RL-004

# カメラ撮影画像を用いた秘密分散法
# Secret Sharing Schemes using camera capture images

福嶋 貴幸† 甲斐 博† 木下 浩二†
Takayuki Fukushima Hiroshi Kai Koji Kinoshita

## 1. はじめに

秘密情報を安全に守るために鍵を用いた暗号化を行うのが一般的であるが，根本的な問題として，鍵の紛失・漏洩などに備えるために鍵の管理が必要となる．そこで，鍵を用いずに秘密情報を守る方法として秘密分散法が Shamir と Blakley によって独立に提案された．秘密分散法とは秘密情報を複数の分散情報に分け，分散情報を一定数以上集めた場合のみ情報を復元できるというものである．分散情報を 1 つ入手したとしてもそこから元のデータに関する情報は何も得られず，鍵の漏洩・紛失のリスクもないため高い安全性を得ることができる．

秘密分散法の手法の一つに視覚復号型秘密分散法(Visual Secret Sharing Scheme : VSS scheme)[1][3]がある．VSS scheme とは，秘密情報が含まれている画像を複数の画像に分割し，その分割した画像を重ね合わせることで視覚的に復元できる技術である．

VSS scheme の応用として，生成した 2 枚の画像を電子媒体と紙媒体で保持して，紙媒体上の分割画像をカメラで撮影し，もう一枚の分割画像を撮影画像に対して自動で重ねあわせるようにすることで，電子媒体上で復元する手法が提案されている[2]．一般に VSS scheme は紙のみを利用する手法であるが，近年では紙の代用としても広く普及している電子端末と組み合わせることで，その用途が広がると考えられる．

例えばクレジットカードのカード番号やセキュリティコード，免許証などの顔写真に対して，自分の持つ電子端末を通してのみ確認することができるようにする，といった用途が考えられる．しかし，提案されている手法[2]では画像に用いることのできる色が白と黒の 2 値だけとなるので，表現できる画像が限られてしまう．

本研究では一般的に用いられる秘密分散法である Shamir の$(k,n)$閾値秘密分散法による方法を検討する．すなわち 2 値画像に限ることなく，秘密情報が含まれる画像を$(k,n)$閾値秘密分散法を用いて生成した二枚の画像を電子媒体と紙媒体で保持し，紙媒体上の分割画像をカメラで撮影することで秘密画像を復元する方法を検討する．

## 2. 秘密分散法

本節では，2.1 節で秘密分散法の概略を述べ，2.2 節で Shamir の$(k,n)$ 閾値秘密分散法について述べる．また，2.3 節では VSS scheme を用いた中間らの手法について述べる．

†愛媛大学，Ehime University

### 2.1 秘密分散法とは

秘密分散法とは Shamir と Blakley によって独立に提案された．一般的に秘密分散法とは$(k,n)$閾値秘密分散法を指す．$(k,n)$閾値秘密分散法は秘密情報を分散する分散段階と，秘密情報を復元する復元段階から構成される．分散段階では，秘密情報$S$から$n$個の分散情報$D_1, D_2, \dots, D_n$を生成しそれぞれを参加者に配布する．復元段階では，分散情報を$k$個以上集め，計算を行い秘密情報を復元する．また，$(k,n)$閾値秘密分散法は$k-1$個以下の分散情報からは秘密情報に関する情報が一切得られないという特徴を持つ．

### 2.2 Shamir の$(k,n)$閾値秘密分散法

$(k,n)$閾値秘密分散法としては，有限体上の多項式を分散式として用いる Shamir の$(k,n)$閾値秘密分散法が代表的である．この方法は次の補間定理に基づいている．

**定理 2.1** 二次平面上に異なる$x$を持つ$k$個の点$(x_1,y_1),(x_2,y_2),\dots,(x_k,y_k)$が与えられたとき，すべての$i$に対して$f(x_i)=y_i$を満たすような$k-1$ 次多項式$f(x)$が唯一つ存在する．

Shamir の$(k,n)$閾値秘密分散法の構成を次に示す．

【分散段階】
1. 秘密情報$S$に対して素数$p$を選ぶ．以後の計算は GF($p$)で行う．
2. $k-1$次多項式
   $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1}$
   の係数$a_0=S$として，$a_1,a_2,\dots,a_{k-1}$をランダムに選ぶ．
3. 分散情報$D_i=\big(i,f(i)\big), i=1,\dots,n$として参加者に分配する．

【復元段階】
1. 分散情報を$(t\geq k)$個集める．
2. 多項式補間により定数項$a_0=S$を求める．

### 2.3 カメラ撮影画像を用いた VSS scheme

画像に対する秘密分散法は，最初 1994 年に Naor と Shamir によって提案された．

彼らの方法は 2 つの分散画像を重ねあわせることで秘密画像を復元するというものである．この方法において分散画像はランダムな 2 値画像の模様であり，秘密画像は$(k,n)$閾値秘密分散法に基づいて分散画像を重ねあわせることで視覚的に見えるようになる．

2 値で表現された秘密画像から視覚復号型秘密分散法を用いて生成した 2 枚の分散画像をそれぞれ電子媒体と紙媒体で保持し，紙媒体に印刷した分散画像をカメラで撮影することで秘密画像を視覚的に復元する方法が中間らによって提案されている[2].



Copyright © 2015 by Information Processing Society of Japan and
The Institute of Electronics, Information and Communication Engineers
All rights reserved.

この手法の問題点として，VSS scheme の特徴から，

- 2 値画像しか扱えない
- 復元された画像が元の秘密画像と比較して黒味がかった画像になる
- 分散画像と復元された秘密画像が，元の秘密画像と比較して縦横の大きさがそれぞれ 2 倍になってしまう

という点が挙げられる．

これらの点を改善するため，本研究では 3 節にて述べる Shamir の$(k,n)$閾値秘密分散法を用いた VSS scheme の方法を検討した．

## 3. Shamir の$(k,n)$閾値秘密分散法によるカメラ撮影画像を用いた秘密分散法

本節では Shamir の$(k,n)$閾値秘密分散法による方法を提案する．提案手法では $p$ 階調の秘密画像を扱うことを考える．ここで $p$ は素数である．

### 3.1 提案手法の構成

提案手法は従来手法[2]と同じく分散段階と復元段階に分けられる．分散画像は電子媒体と紙媒体の 2 枚を保持するため，(2,2)閾値秘密分散法を用いる．

【分散段階】

入力：$m \times m$の秘密画像$S$（$p$ 階調の濃淡画像とする）

出力：2 枚の$m \times m$の分散画像$I_k(k = 1,2)$

方法：

1. 以下，全ての作業は GF$(p)$で行われる．
   秘密画像$S$の各画素値を$s_{i,j}$とする．$s_{i,j}$それぞれについて，1 次多項式
   $$F_{i,j}(x) = s_{i,j} + a_{i,j} \times x \bmod p$$
   を生成する．係数$a_{i,j}$は法$p$のもとでランダムに決定され，画素ごとに値は決定される．$x_k$を分散画像の評価点として選び，$x_1 \neq x_2$となるように値を選ぶ．
   生成した$F_{i,j}(x_k)$の値を分散画像$I_k$の画素値とし，この作業を全ての画素に対して行うことで分散画像$I_k$を生成する．
2. 生成した分散画像$I_k$の 1 枚を電子端末に，もう 1 枚を紙媒体に保存する．
   この際，次の復元段階に述べるカメラ撮影画像の補正の精度を上げるために，画像に黒枠をつけて出力する．

【復元段階】

入力：電子端末に保存された分散画像$I$とグレースケールで撮影されたカメラ画像$J$

出力：復元された秘密画像$S'$

方法：

1. カメラ撮影画像から復元の対象となる部分の画像を抽出する．抽出方法は以下の図 3.1 に示す．図 3.1(a)が歪んだカメラ撮影画像として，斜線部が復元の対象となる部分とする．画像を補正するために，まず歪んだ画像から Hough 変換を用いて 4 つの辺を抽出する．画像から直線を抽出した結果が図 3.1(b)のようになる．4 本の直線が斜線部を正しく囲むことができれば，直線の交点を求めることで 4 つの頂点の座標を得ることができる．4 つの頂点が分かれば，対応する点を比例関係で求めることができ，図 3.1(c)のように補正される．

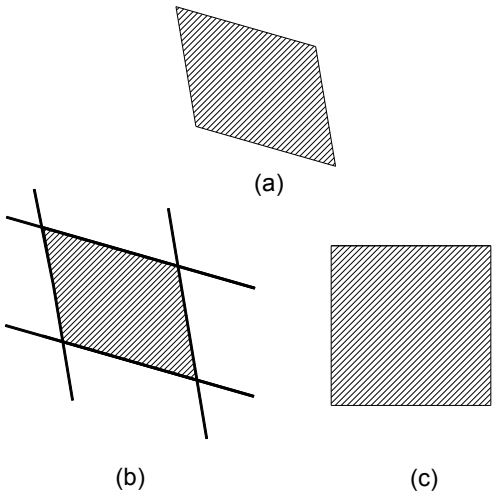



**図 3.1 カメラ撮影画像の補正**

2. 画像の補正後，各画素値を読み込み，その値と電子媒体に保存してある画像を用いて秘密画像 $S'$ を復元する．秘密画像 $S'$ の各画素値 $s'_{i,j}$ はラグランジュ補間を用いて
   $$s'_{i,j} = I_{i,j}\frac{x_2}{x_2 - x_1} + J_{i,j}\frac{x_1}{x_2 - x_1} \bmod p$$
   の式から復元する．ここで $x_1, x_2$ はそれぞれ分散画像 $I, J$ の評価点とする．

### 3.2 提案手法の実例

提案手法の実例を示す．以下では，秘密画像 $S$ はもともと 256 諧調の濃淡画像を用意し実験を行った．GF$(p)$ で作業するため，秘密画像内に現れる画素値の最大値を $p-1$ となるように変換する．以下の数式に基づいて画素値を変換した．秘密画像 $S$ の各画素値を $s$ とすると

$$s < 256/p \times (i+1) \qquad (i = 0,1,\dots,p-1)$$

を満たす最小の $i$ の値を秘密画像 $S$ の画素値 $s$ に置き換える． 256 諧調をそのまま使う場合は拡大体を使えばよい．

ここではそれぞれパラメータを $p = 7$，$x_1 = 1$，$x_2 = 2$ として，用いる元画像は図 3.2 に示す大きさ 64×64 ピクセルの画像とし，上数式を用いて画素値を変換した秘密画像が図 3.3 となる．

復元画像の品質の尺度としてピーク信号対雑音比(Peak signal-to-noise ratio：PSNR[3])を使用する．PSNR の定義はモノクロの 2 枚の $m \times n$ の画像 $I$ と $K$ において，MSE(平均二乗誤差)を以下とした場合，

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

となり，PSNR の定義は，

$$PSNR = 10 \times \log_{10}\frac{MAX_I^2}{MSE}$$



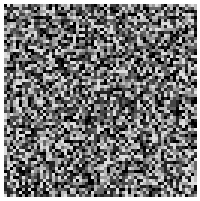
Copyright © 2015 by Information Processing Society of Japan and
The Institute of Electronics, Information and Communication Engineers
All rights reserved.

となる．ここで$MAX_I$は画像が取りうる最大のピクセル値である．

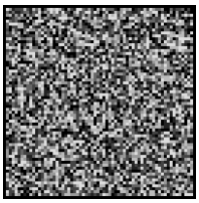
図 3.3 の秘密画像から作成した分散画像は，電子媒体に保存する画像が図 3.4(a)，紙媒体に保存する画像が図 3.4(b)となる．

図 3.2 原画像

図 3.3 秘密画像



(a)分散画像 1



(b)分散画像 2

図 3.4 分散後の画像

紙媒体に保存された図 3.4(b)の画像をカメラで撮影した画像が図 3.5 となり，補正後の画像が図 3.6 となる．この図 3.6 と電子媒体に保存した図 3.4(a)の 2 枚の画像を用いて復元した画像が図 3.7 となる．

図 3.5 カメラ撮影画像

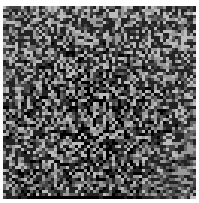


図 3.6 補正画像

図 3.7 復元画像

図 3.7 を見ると環境光などによりノイズが混ざっているが，秘密画像が復元されていることが視覚的に確認できる．PSNR の値は 15.2774dB となった．

### 3.3 環境光による影響に対する補正

前節で示したように，カメラ撮影時に環境光の影響を受けた場合，正しく各画素値を正しく読み込めなくなり，ノイズが含まれることになる．

実際に環境光の影響を受け，画像全体が明るくなったカメラ撮影画像を用いた復元結果を以下に示す．図 3.8 が補正画像で図 3.9 が復元画像となる．図 3.9 を見てもノイズが多く，視覚的に復元できたとはいえず，PSNR も 7.80917dB となった．

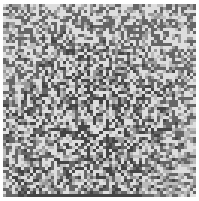


図 3.8 補正画像

図 3.9 環境光の影響を受けた復元画像

解決策としてカメラ撮影画像を補正する際にヒストグラムを用いた画素値の補正手順を検討した．

ヒストグラムの値は携帯電話に分散情報とともに保存されていると仮定する．

すなわち，秘密画像から 2 枚の分散画像を生成する際，紙媒体に保存する分散画像のヒストグラムを取得する．このヒストグラムの値は電子媒体に記憶させておき，カメラ撮影画像を読み込んだ際にカメラ撮影画像が元の分散画像のヒストグラムと等しくなるよう補正を行う．

ここでは研究の第一段階としてヒストグラムの補正を以下のような簡単な手順で行った．

【ヒストグラムを用いた補正】

入力：256 階調のカメラ撮影画像 $I$，分散画像のヒストグラム

出力：$p$ 諧調の濃淡画像 $I'$

方法：

1. 初期値$\alpha = 0$，$s = 0$，count $= 0$とおく．ここで$\alpha = 0, \cdots, p-1$のときヒストグラムはそれぞれ値を持ち，$s = 0, \cdots, 255$は$I$の画素値とする．
2. $\alpha$の値のヒストグラムの値が 0 の場合，$\alpha$に 1 を加える．$\alpha = p$であれば画像$I$を画像$I'$として出力し，この補正手順を終了する．そうでなければ手順 3 に移る．
3. 画像 $I$ から画素値が $s$ の画素をすべて探し出し，その画素の画素値を $\alpha$ にすべて置き換えた画像を再び画像 $I$ とする．$\alpha$に置き換えた画素数を count に加える．
4. count の値がヒストグラムの画素値$\alpha$の値を超えていれば$\alpha$と$s$に 1 を加え，count $= 0$とし手順 2 に戻る．そうでなければ$s$に 1 を加えて手順 2 に戻る．

図 3.8 にこの補正を適用した補正画像が図 3.10 となる．図 3.10 を用いて秘密画像を復元すると図 3.11 が得られる．



Copyright © 2015 by Information Processing Society of Japan and
The Institute of Electronics, Information and Communication Engineers
All rights reserved.

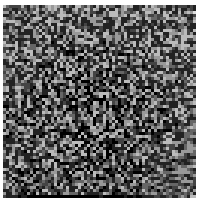


図 3.10 ヒストグラムを用いた方法による補正画像

図 3.11 復元画像

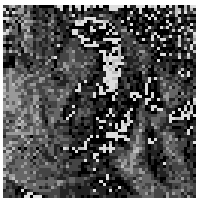
図 3.11 を見ると，ノイズが混ざっているが秘密画像が復元されていることが視覚的に確認できる．PSNR の値は 14.3341dB となり，図 3.8 の結果と比べ復元の精度が上がっていることが確認できる．

同様に他の画像を用いた結果を以下に示す．

(a)

(b)

図 3.12 秘密画像



(a)

(b)

図 3.13 環境光による影響を受けた復元画像

(a)

(b)

図 3.14 環境光による影響に対する補正を施して復元した復元画像

表 3.1 に環境光による影響に対する補正を行ったときと行わなかったときの復元画像の PSNR 値を示す．

以上の結果から環境光の影響を受けたカメラ撮影画像に対してヒストグラムを用いた補正を行うことで，復元の精度を上げることができる．

### 3.4 階調数を増やした場合の復元精度

ここではそれぞれパラメータを $p = 13$，$x_1 = 1$，$x_2 = 2$ として，$p = 7$のときに用いた原画像を秘密画像とした場合の復元結果を表 3.2 にまとめる．カメラ撮影画像には前節で述べたヒストグラムによる補正方法を適用した．

表 3.1 環境光の影響を受けた画像を用いた復元画像の PSNR 値

| 用いた秘密画像 | 補正を行わない場合の画像と PSNR 値 | 補正を行った場合の画像と PSNR 値 |
|---|---|---|
| 図 3.2 | 図 3.8<br>7.80917[dB] | 図 3.11<br>14.3341[dB] |
| 図 3.12(a) | 図 3.13(a)<br>11.2904[dB] | 図 3.14(a)<br>21.1757[dB] |
| 図 3.12(b) | 図 3.13(b)<br>10.8061[dB] | 図 3.14(b)<br>19.7519[dB] |

表 3.2 階調数を増やした場合の復元精度

| $p = 7$の場合の PSNR | $p = 13$の場合の PSNR |
|---|---|
| 図 3.11<br>14.3341[dB] | <br>21.8164[dB] |
| 図 3.14(a)<br>21.1757[dB] | <br>19.5331[dB] |
| 図 3.14(b)<br>19.7519[dB] | <br>16.6258[dB] |

階調数を増やした場合，画素値を正しく読み込むことが難しくなり精度が下がると考えられるが，$p = 13$では PSNR の変化の特徴は見られなかった．$p$の値をさらに増やして PSNR の変化を調べ，PSNR が増減した画像の特徴や原因について調べることを今後の課題としたい．

## 4. おわりに

本研究ではカメラ撮影画像における秘密分散法に Shamir の$(k, n)$閾値秘密分散法を用いる方法を提案した．本手法では諧調数$p$の秘密画像に対応できる．但し，カメラ撮影画像にノイズが含まれると秘密情報が得られない．この点について考察し，ヒストグラムを用いる補正を用いて，環境光などのノイズの影響を受け難くする方法を考察した．

また，本稿で示した(2,2)閾値秘密分散法では画像を直接マスクするほうが効率的と考えられる．紙の紛失や破損に対応でき，秘密分散法の特徴を生かせると考えられる$(2, n)$閾値秘密分散法への拡張を今後の課題としたい．

他の課題として，PSNR を改善するための補正方法の見直しなどノイズを抑えたり取り除く方法の検討が考えられる．また，カメラ撮影画像の正しい向きの選択ができるようにし，手軽な復元のために，携帯端末への実装を行うことが考えられる．また，ヒストグラムの利用による安全性の低下がないかどうかを検討することも今後の課題とする．

最後に，ご多忙の折，拙稿の査読の労をとっていただいた査読員の方々に感謝いたします．

### 参考文献

[1] M.Naor, A.Shamir, “Visual cryptography”, IN EUROCRYPT’94, Springer – Verlag Berlin, volume LNCS 950 , page 1-12, (1995).
[2] 中間翔太, 吉岡裕佳子, 栗野直之, 小堀研一, ”視覚復号型秘密分散法による暗号化および復号手法の提案”, 情報処理学会第 75 回全国大会, (2013).
[3] Stelvio Cimato, Ching-Nung Yang, Visual Cryptography and Secret Image Sharing , CRC Press, (2011).



Copyright © 2015 by Information Processing Society of Japan and
The Institute of Electronics, Information and Communication Engineers
All rights reserved.