BPCS ステガノグラフィにおける視覚的アタックを考慮した埋込み方法

新見　道治†（正員）　　野田　秀樹†（正員）
河口　英二†（正員）

An Embedding Method Considering a Visual Attack of BPCS-Steganography

Michiharu NIIMI†, Hideki NODA†, and
Eiji KAWAGUCHI†, *Members*

† 九州工業大学工学部，北九州市
Faculty of Engineering, Kyushu Institute of Technology, 1–1 Sensui-cho, Tobata-ku, Kitakyushu-shi, 804–8550 Japan

あらまし　BPCS ステガノグラフィにおける視覚的アタックを考慮した埋込み方法を示す．BPCS ステガノグラフィの運用形態によっては，秘密データ以外にもコンジュゲートと呼ばれる演算の有無（フラグ）を記録した情報を画像中に埋め込む必要がある．複雑さを利用した領域分割により秘密データは埋め込めるが，そのフラグは固定領域にしか埋め込むことができない．このため，ビットプレーン上に不自然なパターンが発生してしまい，視覚的な観測により容易に埋込み痕跡を検出されてしまう．本論文では，複雑さを利用した領域分割によりすべての情報（秘密データとフラグ）を画像中に埋め込む方法を提案する．

キーワード　ステガナリシス，視覚的アタック，ステガノグラフィ，複雑さ，コンジュゲート演算

1. まえがき

ステガノグラフィ（steganography）とは，重要な情報を何気ないデータ中に隠ぺいし，通信の存在そのものを秘匿する技術である．BPCS ステガノグラフィ [1] は，大量の秘密データを濃淡やフルカラーの可逆符号化画像データ中に埋め込むことができる．

ステガノグラフィに対しステガナリシス（steganalysis）とは，埋込みの事実を検出したり，埋め込まれた情報を取り出したり，あるいは壊したりする技術である [2]〜[4]．ステガナリシスの一つに，画像データを視覚的に観測することにより埋込み痕跡を検出する視覚的アタック（visual attack）[2] と呼ばれる方法がある．痕跡が検出しやすいような画像データの一部分を表示し，不自然な個所を人間の視覚により検出することで秘密データの存在を特定する．

本論文では，BPCS ステガノグラフィにおける視覚的アタックを考慮した埋込み方法を提案する．まず，コンジュゲート演算 [1] の有無を記録した情報を画像中に埋め込む場合，その埋込み痕跡が視覚的に検出可能であることを示す．そして，その情報を画像全体に分散させることにより，視覚的アタックに対してよりロバストな埋込み方法を提案する．

なお，BPCS ステガノグラフィは濃淡及びフルカラーの可逆符号化画像データだけでなく，限定色カラー画像 [5], [6]，ウェーブレット圧縮画像 [7]，JPEG2000 [8] や 3D SPITH データ [9] に対しても適用可能である．

2. BPCS ステガノグラフィの概要

BPCS ステガノグラフィでは，2 値画像がノイズ状であるか否かの判定を，2 値画像の複雑さに基づいて行っている．2 値画像（画素値は 0 または 1 とする）の複雑さの尺度として，2 値画像の境界線の長さを用いている．$m \times m$ 画素の 2 値画像 P において，その境界線の全長が k のとき，P の複雑さ α を次式で定義する．

$$\alpha(P) = \frac{k}{2m(m-1)}, \quad 0 \leqq \alpha \leqq 1$$

ここで，$2m(m-1)$ は市松模様のときに得られる境界線の長さである．

BPCS ステガノグラフィによる情報埋込み処理は，以下の手順で行われる．

（1） N bit/pixel の濃淡画像をビットプレーン分解して，N 枚の 2 値画像を得る．ビットプレーン分解はグレイコードを利用した方が，視覚的影響が少ない [1]．

（2） 各 2 値画像を $m \times m$ 画素の小画像に分割する．小画像の複雑さ α が，しきい値 α_{TH}（$0 \leqq \alpha_{TH} \leqq 0.5$）以上のとき，小画像はノイズ状と判断され，埋込み用の場所となる．

（3） 秘密データを $m \times m$ ビットごとの小ブロックに分割する．小ブロック内の各ビット情報を，画素値に対応させると $m \times m$ 画素の 2 値画像が得られる．この 2 値画像を埋込み用 2 値画像と呼ぶ．埋込み用 2 値画像の複雑さが α_{TH} よりも小さいときは，コンジュゲート演算 [1] によって複雑にする．コンジュゲート演算は，2 値画像と市松模様画像との画素ごとの排他的論理和演算である．コンジュゲート演算前後の画像の複雑さ，α，α^* の間には，$\alpha^* = 1 - \alpha$ の関係がある [1]．

（4） 順次，ノイズ状の小画像を埋込み用 2 値画像と置き換えていく．埋込み用 2 値画像がコンジュゲート演算を受けたか否かの情報（本論文では，コンジュゲーションフラグと呼ぶ）を記録しておく．

埋め込まれた情報の抽出は，複雑さのしきい値 α_{TH} とコンジュゲーションフラグをもとに，埋込みと逆の手順で行われる．

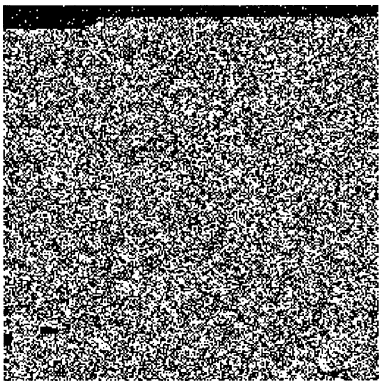
3. 視覚的観測による埋込み痕跡検出

秘密鍵暗号システムでは，秘密鍵により秘密データが暗号化され，その暗号化されたデータは秘密鍵により復号化される．このようなシステムでは，秘密鍵のみで暗号化及び復号化が可能である．ステガノグラフィは秘密鍵暗号システムとして考えることができ，BPCS ステガノグラフィではしきい値を秘密鍵として利用できる．ある定められたしきい値により埋込みを行うと，コンジュゲーションフラグ情報が生成される．コンジュゲーションフラグは，小画像サイズ，秘密データ及びしきい値により変化する．埋め込まれた情報を抽出するためには，しきい値とコンジュゲーションフラグが必要である．秘密鍵暗号システムでは，秘密鍵のみで暗号化及び復号化が可能であり，そのような利便性を BPCS ステガノグラフィに求めた場合，コンジュゲーションフラグは画像中に埋め込む必要がある．しかしながら，コンジュゲーションフラグは秘密データと同様に複雑さのしきい値処理を利用して埋め込むことはできない．なぜなら，コンジュゲーションフラグが埋め込まれた小画像に対して，更にコンジュゲーションフラグが必要になるからである．したがって，コンジュゲーションフラグは画像中の固定領域に埋め込むことになる．

コンジュゲーションフラグを画像中に埋め込む方法はいくつか考えられる．最も単純な方法では，LSB（Least Significant Bit）プレーンに画像データ中の全小画像分のコンジュゲーションフラグを保存できる領域を確保し，そこにコンジュゲーションフラグを埋め込む．濃淡表現された画像データでは，LSB の変化は視覚的にほとんど識別できないので，見た目を損なうことなく埋め込むことが可能である．しかしながら，LSB プレーンのみ観測すれば，不自然な領域を容易に検出できる．例えば，GIRL（256×256，8 bit/pixel）に対して，$m = 8$，$\alpha_{TH} = 46/112$ とし，ノイズ状と判断された小画像すべて（画像データの約 31%）をノイズ状データで置換した．その結果を図 1 に示す．

図 1 より，LSB プレーンの上方に特異なパターンが現れているのが分かる．一般に，このようなパターンは自然画像には現れないため，視覚的な観測により BPCS ステガノグラフィの埋込み痕跡が容易に検出できる．ただし，圧縮技術や M 系列，乱数系列との排他的論理和を用いることにより，図 1 (b) の上方のパターンはランダムなパターンに変形できる．しかしながら，そのような場合でも，複雑さのしきい値処理を利用していないため，簡単な領域が複雑なパターンで置き換わる可能性がある．つまり，コンジュゲーションフラグを固定領域に埋め込むと，複雑な領域が簡単なパターンで置き換わったり，簡単な領域が複雑なパターンで置き換わったりする場合が発生し，特定の場所に不自然なパターンが現れることになり，視覚的な観測により BPCS ステガノグラフィの埋込み痕跡を検出されてしまうおそれがある．

(a) Gray scale representation



(b) LSB of (a) with Gray code

図 1 BPCS ステガノグラフィに対する視覚的アタック
Fig. 1 Visual attack to BPCS-Steganography.

4. 提 案 法

4.1 概 略

前章で述べた視覚的アタックの原因は，複雑さによる領域分割を利用せずに，コンジュゲーションフラグを埋め込む点にある．よって，複雑さによる領域分割だけで，秘密データとコンジュゲーションフラグが埋め込めれば，視覚的アタックに対してよりロバストに

なる．これを実現するために，提案法では，コンジュゲーションフラグを各埋込み用 2 値画像内に配置し，複雑さのしきい値処理を利用して埋め込む．

4.2 視覚的アタックを考慮した埋込み抽出法

埋込み用 2 値画像を S と表記する．S のコンジュゲーションフラグを S 内に埋め込むためには，S 中の 1 画素をコンジュゲーションフラグに対応させればよい．本論文では，この画素を制御画素と呼び，その値が “1” の場合コンジュゲート演算が必要である，“0” の場合コンジュゲート演算が必要でないと定義する(注1)．

提案法では，制御画素をある値で初期化しておき，S の複雑さを計算し，その後，コンジュゲーションフラグの値を制御画素の値に設定する．この場合，制御画素の初期値，制御画素の近傍画素の値により，S の複雑さが変化し，BPCS ステガノグラフィの抽出方法により，埋め込んだデータが取り出せない場合が生じる．

まず，制御画素を「コンジュゲート演算必要（1）」と初期化した（この 2 値画像を $S_{CP=1}$ と表記する）場合を考える．コンジュゲート演算が必要ない（$\alpha_{TH} \leqq \alpha(S_{CP=1})$）場合，制御画素の値を “0” に変化させなければならない（この 2 値画像を $S_{CP=0}$ と表記する）．制御画素の値が変化することによる複雑さの変化量を $\pm\Delta$ とすれば，$\alpha(S_{CP=0})$ は，

$$\alpha(S_{CP=1}) - \Delta \leqq \alpha(S_{CP=0}) \leqq \alpha(S_{CP=1}) + \Delta$$

の範囲内に限定される．よって，複雑さが減少する場合，$\alpha_{TH} \leqq \alpha(S_{CP=0})$ を満たさない可能性がある．秘密データを埋め込んだ小画像なのに，抽出時に，秘密デーが含まれていないと判断されるため，この初期化は利用できない．

次に，制御画素を「コンジュゲート演算不要（0）」と初期化した場合を考える．コンジュゲート演算が必要な（$\alpha(S_{CP=0}) < \alpha_{TH}$）場合，制御画素を “1” に変化させなければならない．図 2 に，制御画素の値の変化及びコンジュゲート演算による複雑さの変化を示す．ここで，$C_0 = \alpha(S_{CP=0})$ とする．制御画素値の変更により複雑さが減少する場合（C_0 から左側への実線矢印），変更前と同様にコンジュゲート演算を行う領域なので問題はない．複雑さが増加する場合（C_0 から右側への実線矢印），α_{TH} 以上の値となり，コンジュゲート演算が必要ない領域に変化する場合がある．しかし，このような場合でもコンジュゲート演算は可能であり，更に，演算後の小画像の複雑さは，秘密データを含んでいる小画像と判定される領域となる．しかし，しきい値が 0.5 に非常に近づくと，複雑さが増加する場合に問題が生じる．

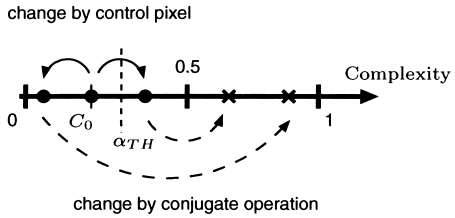


図 2 しきい値と複雑さの変化
Fig. 2 Threshold and changes of complexity.

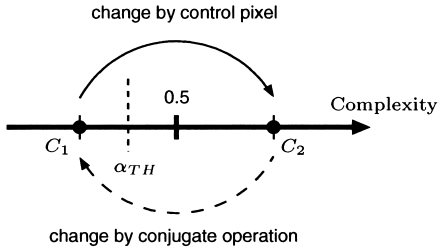


図 3 しきい値が 0.5 に非常に近い場合の複雑さの変化
Fig. 3 Changes of complexity in case that threshold is nearly equal to 0.5.

今，2 値画像内の画素を，四近傍において隣接する画素数をもとに三つのグループ X，Y，Z に分類する．グループ X は画像の四角の画素とし，グループ Y は X を含まない画像の縁の画素であり，グループ Z は X，Y 以外の画素とする．このとき，グループ X に含まれる画素に隣接する画素数は 2 であり，Y，Z はそれぞれ 3，4 である．よって，X，Y，Z それぞれに含まれる画素の値が変化することによる，境界線長の最大変化量はそれぞれ ±2，±3，±4 となる．

図 3 にしきい値が 0.5 に非常に近い場合を示す．ここで，$C_1 = 0.5 - 1/2m(m-1)$，$C_2 = 0.5 + 1/2m(m-1)$ である．しきい値を $\alpha_{TH}(0.5 - 1/2m(m-1) < \alpha_{TH} < 0.5)$ と設定し，$\alpha(S_{CP=0}) = 0.5 - 1/2m(m-1)$ とする．このとき，しきい値より複雑さが小さいので，コンジュゲート演算が必要となる．グループ X から制御画素を選んだとしても，画素値の変更により，境界線の長さは最大 2 変化するので，$\alpha(S_{CP=1}) = 0.5 + 1/2m(m-1)$ となる場合があ

(注1)：制御画素の意味を逆（制御画素が “0” の場合コンジュゲート演算が必要である，“1” の場合コンジュゲート演算が必要でない）にしても以後の議論は成り立つが，提案法を理解しやすくするために，具体的な値で定義した．

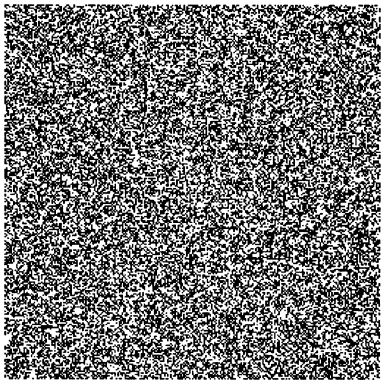


図 4　提案法に対する視覚的アタック
Fig. 4　Visual attack to the proposed method.

る（C_1 から右側への実線矢印）．この 2 値画像にコンジュゲート演算を行うと，$0.5 - 1/2m(m-1)$ となり（C_2 から左側への破線矢印），複雑さのしきい値処理で秘密情報を取り出せなくなる．よって，提案法では複雑さのしきい値を，

$$0 \leqq \alpha_{TH} \leqq 0.5 - \frac{1}{2m(m-1)} \qquad (1)$$

と限定する．このような条件を加えた場合，グループ X，Y に属する画素を制御画素として利用すれば，しきい値処理だけにより，埋め込んだデータを抽出できる．

以上より，提案法での埋込み用 2 値画像は，以下の手順により作成される．

（1） グループ X または Y に含まれる画素から制御画素を一つ選び，「コンジュゲート演算不要（0）」で初期化する．

（2） 制御画素以外を秘密データに対応させる．

（3） 複雑さを計算する．

（4） その複雑さが α_{TH} より小さい場合，制御画素の値を「コンジュゲート演算必要（1）」に変化させ，コンジュゲート演算を行う．

埋め込んだデータを復元するときは，まず，複雑さのしきい値処理で秘密データを含んだ小画像を抽出する．制御画素の値が “0” の場合は，制御画素以外の画素値が秘密データとなり，制御画素の値が “1” の場合は，小画像に対してコンジュゲート演算を行い，その結果得られる 2 値画像の制御画素以外の画素値が秘密データとなる．

提案法を利用して埋込み処理を行った場合の一例を示す．GIRL（256 × 256，8 bit/pixel）に対して，$m = 8$，$\alpha_{TH} = 46/112$，グループ X の画素を制御画素とし，ノイズ状と判断された小画像すべてをノイズ状データで置換した．図 4 は，その結果得られた濃淡画像の LSB プレーンを示す．視覚的には不自然な個所を検出できないことが確認できる．

5. むすび

BPCS ステガノグラフィにおける視覚的アタックを考慮した埋込み方法を示した．提案法では，コンジュゲーションフラグの埋込み位置を画像全体に分散させることにより，しきい値処理のみで秘密データの埋込み及び抽出を行う．これにより，視覚的アタックに対してロバストとなる．

文　献

[1] 新見道治，野田秀樹，河口英二，“複雑さによる領域分割を利用した大容量画像深層暗号化，” 信学論（D-II），vol.J81-D-II, no.6, pp.1132–1140, June 1998.

[2] P. Wayner, Disappearing Cryptography second edition:Information Hiding: Steganography & Watermarking, pp.303–314, Morgan Kaufmann Publishers, 2002.

[3] S. Katzenbeisser and F.A. Petitcolas, eds., “Information hiding: Techniques for steganography and digital watermarking,” in Computer Security, pp.79–93, Artech House, 2000.

[4] N.F. Johnson, Z.Duric, and S. Jajodia, “Information hiding: Steganography and watermarking — Attacks and countermeasures,” in Advances in Information Security, pp.47–76, Kluwer Academic Publishers, 2001.

[5] M. Niimi, R.O. Eason, H. Noda, and E. Kawaguchi, “A method to apply BPCS-steganography to palette-based images using luminace quasi-preserving color quantization,” IEICE Trans. Fundamentals, vol.E85-A, no.9, pp.2141–2148, Sept. 2002.

[6] R. Ouellette, H. Noda, M. Niimi, and E. Kawaguchi, “Topological ordered color table for BPCS-steganography using indexed color images,” 情処学論，vol.42, no.1, pp.110–113, 2001.

[7] 野田秀樹，スポールディング ジェレマイア，ヌリシラジ マハダド，新見道治，河口英二，“ビットプレーン分解ステガノグラフィのウェーブレット圧縮画像への適用，” 情処学論，vol.43, no.5, pp.1548–1551, 2002.

[8] H. Noda, J. Spaulding, M. Shirazi, and E. Kawaguchi, “Application of bit-plane decomposition steganography to JPEG2000 encoded images,” IEEE Signal Process. Lett., vol.9, no.12, pp.410–413, 2002.

[9] 古田智憲，野田秀樹，新見道治，河口英二，“3D SPIHT 符号化ビデオデータを用いた BPCS ステガノグラフィ，” 信学論（D-II），vol.J86-D-II, no.7, pp.1135–1138, July 2003.

（平成 15 年 8 月 25 日受付）