1T-6

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

中間　翔大†　　吉岡　裕佳子†　　栗野　直之†　　小堀　研一†

†大阪工業大学

1. はじめに

近年，情報化社会の発展に伴い，重要な情報をコンピュータによって管理する機会が増えている．しかし，コンピュータによる管理では，情報が漏洩し，第三者に悪用されるリスクを伴う．そのため，情報を暗号化して管理する技術が注目されている．

情報を暗号化するための技術の一つに視覚復号型秘密分散法(VSSS)[1]がある．VSSS とは，重要な情報が含まれている画像を複数の画像に暗号化し，その暗号化した画像を重ね合わせることで視覚的に情報を復号できる技術である．一般に，紙のみを利用して復号する手法であるが，近年では紙の代用としても広く普及している電子端末を利用することで，その用途が広がると考えられる．

本研究では，2 値やグレースケール画像から暗号化した二枚の画像を電子媒体と紙媒体で一枚ずつ保持する．そして，紙媒体上の暗号画像をカメラで撮影し，もう一枚の暗号画像を撮影画像に対して自動で重ね合わせるようにすることで，電子媒体上で復号する手法を提案する．提案手法では，撮影画像から暗号画像の角にあたる頂点を検出し，重ね合わせる向きを決定することで，正しい復号結果を得る．これにより，撮影する方向や角度に依存せずに復号できるようにする．

2. 提案手法

2.1 概要

提案手法では，2 値やグレースケールで表現された秘密画像から二枚の分散画像を作成する．そして，作成した分散画像を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号する．以後，電子媒体で保持する分散画像を鍵画像とし，紙媒体で保持する分散画像を暗号画像とする．

2.2 暗号化

提案手法では，従来手法[1]から，図 2.1 に示す白画素と黒画素の数が同数である 6 種類の画素パターンを用いて暗号化する．2 値画像とグレースケール画像を暗号化する手順をそれぞれ 2.2.1 項と 2.2.2 項で述べる．

2.2.1 2 値画像

2 値画像の暗号化の手順を説明する．暗号化は画素ごとに行う．

画素を暗号化する際の手順を，図 2.2，2.3 を用いて説明する．まず，白画素の場合は図 2.2(a)の画素を同図(b)に示すように 4 分割する．そして，図 2.1 の画素パターンからランダムで 1 種類を決定し，暗号画像の画素とする．そして，図 2.2(c)のように暗号画像と鍵画像の画素に同じ画素パターンを配置することで暗号化し，重ね合わせると同図(d)のように白画素が含まれるようにする．黒画素の場合は，図 2.3(c)のように暗号画像と鍵画像に黒画素の位置が反対の画素パターンを配置することで暗号化する．これを重ね合わせることで，同図(d)のように全ての画素が黒画素となる．この処理を全ての画素に対して行うことで画像を暗号化する．

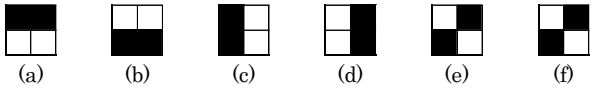


図 2.1　画素パターン

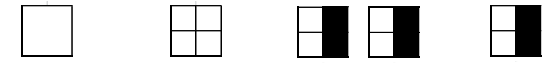


図 2.2　白画素の場合

図 2.3　黒画素の場合

2.2.2 グレースケール画像

グレーススケール画像の暗号化の手順について説明する．グレースケール画像は，ハーフトーニングの手法の一つである誤差拡散法[2]を用いることで，濃淡を表現した 2 値画像に変換する．そして，変換した 2 値画像を 2.2.1 項で示した手順で暗号化する．

2.3 復号手法

提案手法で復号する際の処理フローを図 2.4 に示す．まず，取得したカメラ画像から，暗号画像の角にあたる頂点を検出する．次に，検出した頂点を用いて，暗号画像と鍵画像の画素の対応付けを行う．最後に，暗号画像と鍵画像の重ね合わせる向きを決定することで，正しい復号結果を得る．なお，暗号画像を撮影する際は，カメラ画像の中心が暗号画像の中に含まれるようにする．

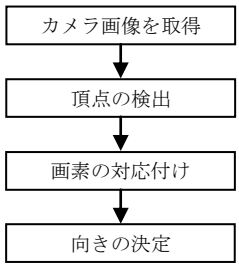


図 2.4　処理フロー

2.3.1 頂点の検出

提案手法では，取得したカメラ画像から，図 2.5 の丸で

A Study on Visual Cryptography
Shota Nakama† , Yukako Yoshioka†, Naoyuki Awano† and Ken-ichi Kobori†
†Osaka Institute of Technology

示す暗号画像の4頂点を検出する．頂点検出の流れを図2.6に示す．

まず，取得したカメラ画像を 2 値化し，同図(a)を得る．そして，同図(a)の黒画素に対して膨張・収縮処理を行うことで，暗号画像を黒画素で塗りつぶした同図(b)を得る．次に，同図(b)から暗号画像の輪郭のみを抽出するため，膨張・収縮した画像からエッジを抽出した同図(c)を得る．最後に，画像の中心から最も近い白画素のエッジをたどることで，暗号画像の輪郭として抽出した同図(d)を得る．そして，抽出した輪郭の角を暗号画像の頂点として検出する．

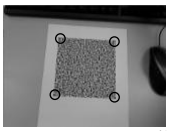


図 2.5　カメラ画像

(a)2 値化　(b)膨張・収縮　(c)エッジ抽出　(d)輪郭抽出

図 2.6　処理手順

2.3.2　画素の対応付け

取得した暗号画像は，撮影するカメラの位置によって歪んだ形となる．そのため，暗号画像と鍵画像を重ね合わせるために，歪みを補正する．提案手法では，射影変換の際にバイリニア補間を用いることで補間する．

暗号化の際は，図 2.1 のパターンを用いているため，2×2 画素ごとの黒画素と白画素の画素数が同数となる．そのため，補正後の暗号画像に対して，2×2 画素ごとに走査し，4 つの画素から画素値が大きい 2 画素に白画素を，残り 2 画素に黒画素を割り当てる．この処理により，補正の精度を向上させる．

2.3.3　向きの決定

正しい向きで暗号画像と鍵画像を重ね合わせなければ，画像を復号できないため，重ね合わせる向きを決定できるようにする．

重ね合わせる向きとして，鍵画像を 90 度ずつ回転させた 4 種類の向きが考えられる．そこで，各向きにおいて，暗号画像と鍵画像を重ね合わせた際に黒画素となる画素数を算出する．そして，4 種類の向きにおける黒画素数の平均と各向きの黒画素数の差が最も大きい向きを正しい向きとする．

3.　実験と考察

提案手法により，秘密画像を視覚的に復号できることを検証するため，解像度が 1600×1200 の Web カメラを用いて実験を行った．実験に用いた 2 値画像とグレースケール画像を図 4.1(a)，(b)に示す．また，同図(b)を誤差拡散法により 2 値化した画像を同図(c)に示す．なお，実験に用いた画像の解像度は，図 4.1(a)が 150×150 で，図 4.2(b)が 200×200 である．

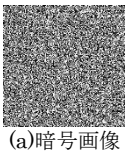
まず，同図(a)，(c)を暗号化し，作成した暗号画像と鍵画像を図 4.2，4.3 に示す．これにより，暗号画像や鍵画像単体では，元画像の情報を読み取れないことがわかる．

(a)2 値画像

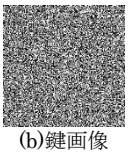
(b)グレースケール画像

(c)ハーフトーニング画像

図 4.1　実験画像

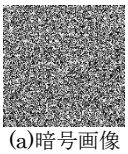


(a)暗号画像

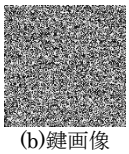


(b)鍵画像

図 4.2　図 4.1(a)の暗号化

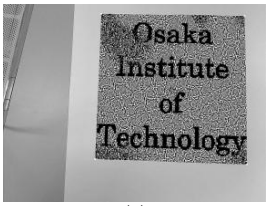


(a)暗号画像



(b)鍵画像

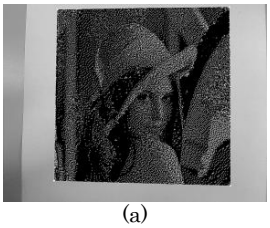
図 4.3　図 4.2(c)の暗号化



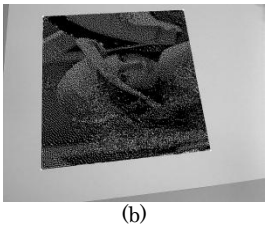
(a)

(b)

図 4.4　図 4.2 の復号



(a)



(b)

図 4.5　図 4.3 の復号

次に，図 4.2(a)，4.3(a)の暗号画像を紙に印刷し，Web カメラで撮影した結果を図 4.4，4.5 示す．図 4.4(a)，4.5(a)より，2 値画像とグレースケール画像ともに正しく復号できていることがわかる．

また，図 4.4(b)，4.5(b)より，斜めの角度から撮影した場合や異なる方向から撮影した場合でも復号できており，撮影する方向や角度に依存せず復号できていることがわかる．

4.　おわりに

本研究では，視覚復号型秘密分散法によって暗号化した画像を電子媒体と紙媒体で保持し，紙媒体上の暗号画像をカメラで撮影することで，秘密画像を視覚的に復号できる手法を提案した．

実験により，撮影する方向や角度に依存せず秘密画像を復号できることを確認した．

現在，Web カメラを用いて復号しているが，手軽に復号できるようにするために，携帯端末への移植を行うことが考えられる．

参考文献

[1]　M.Naor，A.Shamir，“Visual Cryptography”，In EUROCRYPT ‘94，LNCS950，pp.1-12，1995.

[2]　CG-ARTS 協会，“ディジタル画像処理”，CG-ARTS 協会，pp.38-40，2004.