微小な復号誤り確率を許容する効率的な秘密分散法の研究

古　賀　弘　樹　　筑波大学大学院システム情報工学研究科准教授

1 はじめに

秘密分散法は、インターネット社会の安全性を守るセキュリティ技術として注目されている。秘密分散法では、**ディーラ**と呼ばれる人物が、１つの秘密情報から、ディーラだけが用いることができる一様乱数を用いて、**シェア**と呼ばれる分散情報を生成する。生成されたシェアは、m 人のユーザそれぞれに１つずつ、秘密裏に配布される。特に**(t,m)しきい値法**として知られる秘密分散法は、任意の t 人がもつシェアから秘密情報が復元でき、逆に、どんな $t-1$ 個のシェアからも秘密情報が一切漏れないという性質をもっている。

秘密分散法に関しては、秘密分散法が Shamir [1]と Blackley [2]によって独立に提案されて以降、様々な研究が行われてきた。Karnin ら[3]は、(t,m)しきい値法のシェアのエントロピーが、必ず秘密情報のエントロピー以上になることを示しており、この結果は (t,m)しきい値法に限らない一般の秘密分散法に拡張されている。また、Blundo ら[4]は、ディーラが必要とするランダムネスに注目し、任意の (t,m)しきい値法に関してランダムネスが $(t-1)\log|\mathrm{X}|$以上必要であることを示した。ここに X は秘密情報が値をとる有限集合（アルファベット）であり、$|\mathrm{X}|$はその要素数である。しかしながら、Blundo らはランダムネスを、秘密情報 S を与えたときの m 個のシェアの条件つきエントロピーと定義しており、一様乱数のビット長とは一致しないこと、また下界が $(t-1)H(X)$（$H(X)$は秘密情報 X のエントロピー）とは異なりやや直観に反する、という問題点があった。

本研究では、復号時に微小な復号誤りを許すという問題設定のもとで、(t,m)しきい値法を実現するためにディーラに必要な一様乱数の長さ（レート）を評価する。本研究では、ある情報源から出力される n 個の秘密情報を、ディーラが一様乱数を用いて n 個の秘密情報を一括して m 個のシェアに変換する状況を考える。情報源としては**一般情報源**と呼ばれるクラスを考える。一般情報源のクラスは無記憶情報源、マルコフ情報源などあらゆる情報源クラスを含んでいる。本稿では、第２節で、微小な復号誤り確率を許す (t,m)しきい値法を定義し、シェアのレートおよびディーラが用いる一様乱数のレートに関連する不等式を与える。与えた不等式において、情報源の無記憶性を仮定すると、(t,m)しきい値法においてディーラが必要な一様乱数のレートの下界が $(t-1)H(S)$となることがわかる。また、ある仮定のもとで、得られた下界を達成する、微小な復号誤りを許す (t,m)しきい値法が構成できることも示す。この結果を第２節で述べる。

本研究ではまた、シェアをもつユーザになりすます不正者がいる状況のもとでの、不正者特定のための(3,3)しきい値法について考察した。この結果を第３節で述べる。さらに、本研究では複数の画像を復元できる視覚復号型秘密分散法に関する結果も得ることができた。この結果を第４節で述べる。

2 復号時に微小な復号誤りを許す秘密分散法

本節で考える (t,m)しきい値法のブロック図を図１に示す。各 $n\geqq 1$ に対して、情報源は長さ n の系列 X^n を出力する。情報源には無記憶性を仮定せず、アルファベットサイズは可算無限であってよい。他方、乱数生成器は、X^n と独立な一様乱数 E_n を出力する。符号器は X^n と E_n から、m 個のシェア $W_n^{(1)}, W_n^{(2)}, \ldots, W_n^{(m)}$ を生成する。復号器は、任意の t 個のシェア $W_n^{(i1)}, W_n^{(i2)}, \ldots, W_n^{(im)}$ から X^n を復号する。我々は、n が十分大きいときに (t,m)しきい値法になるように、以下の２つの条件を課す。

(1) 任意の t 個のシェアから秘密情報 X^n を復元するとき、復号誤り確率は $n\to\infty$ で 0 に収束する。

(2) （確率的上極限の意味で）どの t 個未満のシェアの組からも X^n の情報が得られない。

通常の秘密分散法の枠組みでは、条件(1)の復号誤り確率は０に等しいが、本研究では情報理論的な深い議論を可能にするため、復号誤り確率が漸近的に 0 になるとしている。また、条件(2)は、t 個未満の任意のシェアと、情報源出力が独立である定義されるが、本研究では、n が十分大きいときは１に近い確率で、t 個未満の任意のシェアと情報源出力がほとんど独立になることを要請する。

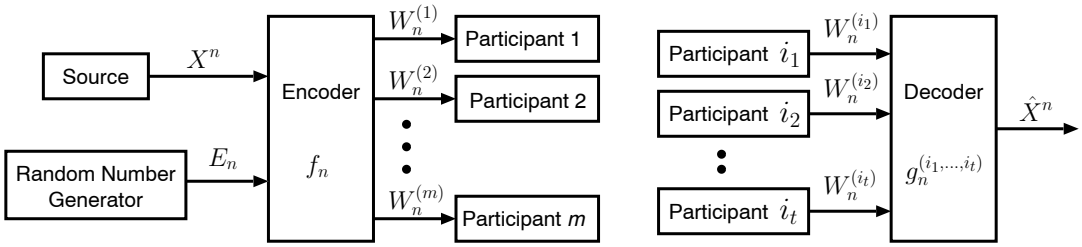

図１　微小な復号誤りを許す *(t, m)*しきい値法

我々は逆地理に相当する次の定理を得た[5]。

定理１　与えられた情報源 X^n, $n \geqq 1$, のもとで、上の条件(1), (2)を満たす任意の *(t, m)*しきい値法は、任意の定数 $\alpha > 0$ に対して

$$p - \liminf_{n\to\infty} \frac{1}{n^{\alpha}} \log(M_n P_{X^n}(X^n)^{t-1}) \geq 0$$

を満たす。ここに、確率変数列 *Zn*, $n \geqq 1$ に対して確率的下極限は

$$p - \liminf_{n\to\infty} Z_n = \sup\{\alpha : \lim_{n\to\infty} \Pr\{Z_n > \alpha\} = 0\}$$

と定義され、*Mn* は一様乱数 E_n のサイズを表す。

定理１より、情報源が定常無記憶であれば、一様乱数のサイズ *Mn* に関して

$$\liminf_{n\to\infty} \frac{1}{n} \log M_n \geq (t-1)H(X)$$

が成り立つ。ここに *H(X)*は情報源のエントロピーである。この結果は、復号誤りが漸近的に０に収束する状況であっても、*(t, m)*しきい値法を実現するためには、少なくとも *(t-1)H(X)*のレートの一様乱数が必要であることを示している。

我々はまた、次の定理で示すように、可算無限アルファベットをもつ一般的な情報源に対しても、上の条件(1), (2)の意味での *(t, m)*しきい値法を構成できることを示した[5]。

定理２　与えられた情報源 X^n, $n \geqq 1$, に対して、各 $n \geqq 1$ に対して $p_n > m$ かつ

$$\lim_{n\to\infty} \Pr\{\log(p_n P_{X^n}(X^n)) \geq 0\} = 0$$

を満たす素数列 p_n, $\geqq 1$ が存在すれば、一様乱数のレートが $\log p_n$ に等しい *(t, m)*しきい値法が構成できる。

3 攻撃者を特定できる(3,3)しきい値法

前節で述べたような通常の秘密分散法では、シェアをもつユーザは、秘密情報の復号に際して正直に自分のもつシェアを供出することを仮定する。ところが、秘密分散法において、自分のもつシェアと異なる不正なシェアを供出するユーザのような敵対者の存在を仮定すると、秘密分散法はまた別の面白さを見せる。実際、Shamir の *(t, m)*しきい値法[1]のような代表的な秘密分散法では、敵対者の攻撃は確率１で成功してしまう。したがって、敵対者による不正を検出する、もしくは敵対者を特定することも可能な、秘密分散法を構成する必要がある。敵対者の存在のもとでの秘密分散法は McElice [6], Tompa and Woll [7]などによって議論され、様々な構成法が提案されてきているが、敵対者の不正の成功確率の上界を ε とするときシェアのサイズが $1/\varepsilon$ を含み、ε を０に近づけるとシェアサイズが無限大になるという弱点をもっていた。本研究では、不正者が存在する状況のもとで(3, 3)しきい値法を議論し、任意の２つのシェアの間に相関があれば、ある仮定のもとで高い確率で不正を行ったユーザの特定ができることを示した。任意の２つのシェアが相関を

もつ(3,3)しきい値はBIBD (Balanced Incomplete Block Design)として知られる組合せ構造を用いることで実現できる。

3.1 BIBD を用いた(3,3)しきい値法の構成法

任意の 2 つのシェアが相関をもつ(3,3)しきい値法を構成するために、BIBD と呼ばれる次の構造を用いる。

定義１ (BIBD) v, k, λを、$v > k \geqq 2$ を満たす正整数とする。点の集合 Vとブロックの集合 B の組(V, B)が以下の 3 条件をすべて満たすとき、(v, k, λ)-BIBD という。

（条件１）$|V| = v$。

（条件２） すべてのブロックはちょうど k 個の点をもつ。

（条件３）相異なる２点は、ちょうど λ 個のブロックに含まれる。

いま V={0,1,2,3,4,5,6}, B = {012, 034, 056, 135, 146, 236, 245} とおくと、(V, B)は上の 3 条件を満たす。ゆえに(V, B)は(7,3,1)-BIBD となっている。

(3,3)しきい値法の構成のため、我々は２つの BIBD を用いる。以下、例をもとに説明する（図２）。いま V = {0,1,2,3,4,5,6}に対して

B_0 = {012, 034, 056, 135, 146, 236, 245}

B_1 = {016, 024, 035, 123, 145, 256, 346}

とおくと、(V, B_0)と(V, B_1)はともに(7,3,1)-BIBD になっていて、さらに B_0 と B_1にともに属するブロックはない。よって、秘密情報 S が 0 または 1 の値をとるとき、S=0 ならば B_0から、S=1 ならば B_1から、一様ランダムにブロックを選び、選んだブロックの３つの点に一様ランダムな置換を施して、ブロックの各点を 3 人のユーザがもつシェアとする方式が考えられる。B_0 と B_1にともに属するブロックがないことから、3 人のシェアから秘密情報 Xを誤りなく復元できることは明らかである。また(V, B_0)と(V, B_1)がともに BIBD であることから、任意の２つのシェアの組は B_0 と B_1にちょうど１個含まれ、２つのシェアから秘密情報が漏れないことは直観的にも明らかである。この方式は Stinson-Vanstone [7]により提案された方式の特殊な場合になっている。

さらに、このように得られたシェアの相互情報量を計算することにより、次の定理を得ることができる。導出については文献[9]を見られたい。

定理３ (V, B_0)と(V, B_1)を共通のブロックがない２つの$(v,3,1)$-BIBD とすると、２値の情報源に対して(3,3)しきい値法が実現できる。また、実現した(3,3)しきい値法のシェアを X,Y,Z とするとき、シェア間の相互情報量は

$$I(X;Y) = I(Y;Z) = I(X;Z) = \log\,(1 - 1/v)$$

$$I(X;YZ) = I(Y;XZ) = I(Z;XY) = \log\, v - H(S)$$

で与えられる。

一般に、Vが等しく、共通なブロックをもたない c 個の BIBD が存在すれば、c 個のシンボルをもつ情報源に対する(3,3)しきい値法を実現できる。我々は数値実験により、(7,3,1)-BIBD は２個の、(9,3,1)-BIBD は最大７個のシンボルをもつ情報源に適用できることを明らかにした。

3.2 性能評価

3,1 節で構成した(3,3)しきい値法を用いると、ある前金的な枠組みの中では不正検出および不正者特定が実現できる。いま $S_1, S_2, \ldots, S_l$ を、無記憶情報源が出力した l 個の独立な情報源出力とする。簡単のため、情報源出力は集合{0,1}に値をとるとし、共通のブロックをもたない２つの$(v,k,1)$-BIBD $(V, \mathrm{B}_0), (V, \mathrm{B}_1)$が存在することを仮定する。情報源出力 $S_1, S_2, \ldots, S_l$ はシンボルごとに独立に(3,3)しきい値法のシェアに変換され、ユーザ１、ユーザ２，ユーザ３のもつシェアをそれぞれ $X_1, X_2, \ldots, X_l$, $Y_1, Y_2, \ldots, Y_l$, $Z_1, Z_2, \ldots, Z_l$ と書く。X_i, Y_i, Z_iが秘密情報 S_iに対応する３個のシェアであり、X_i, Y_i, Z_iから S_iが復元できる。

本節では、攻撃者が、ユーザ１，ユーザ２，ユーザ３のいずれかになりすます**なりすまし攻撃**だけを考える。また、攻撃者が生成するシェアは、残り２つのシェアとは独立であると仮定する。すなわち、攻撃者がユーザ３になりすますべく $Z_1', Z_2', \ldots, Z_l'$を生成するとき、各成分は独立であり、また、組$(\mathrm{X}_i, \mathrm{Y}_i)$と Z_i'も独

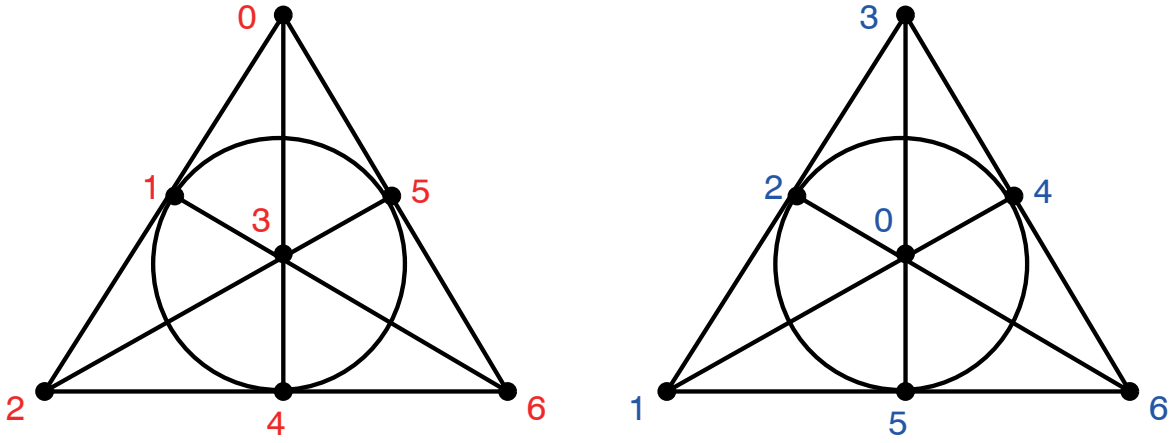

図２　共通のブロックをもたない２つの’(7,3,1)-BIBD

立になる。

このような問題設定では次の定理を示すことができる。詳細は[9]を見られたい。

定理４　次の性質を満たす復号器が構成できる。

(1) 不正者が存在しないとき、正当な３つのシェアが正しく復号される確率は $l\to\infty$ で 1 に漸近する。

(2) ユーザ３のシェアが不正に生成されたとき、３つのシェアが正当であると判断してしまう確率は l が十分大きいとき $2^{-lI(XY;Z)+o(l)}$ 以下となる。

(3) ユーザ３のシェアが不正に生成されたとき、誤ってユーザ１のシェアを不正であると判断してしまう確率は、l が十分大きいとき $2^{-lI(Y;Z)+o(l)}$ 以下であり、誤ってユーザ２のシェアを不正であると判断してしまう確率は $2^{-lI(X;Z)+o(l)}$ 以下となる。

3.1 節で構成した(3,3)しきい値法は相互情報量はいずれも正の値をとっていた（定理 3)。このことから、上の定理 4(2)(3)の中の確率の指数部はともに正の値を取り、l を十分大きくすれば(2)(3)の確率は指数関数的に 0 に収束することがわかる。

4　複数画像を隠すことができる視覚復号型秘密分散法

秘密分散法の中でも、Naor と Shamir により提案された視覚復号型秘密分散法[10]はディジタル画像の共有に有効であり、秘密情報の復号時に計算機を必要としないという特徴をもっている。視覚復号型秘密分散法で (t,m)しきい値法を実現するときには、ディーラが 1 枚の秘密画像から m 枚のシェアを生成し、それぞれのシェアを OHP シートのような透明なシートに印刷して各ユーザに配布する。任意の t 人のユーザは、それぞれが持つシェアを重ね合わせることによって秘密画像を復元できる。他方、どんな $t-1$ 人のもつシェアからも秘密画像に関する情報は一切漏れない。この視覚復号型秘密分散法の枠組みは様々な形に拡張され、加藤と今井[11]は、複数枚の画像を分散共有する方式を提案した。特に[11]では、シェアを重ねる枚数に応じて、2 枚の異なる秘密画像が復元される方式が提案されている。本研究では、この研究をさらに発展させて、重ねるシェアの枚数に応じて k 枚の画像が復元できる方式を提案する。また、シェアを重ねることによって知覚される秘密画像のコントラストの線形和が、ある上界をもつことを示す。

4.1 $(m-1,m)$しきい値法と $(m-1,m,m)$しきい値法

まず、Naor と Shamir によって提案された (t,m)しきい値型の視覚復号型秘密分散法[10]を $(t,m)=(2,3)$ の場合について述べる。図３では、(2,3)しきい値型の秘密分散法を表している。1 枚の秘密画像が 3 枚のシェアに暗号化される。シェアは透明なシートに印刷されて 3 人のユーザに配布される。3 人のユーザの任意の 2 人が集まり、互いのシェアを重ね合わせることで、もとの秘密画像が知覚される。

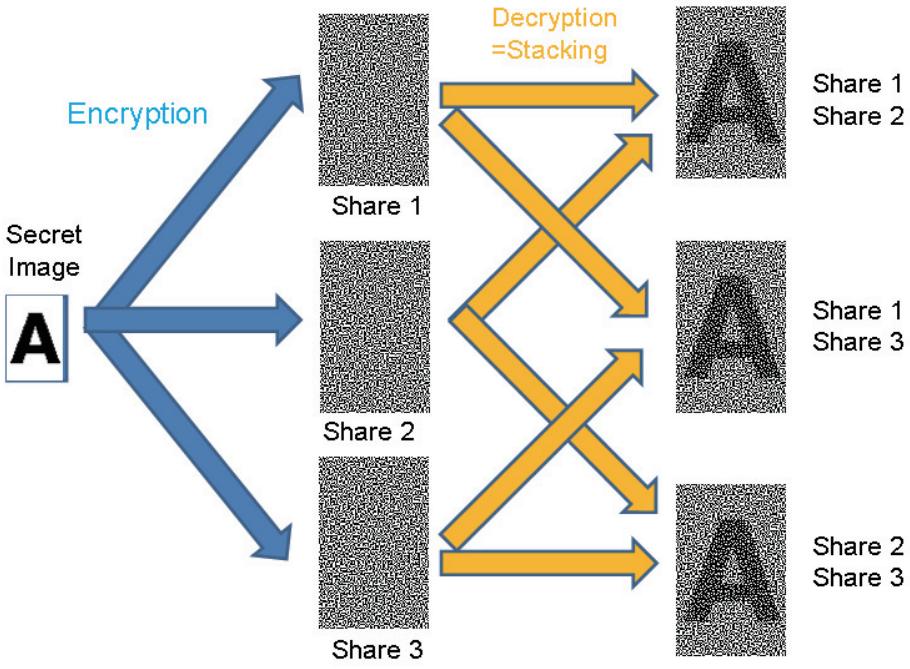

図３　通常の(2, 3)しきい値型の視覚復号型秘密分散法

これに対して、加藤・今井によって提案された(2, 3, 3)しきい値型の視覚復号型秘密分散法[11]の概念図を図４に示す。図４において、秘密画像は２枚、シェアは３枚であり、任意の２枚のシェアを重ねることによって秘密画像１が知覚され、3 枚重ねることによって秘密画像２が知覚されることがわかる。2 枚のシェアからは、秘密画像２の情報は一切漏れない。

ところが、(2, 3, 3)しきい値型の秘密分散法は様々な変形をもつ。実際、2 枚のシェアを重ねたときに１枚目の秘密画像が図４（図５左と同じ）よりクリアに見えるようにすると、3 枚のシェアを重ねたときに見える 2 枚目の秘密画像が暗く見えることになる（図５中央)。逆に、3 枚のシェアを重ねたときに見える秘密画像をクリアに見えるようにすると、2 枚のシェアを重ねたときに見える秘密画像が暗く見えてしまう（図５右)。このトレードオフを厳密に定式化することが本研究の１つの目的である。

*(m-1, m, m)*しきい値型の視覚復号型秘密分散法は、基本行列と呼ばれる 4 個の基本行列を用いて構成される。

定義４　4 個の *m* 行 *q* 列のブール行列 $X_{00}, X_{01}, X_{10}, X_{11}$ が以下の 4 個の性質を満たすとき、(*m-1, m, m*) しきい値型の視覚復号型秘密分散法の基本行列であるという。

（条件１） $X_{00}, X_{01}, X_{10}, X_{11}$ の任意の *m*-2 行は、列の並べ替えによって同一の行列にできる。

（条件２） X_{00}, X_{01} の任意の *n-1* 行は、列の並べ替えによって同一の行列にできる。同様に、X_{10}, X_{11} の任意の *m*-1 行も列の並べ替えによって同一の行列にできる。

（条件３） $S \in \{1,2,...,m\}$ をサイズ *m*-1 の任意の部分集合とするとき、ある非負整数 C_0, C_1 が存在して

$$HW(OR(X_{00}[S])) = HW(OR(X_{01}[S]) = C_0$$
$$HW(OR(X_{10}[S])) = HW(OR(X_{11}[S]) = C_1 > C_0$$

が成り立つ。ここに $X_{00}[S]$ は X_{00} の行を S に制限した行列を、OR は行列の列ごとの OR をとる

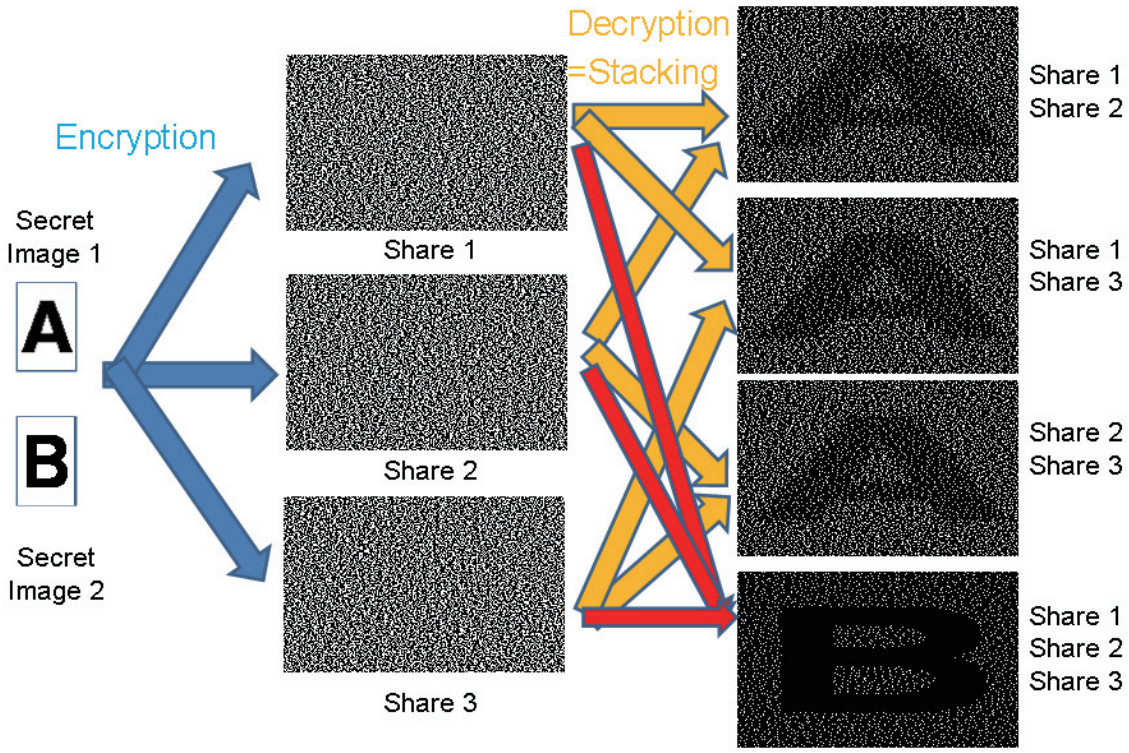

図４　　２枚の画像を隠すことができる視覚復号型秘密分散法

演算を、HW はハミング重みを表す。

（条件４）$S \in \{1,2,...,m\}$ をサイズ m の部分集合とするとき、ある非負整数 D_0, D_1 が存在して

$$HW(OR(X_{00})) = HW(OR(X_{10}) = D_0$$
$$HW(OR(X_{01})) = HW(OR(X_{11}) = D_1 > D_0$$

が成り立つ。

いま、**相対差**(relative difference)と呼ばれる量を

$$\alpha_{m-1} = \frac{HW(OR(X_{10}[S])) - HW(OR(X_{00}[S]))}{m}$$
$$\alpha_m = \frac{HW(OR(X_{10})) - HW(OR(X_{00}))}{m}$$

と定義する。α_{n-1} は $m-1$ 枚のシェアを重ねたときに復号される秘密画像の明るさ、α_m は m 枚のシェアを重ねたときの秘密画像の明るさを表す量であり、一般に大きければ大きいほど秘密画像が明るく見えることになる。我々は**正準**(canonical)な基本行列のクラスを定義し、次の結果を得た[12]。

定理５　正準な任意の $(m-1, m, m)$ しきい値型の視覚復号型秘密分散法の基本行列に対して、

$$m2^{m-1}\alpha_{m-1} + 2^m \alpha_m \le 1$$

が成り立つ。

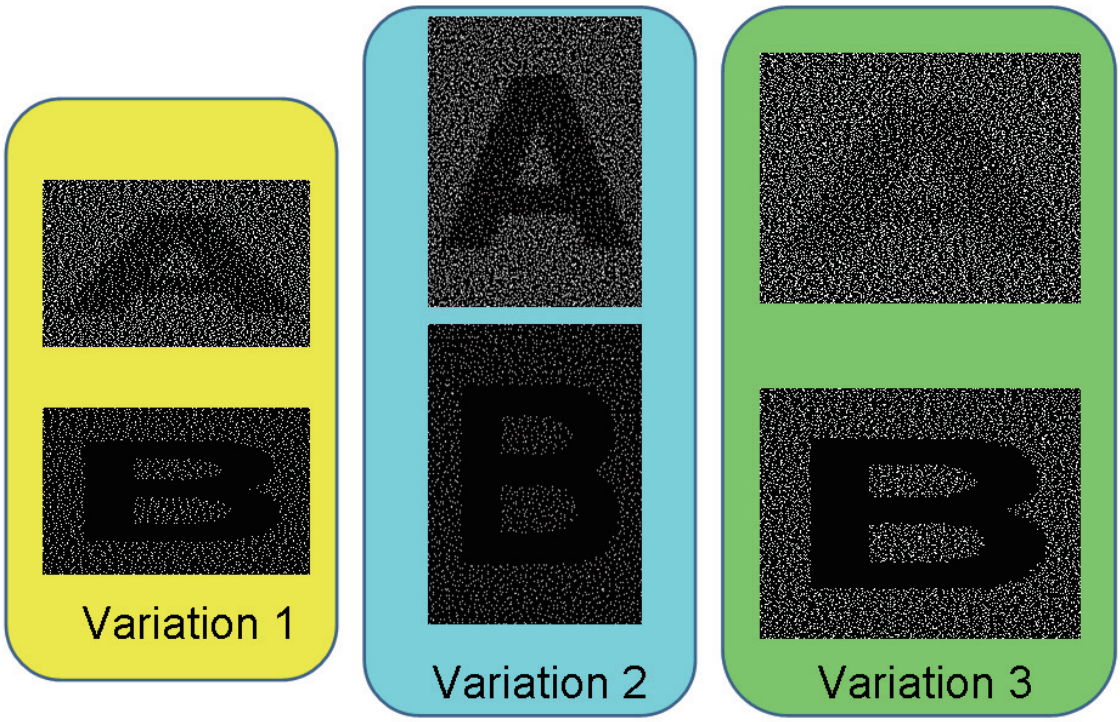

図５　復号される２つの秘密画像のコントラストの違い

定理５はα_{n-1}とα_mを同時には大きくできないことを主張している。特に m=3 のときに上の等号が成立するようにすると$\alpha_{n-1}=\alpha_m=1/10$となり。加藤と今井が与えた構成はこの値を達成していることが確認できる。

4.2　(*m*-2,*m*-1,*m*,*m*)しきい値型への拡張

(*m*-2, *m*-1, *m*-1, *m*) しきい値型の視覚復号型秘密分散法では、。3 枚の秘密画像が *m* 枚のシェアに暗号化され、*m*-2 枚の任意のシェアを重ねると 1 枚目の秘密画像が、*m*-1 枚の任意のシェアを重ねると 2 枚目の秘密画像が、*m* 枚の任意のシェアを重ねると 3 枚目の秘密画像がそれぞれ現れる。また、*m*-3 枚のシェアからはすべての秘密画像の情報が、*m*-2 枚のシェアからは秘密画像 2 と 3 の情報が、*m*-1 枚のシェアからは秘密画像 3 の情報が、それぞれ一切漏れないようになっている。(*m*-2, *m*-1, *m*, *m*) しきい値型の場合は 8 個の基本行列を使うことになるが、(*m*-1, *m*, *m*) しきい値型の場合と同様に、相対差および正準な基本行列のクラスを定義することができ、次の定理が成り立つことを示すことができる。

定理６　正準な任意の (*m*-2, *m*-1, *m*, *m*) しきい値型の視覚復号型秘密分散法の基本行列に対して、

$$m(m-1)2^{m21}\alpha_{m-2}+m2^{m-1}\alpha_{m-1}+2^m\alpha_m \le 1$$

が成り立つ。

$\alpha_{m-2}=\alpha_{n-1}=\alpha_m$ のもとでは、m=4 のときには相対差の上限は 1/36 になり、この値を達成する基本行列を構成することができる。定理６はまた、k 枚の秘密画像を隠す場合へと容易に拡張することができる。詳しくは[12]を見られたい。

【参考文献】

[1] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, n¥ pp, 612—613, 1979.

[2] R. Blackley, “Safegarding cryptographic keys,” *Proc. AFIPS 1979; National Computer Conference*, vol. 48, pp.313—317, 1979.

[3] E. D. Karnin, J. M. Greene, and M. E. Hellman, “On secret sharing systems,” *IEEE Trans.. formation Theory*, vol. 29, pp. 35—41, 1983.

[4] C. Blundo, A. De Santis, and U. Vaccaro, “Randomness in distributed protocols,” *Information and Computation,* vol. 131, no. 2, pp. 111—139, 1996.

[5] H. Koga, “Coding theorems on the threshold scheme for a general source,” I*EEE Trans. Information Theory,* vol. 54, no. 6, pp. 2658—2677, 2008.

[6] R. J. McElice and D. V. Sarwate, “On the secret sharing scheme and Reed-Solomon codes,” *Communications of the ACM,* vol. 24, no. 9. pp. 583—584, 1981.

[7] M. Tompa and H. Woll, “How to share a secret with cheaters,”. *J. Cryptology*, vol. 1, no. 2, pp.:133-138, 1988.

[8] D. R. Stinson and S. A. Vanstone, “A combinatorial approach to threshod scheme,” SIAM J.. Discrete Math. Vol. 1, no.2, pp. 230--236, 1988.

[9] 古賀弘樹, “任意の2つのシェアが相関をもつ(3,3)しきい値法の一構成法とその不正者検出への応用,” 第31回情報理論とその応用シンポジウム、pp. 798—803, 2008.

[10] M. Naor and A. Shamir, “Visual cryptography,” Advances in Cryptography—EUROCRYPT 94, pp. 1—12, 1994.

[11] 加藤拓、今井秀樹, “視覚復号型秘密分散法の拡張構成方式,” 電子情報通信学会和文論文誌A, vol. J79-A, pp. 1344—1351, 1996.

[12] H. Koga and M. Miyata, “A construction of a visual secret sharing scheme for plural secret images and its basic properties,” Proc. International Symposium on Information Theory and its Applications, pp. 24—29, 2008.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Coding theorems on the threshold scheme for a general source	IEEE Transactions on Information Theory	2008.8
任意の２つのシェアが相関をもつ(3,3)しきい値法の一構成法とその不正者検出への応用	第３１回情報理論とその応用シンポジウム予稿集	2008.19
A construction of a visual secret sharing schyeme for plural secret images and its basic properties	Proceedings of 2008 International Symposium on Information Theory and its Applications	2008.12