L-008

カメラ撮影画像を用いた秘密分散法の RS 符号を用いたノイズ除去
Noise Reduction Using Reed Solomon Codes for A Secret Sharing Scheme of Camera Capture Images

上野　ひかり† 　甲斐　博† 　森井昌克‡
Hikari Ueno 　Hiroshi Kai 　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[1]と Blakley [4]によって独自に提案されている．

Shamir の(k,n)閾値秘密分散法 [1] の応用として，1枚の秘密画像から生成された2枚の分散画像について，1枚の分散画像を電子媒体で保管し，もう1枚の紙媒体上の分散画像をカメラで撮影して，情報を抽出することで秘密画像を復元する手法が提案されている [2] [3]．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ノイズにより，復元される秘密画像にもノイズが生じてしまう．

本研究では分散情報を読み取る際に含まれるノイズを考慮した手法として，[3] で用いられた 7 階調のグレースケールの分散画像を，カラー画像として紙媒体に印刷にする手法を用いる．さらに リードソロモン符号（RS 符号）を用いた方法を検討し，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 [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 [2] 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 階調のグレースケール画像とする）

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
   $$F_{i,j}(x) = s_{i,j} + a_{i,j} \times x \mod p$$
   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枚を電子媒体に，もう1枚を紙媒体に保存する．

【復元段階】

入力：電子媒体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

手法：

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．抽出方法は画像の2値画像を作成し，その画像に対して Hough 変換を行うことで抽出する．
2. 画像の補正後に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を復元する．秘密画像の各画素値は連立方程式から得られる以下の式により求めることができる．
   $$s_{i,j} = F_{i,j}(x_1) - \frac{F_{i,j}(x_1) - F_{i,j}(x_2)}{x_1 - x_2} x_1$$
   ここでの$F_{i,j}(x_1)$，$F_{i,j}(x_2)$はそれぞれの分散画像I，Jの評価点とする．

紙媒体で分散画像を保管する上で，紙媒体の劣化や破損によって復元した秘密画像にノイズが混入することが問題となっており，ヒストグラムを用いた方法や紙媒体をカラー化して保存する方法などが提案されている．しかし，完全にノイズを除去することができていない．

そこで，本論では RS 符号および紙媒体への保存でカラー画像を用いることで，紙媒体を撮影する時に混入するノイズを除去することを検討する．

3. RS 符号を用いた提案手法

紙に印刷する分散画像に対し K 画素ごとに (N,K) RS 符号を適用することを考える．

例えば，$m = 64$ の分散画像に対して，p 諧調の64画素ごとに GF(2^6) 上の (63,55) RS 符号を短縮した (40,32) RS 符号を適用することを考える．ただしここで$p < 2^6$とする．

例えば $p = 7$ の場合， 64×64 の分散画像の各画素値は 7 諧調のため，各画素値は 3 ビットで表現できる．各画素値を GF(2^6)上で符号化する時に，本研究では，2 つの（隣り合う）画素をまとめて 6 ビットとすることを行う．つまり 64 画素を 32 シンボルで表現し，上述の (40,32) RS 符号で符号化することを行う．

符号化の結果，64×40 の GF(2^6) 上の値が得られるが，これを紙に印刷する際に，6 ビットで表現された各シンボルを 2 つの 3 ビットの値に分割し，64×80 の 8 諧調画像で表現することを行う．

以上の例をまとめると，7 諧調64×64の分散画像は，(40,32) RS 符号化され 64×80 の印刷用の画像に変換される．この印刷された画像をカメラで撮影することにより，各画素値を読み取り，誤り訂正を行った上で，得られる秘密画像のノイズを低減させることを検討する．

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

4. RS 符号を用いた提案手法の実験

本研究では$m = 64, p = 7, x_1 = 1, x_2 = 2$ として，前節で説明した (40,32) RS 符号を用いる．その結果，印刷する分散画像は 64×80 の 8 諧調の画像が得られる．

ここで論文 [3] で述べたカラー化を行う手法を用いて，画素値と画素値の間のユークリッド距離を大きくすることを行い，各画素を読み取ることを簡単にする操作を加える．

本研究では 8 階調の分散画像を表 1 のカラーテーブルに従って，24bitのカラー分散画像に変換して分散画像の印刷を行う．

表１　8 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	[0,0,0]
1	[[255,0,0]
2	[0,255,0]
3	[0,0,255]
4	[255,255,0]
5	[0,255,255]
6	[255,255,255]
7	[255,0,255]

実験では図 1 の64×64の7諧調画像を秘密画像として用いる．

図１　秘密画像

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 [5])を使用する．

図 1 の画像に対して上で述べた手法を使い分散画像を作成する．それを紙に印刷後，あまり環境光の影響を受けない室内で撮影し，秘密画像の復元を試みたところ，もとの秘密画像と同じ画像が得られた．文献[2]では 2 節で述べた手法を用いた場合，図 1 について PSNR の値は 15.28dB となっており，本手法により大きな改善ができていることがわかる．

また紙の折れ（図 2 の撮影画像において黒い太線で強調した線は折れ目の位置である）や環境光による影響について図 3 を用いて以下の 2 種類の実験を行った．

- 実験 1: 分散画像が保存されている紙媒体に縦横4本ずつ折り目を付けて部分的にノイズが乗るようにして撮影し(図 2 左)，本手法で実験を行う．
- 実験:2: 外で撮影することにより環境光を室内よりも広範囲に多く混入させて撮影し(図 3 左)，同様に実験を行う．

実験 1 の結果としては，各行に部分的なノイズが含まれたものの，最大でも誤りの数が (40,32) RS 符号が訂正可能な 4 以下であった．その結果，図 2 に示すように，原画像と同じ画像を得ることができ，部分的なノイズに強いことが確認できた．

実験 2 の結果では，図 3 に示すように環境光の影響が大きい下辺にノイズが多くのることが問題になる．画像の PSNR 値は24.81dBであり，さらに改良を加える必要がある．

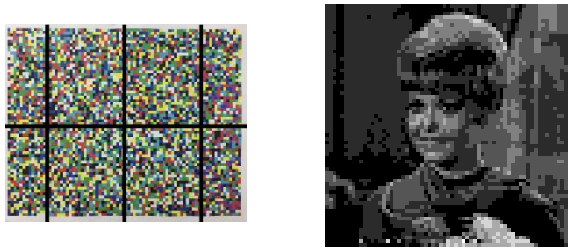

図２　部分的にノイズを含む撮影画像とその画像から得られた秘密画像

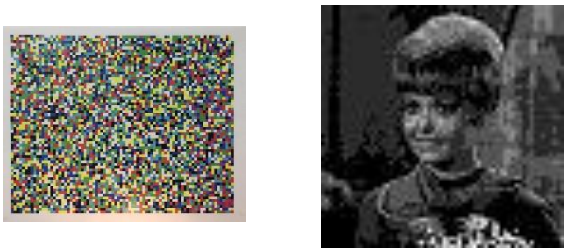

図３　広く環境光の影響がみられる撮影画像とその画像から得られた秘密画像

5. おわりに

本研究では先行研究であるカメラ撮影画像における秘密分散法に RS 符号を用いた方法を提案した．本研究は階調数 p の秘密画像に対応でき，分散して混入したノイズであれば除去できるため，高画質の画像を得ることができる．

しかし，撮影時に広い範囲でノイズが混入した場合に対しては PSNR 値の高い秘密画像が得られないため，この点については文献[2][3]で用いたようなヒストグラムを用いた補正や符号化のときのシンボルの取り方を変えるなどの検討が必要である．

参考文献

[1] A.Shamir, “How to share a secret”, Communications of the ACM, Volume 22 Issue 11, pp. 612-613 , (1979)
[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”, 第 14 回情報科学技術フォーラム講演論文集 14(4), pp. 19-22, (2015)
[3] 福嶋貴幸, 甲斐博, 木下浩二, 森井昌克, “雑音を考慮したカメラ撮影画像に対する秘密分散法”, 第 15 回情報科学技術フォーラム講演論文集, pp. 1-2, (2016)
[4] G.R. Blakley, Safeguarding cryptographic keys, Proceedings of the National Computer Conference 48, pp.313–317, (1979).
[5] Stelvio Cimato, Ching-Nung Yang, Visual Cryptography and Secret Image Sharing, CRC Press, (2011).