2. 画像を用いたステガノグラフィ

河口英二　九州工業大学工学部
kawaguch@know.comp.kyutech.ac.jp
野田秀樹　九州工業大学工学部
noda@know.comp.kyutech.ac.jp
新見道治　九州工業大学工学部
niimi@know.comp.kyutech.ac.jp

■まえがき

社会の情報化とネットワーク化が進み，インターネットはすでに日常生活に必須のものとなった．そして，情報セキュリティに関する社会の関心も高くなった．このような状況の中で，最近，“ステガノグラフィ(steganography)”という言葉が少しずつ広まりつつある．しかし，この言葉はまだ普通の辞書には見出し語がなく，意味がつかみにくい．本稿では画像を用いたステガノグラフィに関する一般的な解説をするとともに，筆者らの研究グループが取り組んでいる最新の研究テーマについても解説する．

■ステガノグラフィの位置づけ

人類は“他人に気付かれることなく特定の相手とこっそり情報交換できる技”を太古の昔から探し求めてきた．その願いはギリシャ時代から“steganos”という言葉で語られる特殊な技芸として位置付けられてきたそうであり，そのような時代を物語るものとして，「奴隷の頭髪を剃り上げ，頭皮に秘密のメッセージを入れ墨し，髪が伸びた後でその奴隷を敵陣に放って味方との連絡にあたらせた」との逸話は有名である．

従来からの steganography は物理化学的な現象を利用したアナログ技術であった．しかし，今日話題になりつつある steganography はディジタル・ステガノグラフィ(digital steganography)のことである．

“steganography”の日本語訳としては，“画像深層暗号”，“電子あぶり出し”，あるいは“情報迷彩”などがあるが，筆者らは一般の人にも分かりやすいように“電子あぶり出し”と呼んでいる．しかし，“ステガノグラフィ”がそのまま日本語として定着することが望ましい．

表 -1 は，2002 年 12 月中旬の段階で steganography に関連したことばを含む Web ページ数を示しており，“暗号”に比べて“ステガノグラフィ”の知名度が低いことが分かる．

ステガノグラフィと電子透かしは，しばしば混同されるディジタルデータ処理技術である．いずれも“ある情報を別の情報媒体の中に紛れ込ませる”技術であり，ともに情報ハイディング技術（information hiding）である．しかしながら，両者は目的と技術条件が正反対である（**表 -2** 参照）．このような違いを根拠として筆者らは“ステガノグラフィは電子透かしとはまったく違うものである”との立場をとっている．

ステガノグラフィを“特殊暗号”と位置づける人もいるが，暗号とはまったく別物である．暗号は第三者に

単語やフレーズ	Webページ数（概数）	検索されたページの言語
cryptography	850,000	任意の言語
digital watermark	67,500	
steganography	57,500	
暗号	201,000	日本語
電子透かし	9,800	
ステガノグラフィ	380	
画像深層暗号	63	
電子あぶり出し	89	
情報迷彩	29	

表 -1　“Steganography”に関連したことばを含む Web ページ数（2002 年 12 月，Google による）

	ステガノグラフィ	電子透かし
価値ある情報とは	外からは見えない 埋め込まれた秘密情報	外に表れた情報（画像や 音楽データなどの作品）
埋め込みデータの 頑強さ	外に見える情報に手を 加えると容易に壊れても 構わない	どのような処理をしても 壊れないこと （取り除けないこと）
埋め込みデータが 復元できるための条件	埋め込み前のダミー・データ を参照しない	埋め込み前の作品データを 参照してもよい
埋め込み容量	なるべく大きいことが 望ましい	少量の目印情報が 埋め込まれる程度でよい

表 -2　ステガノグラフィと電子透かしの違い

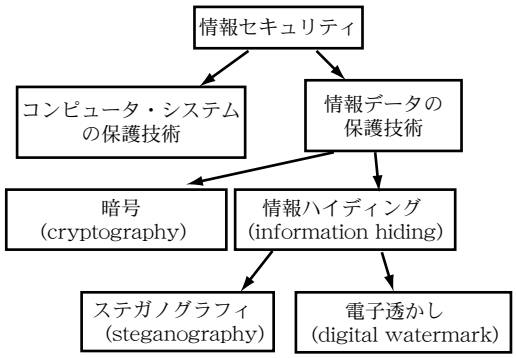

図 -1　ステガノグラフィ技術の位置付け

知られたくない情報データを“かき混ぜて（scrambling）”内容を分からなくする技術であるが，“そこに怪しげなデータが存在する”ことは隠せない．すなわち，秘密の内容は保護するが，秘密の存在を強調してしまう．

これに対してステガノグラフィとは，秘密情報を何気ない別の情報媒体に紛れ込ませて（埋め込んで），秘密の存在までも分からなくする技術である．秘密情報の埋め込み対象となる“何気ない別の情報媒体”は，“vessel”，“container”，“cover”あるいは“ダミーデータ”と呼ばれる．秘密情報を埋め込んだ後のダミー画像はステゴ画像と呼ばれることもある．秘密情報をあらかじめ暗号化しておき，それをステガノグラフィで秘匿すればきわめて強力な情報保護技術となるので，ステガノグラフィと暗号は協調できる技術である．**図 -1** は上記に従ってステガノグラフィを位置づけたものである．

■従来からのステガノグラフィ

画像に対するステガノグラフィは，画素置換型と変換領域利用型に大別できる．ここではその代表的な方法を紹介する．なお，文献 1）や，Web ページ（http://www.ipa.go.jp/security/fy10/contents/crypto/report/Information-Hiding.htm）では詳しく従来研究をサーベイしている．

◇画素置換型ステガノグラフィ

画素の一部分を直接秘密情報で置き換える手法である．基本的に，可逆画像フォーマットをカバー画像とし，大量に秘密情報を埋め込めるという特徴を持つ．

LSB ステガノグラフィは，画素の最下位ビットを秘密情報で置き換える最も単純な手法である．一般に，置換場所は画像ごとに異なる情報を利用することなしに決定される．流布しているステガノグラフィソフトウェアでは，この埋め込み法がよく使われている．

LSB ステガノグラフィを拡張し，より上位ビットまで秘密情報で置換しようとする考え方がある．しかし，どの画素でも同一の下位ビットを置換すると，画質への影響が大きくなる．そこで，ノイズ状の領域に含まれる画素にはたくさんの情報を埋め込み，そうでない画素には少量の情報を埋め込む．基本的に，ほとんどの画素置換型ステガノグラフィは，この原理に従って埋め込みを実現している．たとえば，著者らが提案した BPCS ステガノグラフィ（Bit-Plane Complexity Segmentation Steganography）[2] は，局所領域ごとに視覚的影響を考慮して，置換可能なビットプレーンを決定する．

この種の埋め込み法では，非可逆画像フォーマットに対する耐性がまったくない．

◇変換領域利用型ステガノグラフィ

基本的に，他空間に変換された情報（係数）を加工することにより秘密情報を埋め込む手法である．JPEG や JPEG2000 などの特定の変換符号化をベースとする画像フォーマット用の方法や，符号化方式に関係なく変換領域を利用する方法に大別できる．

JPEG をカバー画像とする場合，局所領域から計算された DCT 係数に秘密情報を対応させる手法が多い．この時，なるべく視覚的な損失が少ないような係数を加工する．JPEG2000 では，レイヤ構造を利用して，下位レイヤに秘密情報を埋め込むことができる [3]．この時，下位レイヤを表示しないようにすることによって高画質な

ステゴ画像を得ることができる．

特定の非可逆画像符号化に依存しない方法としては，スペクトル拡散を利用したり，秘密情報を画像として与え，それをフラクタル画像に変形したりする方法がある[4]．

一般的に，耐性と埋め込み量はトレードオフである．この種の埋め込み法では，特定の符号化に対しては耐性を持つが，埋め込める情報量が少ない．

■学会や文献，実験プログラムの公開

従来，ステガノグラフィに関する研究は，カバーデータ，画像や音声処理の一応用技術として，あるいは，暗号，セキュリティの一部として研究発表されてきた．しかしながら近年，ステガノグラフィも主要な研究分野として扱われつつある．代表的な国際的な会議としては，

- International Workshop on Information Hiding
  2002年10月に第5回目がデンマークで開催された．1.5年に1回の頻度で開催される．プロシーディングスは，Springerよりレクチャーノートとして出版される．
- Pacific Rim Workshop on Digital Steganography (http://www.know.comp.kyutech.ac.jp/STEG/)
  著者らの研究グループが主宰している．2003年7月に第2回目が九州工業大学で開催される．
- Security and Watermarking of Multimedia Contents (in Electronic Imaging)
  SPIE主催の毎年1月に開催される国際会議である．発表件数が多い．

などがある．

ステガノグラフィに関するさまざまな情報，参考文献，ソフトウェアなどはWebページ(http://www.jjtc.com/Steganography/)より入手できる．また，http://members.tripod.com/steganography/stego/software.html にもソフトウェアがアップロードされており，ステガノグラフィが手軽に楽しめる．

電子透かしと比較すると研究者人口は格段に少ないが，海外では，Ross Anderson (http://www.cl.cam.ac.uk/users/rja14/)，Fabien Petitcolas (http://www.cl.cam.ac.uk/~fapp2/)，さらにJessica Fridrich (http://www.ssie.binghamton.edu/fridrich/) などの研究者がいる．

■ BPCSステガノグラフィ

画像のビットプレーン分解と人間の視覚特性を考慮したステガノグラフィとして，BPCSステガノグラフィが提案されている[2]．BPCSステガノグラフィは，ビットプレーン分解で得られる2値画像の中で，複雑なノイズ状の領域を秘密データと置き換えるものである．これは，2つの複雑なノイズ状の2値画像は視覚的に区別することが困難であることに基づいており，秘密データを2値画像と考えたとき，それがノイズ状であることを前提としている．そうでない場合に対しては，簡単な（ノイズ状でない）パターンを可逆で複雑な（ノイズ状の）パターンに変換できる，コンジュゲート演算と呼ばれる操作が用意されている．

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値画像の複雑さの尺度として，2値画像（0と1）の境界線の長さを用いている．$m \times m$ 画素の2値画像において，その境界線の全長が k であるとき，複雑さ α は次式で定義される．

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

ここで，$2m(m-1)$ は，市松模様のときに得られる，境界線の長さの最大値である．

BPCSステガノグラフィによる情報埋め込みは，通常，以下の手順で行われる．

(1) n-bit/pixelのダミー画像をビットプレーン分解して，n 枚の2値画像を得る．
(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_0 よりも大きいとき，小画像はノイズ状と判断され，埋め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．小ブロックは，$m \times m$ 画素の2値画像となる．秘密データの小画像の複雑さが α_0 よりも小さいときは，コンジュゲート演算によって複雑にする．コンジュゲート演算は，その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[2]．
(4) 順次，ノイズ状の小画像を秘密データの小ブロックと置き換えていく．秘密データの小ブロックがコンジュゲート演算を受けたか否かの情報（コンジュゲーションマップと呼ぶ）を記録しておき，コンジュゲーションマップも秘密データと同様に埋め込む．

埋め込まれた情報の抽出は，複雑さのしきい値 α_0 とコンジュゲーションマップを基に，埋め込みと逆の手順で行われる．

■ JPEG2000圧縮画像への適用

これまで，BPCSステガノグラフィに代表されるビットプレーン分解に基づくステガノグラフィは，非可逆圧縮された画像データへの適用はできないと考えられてい

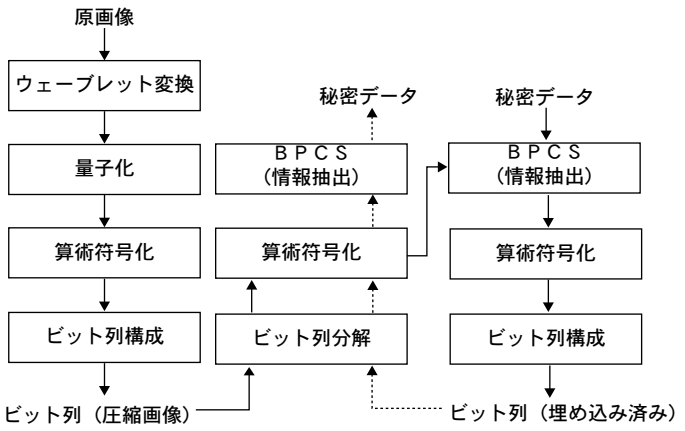

図 -2　JPEG2000 ー BPCS ステガノグラフィによる情報埋め込み，および情報抽出のブロック図

た．非可逆圧縮によってデータ値が変化すれば，抽出される秘密情報が変化することになり，非可逆圧縮が許されなかった．各種データは情報圧縮されたかたちで通信されるのが普通であることを考えると，この点は重大な問題点である．また，全般的に，圧縮データを埋め込み対象にできるステガノグラフィの例は少ない．

ここでは前述の問題点を解決するために提案された，JPEG2000 符号化と統合された BPCS ステガノグラフィ（JPEG2000-BPCS ステガノグラフィ）を紹介する．JPEG2000 符号化は，ウェーブレット変換を用いた逐次近似型の画像圧縮法である．そこでは，画像のウェーブレット係数が，ビットプレーン構造を有するかたちで量子化表現されているため，BPCS ステガノグラフィが適用可能となる．JPEG2000-BPCS ステガノグラフィによって，ビットプレーン分解を用いたステガノグラフィ技術が，情報圧縮された画像データに対して適用可能になり，ステガノグラフィの応用分野を飛躍的に向上させることができる．

■ JPEG2000-BPCS ステガノグラフィ

JPEG2000 符号化 [5] は，前処理，離散ウェーブレット変換，量子化，算術符号化，ビット列構成等から構成される（**図 -2** の左側参照）．前処理は，カラー画像等のベクトル画像におけるベクトル構成要素の変換処理を含む．離散ウェーブレット変換の後，ウェーブレット係数は量子化される．量子化の後，ROI（Region Of Interest）と呼ばれる，注目領域を優先的に処理するオプションが用意されている．量子化ウェーブレット係数は，コードブロックと呼ばれる小ブロックごとに，ビットプレーンごとに算術符号化される．その後，各コードブロックのビット列は，パケットやレイヤと呼ばれる単位にまとめられ，希望する圧縮率（ビットレート）でビット列が生成される．

JPEG2000-BPCS ステガノグラフィにおける，情報秘匿と情報抽出の手順を図 -2 に示す．JPEG2000 の有する圧縮率・画像歪み最適化機能（指定された圧縮率に対して，最も歪みの小さい復元画像を与えるビット列を生成する）を損なわないように，復号化途中の算術復号化後に情報秘匿を行う．これは，圧縮率制御が，符号化の最終段階であるビット列構成（図 -2 の左列最下段）で行われるためである．

JPEG2000-BPCS による情報秘匿は，図 -2 の実線の矢印に従って行われる．図 -2 の左列に従って，原画像は JPEG2000 符号化され，指定する圧縮率で圧縮されたビット列（圧縮画像）が得られる．続いて JPEG2000 ビット列は復号化されるが，途中の算術復号化で復号化を中断する（図 -2 の中央の列）．この時点のデータは量子化ウェーブレット係数である．その量子化ウェーブレット係数からビットプレーンを構成し，BPCS ステガノグラフィによって情報の埋め込みを行う（図 -2 の右列最上段）．情報が埋め込まれた量子化ウェーブレット係数は，再度 JPEG2000 符号化処理を受け，情報が埋め込まれた JPEG2000 ビット列が得られる（図 -2 の右列）．圧縮済みの JPEG2000 符号化画像への情報秘匿も行うことができる．その場合は，図 -2 の中央列の一番下（JPEG2000 ビット列）から処理が開始され，実線矢印に沿って前述のとおりに行えばよい．

情報が埋め込まれた JPEG2000 ビット列からの情報抽出は，図 -2 の破線矢印に従って行われる．復号化途中の算術復号化で復号化を中断する．その時点で得られる量子化ウェーブレット係数からビットプレーンを構成し，BPCS 法によって情報抽出を行う．

◇情報埋め込み実験

JJ2000 プロジェクト（http://jj2000.epfl.ch/index.html）による JPEG2000 符号化プログラムを用い，それと BPCS ステガノグラフィのプログラムモジュールを統合して，JPEG2000-BPCS ステガノグラフィを実装した．JPEG2000-BPCS ステガノグラフィを用いた情報埋め込み実験を行い，埋め込みによる劣化が知覚されなかった場合の結果を**表 -3** に示す．用いた画像は 512 × 512 画素の 3 枚の標準画像（Lena, Barbara, Mandril）である．

画像	埋め込みなし		埋め込みあり	
	圧縮率	PSNR（dB）	埋め込み率（%）	PSNR（dB）
Lena（モノクロ）	1/8	40.5	14.0	37.1
Barbara（モノクロ）	1/8	37.1	16.9	31.9
Mandrill（カラー）	1/24	25.1	15.3	23.3

表 -3　JPEG2000 圧縮画像を用いた情報埋め込み実験結果

画像は 1.0bpp に圧縮した．これは，モノクロ画像では 1/8, カラー画像では 1/24 に圧縮したことになる．埋め込みの単位となる小画像の大きさは 4 × 4 画素，秘密情報としては 2 値乱数を用いた．埋め込みに使用したプレーンは最下層から 2 つのみに限定し，複雑さのしきい値 $\alpha_0 = 8/24$ とした．提案法によると，埋め込み後の圧縮画像ファイルサイズの 15% くらいの量の情報を秘匿できることが確認された．

■ステガナリシス

ステガノグラフィの目的は主として秘匿通信に利用することである．つまり，通信の存在そのものを隠蔽する必要がある．ステガノグラフィの初期の研究では，「大量に情報を埋め込む」ことに関心が集まっていたが，近年「埋め込まれた証拠」を検出しようとする研究，ステガナリシス（steganalysis）が注目を集めている．研究事例は少ないがここでは，Fridrich らにより提案された LSB ステガノグラフィに対するステガナリシス（RS ステガナリシス）[6] を紹介する．

カバー画像として $M \times N$ の画像を考える．画素値は $P = \{0, 1, \ldots, 255\}$ をとるものとする．隣接画素の相関を表現するため，識別関数と呼ぶ実数値関数 f を定義する．f は n 個の隣接画素グループに対して定義する．つまり，画素グループを $G = (x_1, x_2, \ldots, x_n)$ とすると，$f(G)$ を以下のように定義する．

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \qquad (2)$$

ここで，flipping と呼ぶ画素値の可逆操作 F を定義する．flipping は画素値の置換操作であり，2 回施すことにより完全にもとの画素値を得ることができる操作である．つまり，

$$F(F(x)) = x, \quad \text{all } x \in P \qquad (3)$$

である．flipping 関数として，以下で示す F_1, F_{-1}, F_0 の 3 種類を定義する．すなわち，

F_1 : 0 ↔ 1, 2 ↔ 3,..., 254 ↔ 255
F_{-1} : -1 ↔ 0, 1 ↔ 2,..., 255 ↔ 256
F_0 : 0 ↔ 0, 1 ↔ 1,..., 255 ↔ 255

と定義する．

識別関数と flipping 関数を利用して，以下のルールに従い画素を 3 種類のグループ（Regular グループ，Singular グループ，Unstable グループ）に分ける．

Regular グループ : $G \in R \Leftrightarrow f(F(G)) > f(G)$
Singular グループ : $G \in S \Leftrightarrow f(F(G)) < f(G)$
Unstable グループ : $G \in U \Leftrightarrow f(F(G)) = f(G)$

ただし，$(F(G))$ は flipping 操作を $G = (x_1, x_2, \ldots, x_n)$ に対して行うことを意味する．ここで，G 内の各画素ごとに異なった flipping を行えるようマスク M を導入する．M は n 組の値で，1, -1, 0 の 3 種類の値をとる．つまり，$F_{M(1)}(x_1), F_{M(2)}(x_2), \ldots, F_{M(n)}(x_n)$ となる．

マスク M を利用した場合の全画素に対する Regular グループの割合を R_M, Singular グループの割合を S_M と表記する．ここで，$R_M + S_M \leq 1$ であり $R_{-M} + S_{-M} \leq 1$ である．RS ステガナリシスでは，自然な画像に対して，

$$R_M \cong R_{-M} \quad \text{and} \quad S_M \cong S_{-M} \qquad (4)$$

と仮定している．

LSB プレーンをだんだんランダム化していくと（この処理は，秘密情報の埋め込み量を増加させることに相当する），R_M と S_M の差は 0 に近づく．全画素数の 50 パーセントの画素に対して flipping すると，$R_M \cong S_M$ となる．一方，R_{-M} と S_{-M} に関しては，埋め込み量が増加すると，R_{-M} と S_{-M} の差は増加する．**図 -3** に，自然画像に対する R_M, S_M, R_{-M}, S_{-M} グラフを示す．横軸は全画素数に対する flipping された画素数の割合である．この図を RS-diagram と呼ぶ．

RS ステガナリシスの原理は，RS-diagram の 4 つのカーブを推定し，それらの交点を求めることである．ここで，R_{-M} S_{-M} は直線として，また R_M S_M は二次曲線として近似できることを実験的に確認している．

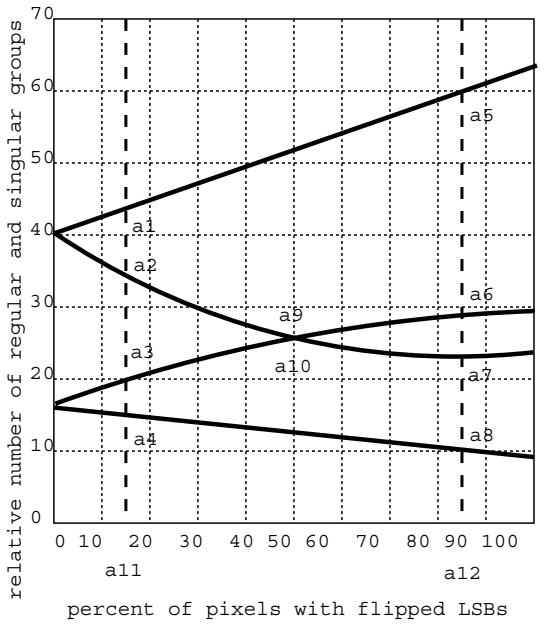

図-3　自然画像の RS-diagram（M = [0110]）[6)]

全画素の p パーセントが秘密情報で置換されているステゴ画像を考える．そのステゴ画像から計算される R，S は，$R_M(p/2)$ $R_{-M}(p/2)$ $S_M(p/2)$ $S_{-M}(p/2)$ に対応する．ここで，1/2 にしているのは埋め込まれるデータはランダム化されたビット系列と仮定しているので，その半分は原データのままであることによる．

ステゴ画像のすべての画素を flipping すると，$R_M(1\text{-}p/2)$ $R_{-M}(1\text{-}p/2)$ $S_M(1\text{-}p/2)$ $S_{-M}(1\text{-}p/2)$ が得られる．$R_M(1/2)$ と $S_M(1/2)$ は LSB プレーンをランダム化することにより求めることができるが，その値はランダム化に依存するので，いくつものランダム化から得られた結果を総合的に評価する必要がある．

$R_{-M}(p/2)$ と $R_{-M}(1\text{-}p/2)$ から，$S_M(p/2)$ と $S_{-M}(1\text{-}p/2)$ から，直線を求めることができる．また，$R_M(p/2)$ と $R_M(1/2)$ と $R_M(1\text{-}p/2)$ から，$S_M(p/2)$ と $S_M(1/2)$ と $S_M(1\text{-}p/2)$ から，放物線を求めることができる．直線と放物線は RS-diagram の左端で交わる．

$R_M(1/2)$ と $S_M(1/2)$ の計算時間を短縮するため，さらに埋め込まれた情報量をより単純に求めるために，以下の 2 つの仮定を設定する．

- 曲線 R_M と直線 R_{-M} の交点の x 座標は，曲線 S_M と直線 S_{-M} の交点の x 座標と等しい．
- R_M と S_M の曲線は，m = 50 パーセントで交差する．

この仮定により，埋め込まれた情報量を簡単な二次方程式の根として記述できる．

385 × 256 の濃淡画像をカバーデータとした実験では，ピクセルグループ（上述の G）を 2 × 2 とし，マスクを M = [1 0 ; 0 1] と設定し，埋め込み量を 0% から 100% まで 5% ずつ増加させた場合の，RS ステガナリシスを試み，誤差がほぼ 1% 以内であったと報告している．

一般的に，「自然なディジタル画像」のモデル化は非常に難しい．今のところ，画像に対するステガナリシスは，理想的な仮定のもとで情報が埋め込まれたことによるなんらかの画像特徴の統計量の変化を検出し，それにより埋め込み事実や埋め込み量の推定を試みている．

■おわりに

画像を用いたディジタルステガノグラフィについて解説した．ステガノグラフィは，暗号技術とは異なる特徴を持つ情報セキュリティ技術であるため，暗号との併用を含めてさまざまな応用が考えられる．また，セキュリティへの利用を離れて，カバーデータに情報が埋め込まれていることを前提とした利用形態，たとえばエンターテインメントへの利用なども考えられる．ステガノグラフィがユビキタス・ネットワーク社会のインフラ技術の 1 つになることを夢見ている．

参考文献

1) Katzenbeisser, S. and Petitcolas, F. A. P.: INFORMATION HIDING － Techniques for Steganography and Digital Watermarking －, Artech House, Norwood, Massachusetts (2000).
2) 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 (1998).
3) 安藤勝悛，小林弘幸，貴家仁志：レイヤ構造を利用した JPEG2000 符号化画像へのバイナリーデータ埋め込み法，信学論（D-II），Vol.J85-D-II, No.10, pp.1522-1530 (2002).
4) Takano, S., Tanaka, K. and Sugimura, T.: Data Hiding via Steganographic Image Transformation, IEICE TRANS. FUNDAMENTALS, Vol.E83-A, No.2, pp.311-319 (2000).
5) Rabbani, M. and Joshi, R. : An Overview of JPEG 2000 Still Image Compression Standard, Signal Processing: Image Communication, Vol.17, pp.3-48 (2002).
6) Fridrich, J., Golijan, M. and Du, R.: Detecting LSB Steganography in Color and Gray-Scale Images, IEEE Multimedia, Vol.8, No.4, pp.22-28 (2001).

（平成 15 年 2 月 10 日受付）