L-010

雑音を考慮したカメラ撮影画像に対する秘密分散法
Secret Sharing Scheme for Noisy Camera Capture Images

福嶋 貴幸† 甲斐 博† 木下 浩二† 森井 昌克‡
Takayuki Fukushima Hiroshi Kai Koji Kinoshita Masakatsu Morii

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．

Shamir の(k,n)閾値秘密分散法[1]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カメラで撮影することで秘密画像を復元する手法を提案した[2]．しかし，提案されている手法では，カメラ撮影などに起因する雑音により，復元される秘密画像にも雑音が生じてしまう．

本研究では雑音を考慮した手法として，2 つの方法を検討する．1 つは[2]で検討したヒストグラムを用いた方法を応用し，分割ヒストグラムを用いる方法を検討する．また，画素値と画素値の距離を大きくし，雑音に耐性を持たせるため，カラー画像を用いた改良を検討し，実験により精度が向上することを示す．

2. 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

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は分散段階と復元段階に分けられる．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．この手法では 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．

【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 Hough 変換を用いて画像の 4 辺を抽出し，4 本の直線が囲む領域を抽出することでカメラ撮影画像を補正する．
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. 分割ヒストグラムデータを用いた方法

カメラ撮影時に環境光などの影響を受けた場合，正しく各画素を読み込めなくなり，ノイズが含まれることになる．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ている[2]．

本研究ではヒストグラムデータを用いた方法を応用し，カメラ撮影画像をいくつかの領域に分割し，それぞれの領域ごとにヒストグラムデータを用いた画素値の補正手順を検討した．

すなわち，紙媒体に保存する分散画像をn個の領域に分割し，それぞれの領域で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，カメラで撮影し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にn個のそれぞれの領域で，ヒストグラムを用いた以下のような補正を行う．

【分割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，n個に分割された分散画像のヒストグラム

出力：p階調の濃淡画像 I'

方法：

1. カメラ撮影画像Iをn個に分割し，$I_m(m = 0, \ldots, n)$とする．
2. 初期値$m = 0$，$\alpha = 0$，$s = 0$，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_m の画素値とする．

† 愛媛大学，Ehime University
‡ 神戸大学，Kobe University

3. αの値のヒストグラムの値が 0 の場合，αに 1 を加える．$\alpha = p$であれば画像I_mを画像I'_mとして出力し，手順 4 に移る．そうでなければ手順 5 に移る．
4. $m = n$であればn分割されたI'_mを結合し，補正画像I'を出力し終了する．そうでなければI'_mを保持しておき，手順 3 に戻る．
5. 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 α にすべて置き換えた画像を再び画像 I とする．αに置き換えた画素数を count に加える．
6. count の値がヒストグラムの画素値αの値を超えていれば α，s に 1 を加え，count = 0とし手順 3 に戻る．そうでなければsに 1 を加えて手順 3 に戻る．

ヒストグラムデータを分割しない例を示す．すなわち，それぞれパラメータを$p = 7$，$x_1 = 1$，$x_2 = 2$，$n = 1$として，用いる秘密画像は図 1 に示す大きさ64×64ピクセルの 7 階調の画像とする．

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．

ヒストグラムデータを使用せずに復元した画像が図 2(a)となり，PSNR の値は 14.8235dB となった．ヒストグラムデータを用いて復元した画像が図 2(b)となり，PSNR の値は 14.8459dB となる．

また，分割ヒストグラムデータを用いた例として，それぞれパラメータを$p = 7$，$x_1 = 1$，$x_2 = 2$，$n = 4$とする．すなわち，紙媒体に保存する分散画像を 4 つの領域（大きさ32×32ピクセルの 4 個の領域）に分割したヒストグラムデータを用いて補正を行う．復元した画像は図 2(c)となり，PSNR の値は 17.3306dB に改善された．

4. カラー画像として紙媒体に保存する方法

遠藤らは QR コードに代表される二次元コードにおいての誤り訂正符号を利用した符号化変調方式による高階調度認識アルゴリズムを提案している[4]．その中で，変調における識別が困難で信頼性の高い復号を行うためには，単位平面上において，信号点同士のユークリッド距離をできる限り大きくすることが望ましいとされる．

そこで，カラー画像として紙媒体に保存することで，カメラで撮影した際，それぞれの画素値同士の色差が大きくなることから，信号点同士のユークリッド距離が大きくなり，より正しく各画素を読み込めると考えられる．

この手法で$p = 7$の手順を以下に示す．

【カラー画像を用いた補正 ： 分散段階】

入力：紙媒体に保存する前の分散画像 I，7階調のカラーテーブルT（表 1）

出力：24 ビットカラー画像 I'

方法：

1. 紙媒体に保存する分散画像を読み込む．
2. 読み込んだすべての画素値に対応する値を表 1 を参照して置き換える．
3. 全ての画素を置き換えたら 24 ビットカラー画像としてI'を出力し，紙媒体に保存する．

【カラー画像を用いた補正 ： 復元段階】

入力：256 階調のカメラ撮影画像I，7 階調のカラーテーブル T（表 1）

出力：7 階調の濃淡画像I'

図 1 秘密画像

(a)

(b)

(c)

(d)

図 2 復元画像

表 1 7 階調のカラーテーブル

変換前の画素値	変換後の画素値$[R,G,B]$
[0]	[0,0,255]
[1]	[0,255,0]
[2]	[0,255,255]
[3]	[255,0,0]
[4]	[255,0,255]
[5]	[255,255,0]
[6]	[255,255,255]

方法：

1. 紙媒体に保存された分散画像をカメラで撮影し，24 ビットカラーのカメラ撮影画像として読み込む．
2. 読み込んだすべての画素を$[r,g,b]$とすると，表 1 の変換後の各画素値$[R_i,G_i,B_i]$ $(i = 0,..,6)$とのユークリッド距離d_iは$d_i = \sqrt{(R_i - r)^2 + (G_i - g)^2 + (B_i - b)^2}$となり，それぞれの画素に対して$d_i$が最も小さくなる$i$を画素値として置き換える．
3. 全ての画素を置き換えたら補正画像として 7 階調の濃淡画像I'を出力する．

この方法を用いて復元した画像が図 2(d)となり，PSNR の値は 21.81dB に改善された．

5. おわりに

本研究ではカメラ撮影画像に対する秘密分散法における雑音を低減する方法を提案した． 2 つの手法を提案したが，これらの方法は同時に利用できる．

また，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として，遠藤ら[4]の提案する誤り訂正手法を用いての画素値の誤り訂正の検討が今後の課題として考えられる．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．

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] 福嶋貴幸, 甲斐博, 木下浩二, “カメラ撮影画像を用いた秘密分散法”, 情報科学技術フォーラム講演論文集 14(4), page 19-22, (2015).
[3] Stelvio Cimato, Ching-Nung Yang, Visual Cryptography and Secret Image Sharing , CRC Press, (2011).
[4] 遠藤祐介, 廣友雅徳, 佐治勇樹, 渡辺優平, 森井昌克, “多値二次元コードにおける高階調度認識アルゴリズムの提案”, 電子情報通信学会論文誌, J95-D(11), page 1935-1943, (2012).