $k = t$ とする。
- (3) $k = n$ ならば終了。そうでなければ, $MP(k)$ を実行。 $MP(k)$ で得られた最適値を β_k として $MP(k)$ の $|D| = k$ の場合の制約条件を

$$\beta_k + \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^0 \leq \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^1, \\ D \subset G: |D| = k$$

に置き換える。また, $MP(k)$ の $|D| = k+1$ の場合の制約条件を

$$X + \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^0 \leq \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^1, \\ D \subset G: |D| = k+1$$

に置き換える。 $k = k+1$ とする。

- (4) (3) を実行。

簡単に言えば, ボトムアップアプローチ 1 はグリーディに重ね合わせが一つ増えるごとにその濃淡差を最大化して行こうということである。 BU1 同様 α_t の最大化に基づく次の方法をボトムアップアプローチ 2 とした。 β_t は式 (13) の最適値を用いる。

[ボトムアップアプローチ 2 (BU2)]

maximize:

$$\sum_{S \subset G: S \cap G \neq \emptyset} (x_{f(S)}^1 - x_{f(S)}^0)$$

subject to:

$$x_{f(S)}^i \in \mathbb{Z}, x_{f(S)}^i \geq 0, i \in \{0, 1\}, S \subset G,$$

$$\sum_{S \subset G} x_{f(S)}^1 = \sum_{S \subset G} x_{f(S)}^0 = m,$$

$$\sum_{S \subset G: S \cap D \neq \emptyset} (x_{f(S)}^1 - x_{f(S)}^0) = 0,$$

$$D \subset G: |D| < t,$$

$$\beta_t + \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^0 \leq \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^1,$$

$$D \subset G: |D| = t$$

$$1 + \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^0 \leq \sum_{S \subset G: S \cap D \neq \emptyset} x_{f(S)}^1,$$

$$D \subset G: |D| \geq t+1$$

BU2 は t 枚の重ね合わせのとき得られる視認性 α_t を最大にしつつ, n 枚の重ね合わせのときになるべく視認性を高めようという考えに基づいている。

BU1 と BU2 を表 3 と同じパラメータで実施した結果が表 4 である。表 3 と同じく $(t, n, m) = (3, 8, 64)$ の場合を見てみよう。 BU1, BU2 とともに $\beta_t = 5$ となり, t 枚重なるときの視認性が式 (14) に比べてよいことが期待される。一方, BU1, BU2 とともに $\beta_n = 35$ となり n 枚重なったときの視認性は式 (13) よりも高まっていることが期待できる。

上記のことを具体例で見てみることにする。秘密画像は図 2 と同じ “MO” という文字とする。このとき

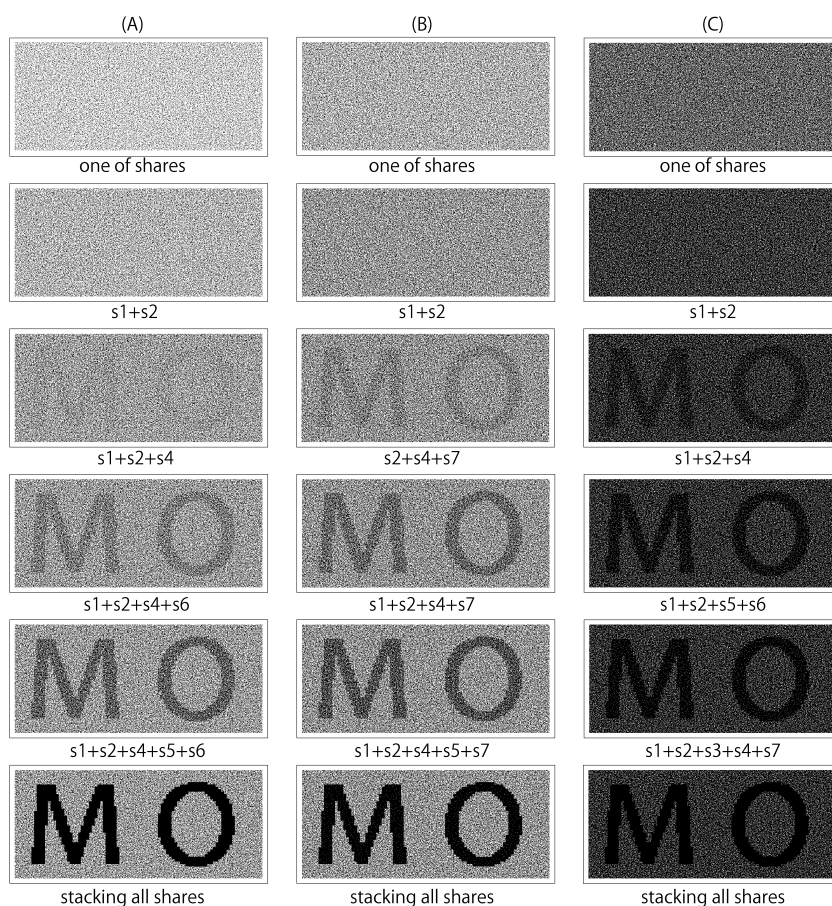


図4 $(t, n) = (3, 8)$ の場合の各方法
(A): $\max \alpha_n$, (B): BUP1, (C): $\max \alpha_t$

式 (14), BU1, 式 (13) を適用したのが図 4 の (A), (B), (C) である。1 段目の “one of shares” はそれぞれの方法で求めたシェア ($s_1 \sim s_8$) の一つ (s_1 だが) を表す。残りの七つのシェアもほぼ同じような画像となる。 $s_1 + s_2$ などはシェア 1 とシェア 2 を重ね合わせて得られる画像を意味する。6 段目の画像はシェア 1 からシェア 8 をすべて重ね合わせた画像である。

$t = 3$ 枚の重ね合わせでは、方法 (A) では “MO” という文字が読み取りにくいのに対して (B) ではそれを読み取ることができる。一方 (C) では全体が暗くなってしまい、読み取りにくくなっている。 n 枚の重ね合わせを見ると (A) が濃淡がはっきりしており、見やすいと言える。(B) も (A) ほどではないが、濃淡がはっきりしていると言える。

ところで、(B) と (C) は同じ $\beta_t = 5$ をもつので、シェアの重ね合わせによりほぼ同じような復元画像が得られるのではないかと想像される方もいらっしゃるのではないと思う。しかしながら、実際に試してみ

ると、上記で見たようになり違うものが得られる。この理由について考えてみる。(A) は n 枚重ねたときの α_n を最大にしなければならないので、そもそもシェアたちが白っぽく (符号化行列に 0 が多く) なければならない。BU1, BU2 もその考えが入っているため、重ね合わせ画像の文字以外の部分は全体的に白くなっている。一方、(C) では n 枚重なったときの最大化を考慮していないため、 α_n の値は小さくなる傾向にあり、文字以外の部分は暗くなる傾向にある。(文字もより黒くなるので悪いばかりではない。その辺の兼ね合いだろうか?)

紙面の関係でそのほかの例を紹介できなかったのが残念だが、ほかのパラメータにおいても上記の傾向は確認できる。

参考文献

- [1] M. Naor and A. Shamir, “Visual cryptography,” *Advances in Cryptography—Eurocrypt 94*, Lecture Notes

- in Computer Science, **950**, pp. 1–12, 1995.
- [2] Y. C. Hou, “Visual cryptography for color images,” *Pattern Recognition*, **36**, pp. 1619–1629, 2003.
- [3] 山口泰, “連続階調画像のための拡張視覚復号型暗号 (チュートリアル),” *応用数理*, **25**, pp. 129–134, 2015.
- [4] 黒澤馨, 『現代暗号への招待』, サイエンス社, 2010.
- [5] H. Koga and E. Ueda, “Proposal of asymptotically contrast-ideal T, n -threshold visual secret sharing scheme,” In *Proceedings of 2006 IEEE International Symposium on Information Theory*, pp. 912–916, 2006.
- [6] C. Blundo, P. D’Arco, A. De Santis and D. R. Stinson, “Contrast optimal threshold visual cryptography schemes,” *SIAM Journal on Discrete Mathematics*, **16**, pp. 224–261, 2003.
- [7] T. Hofmeister, M. Krause and H. U. Simon, “Contrast-optimal out of secret sharing schemes in visual cryptography,” *Theoretical Computer Science*, **240**, pp. 471–485, 2000.
- [8] H. Koga, “A general formula of the (t, n) -threshold visual secret sharing scheme,” *Advance in Cryptology-ASIACRYPT 2002*, Lecture Notes in Computer Science, **2501**, pp. 328–345, 2002.
- [9] M. Iwamoto, “A weak security notion for visual secret sharing schemes,” *IEEE Transactions on Information Forensics and Security*, **7**, pp. 372–382, 2012.
- [10] S. J. Shyu and M. C. Chen, “Optimum pixel expansions for threshold visual secret sharing schemes,” *IEEE Transactions on Information Forensics and Security*, **6**, pp. 960–969, 2011.
- [11] K. Okada and H. Koga, “A construction of the progressive $(3, n)$ -threshold visual cryptography using a BIBD and analysis of its optimality,” In *Proceedings of 2017 IEEE Information Theory Workshop*, 2017, DOI: 10.1109/ITW.2017.8277939.