00-01069

逐次近似圧縮されたメディアデータへの情報秘匿に関する研究

野 田 秀 樹　九州工業大学工学部電気工学科助教授

1 まえがき

インターネットを介した情報通信が普遍的になりつつある今日，インターネット通信における情報セキュリティに関する社会的関心は非常に高まっている。そのような中，暗号技術とは異なる情報セキュリティ技術として情報秘匿技術が関心を集めている。情報秘匿技術は，画像，ビデオ，音楽データ等のメディアデータ中に，第三者に知られたくない重要な情報を隠す技術であり，ステガノグラフィ技術と電子透かし技術に二分される。ステガノグラフィ技術では，メディアデータは秘密情報を埋め込むための容器（ダミーデータ）として用いられ，ダミーデータ中に大量の秘密情報が隠されていても，そのことを第三者に気付かれないことが必要である。

これまでのステガノグラフィではビットプレーン分解[1]がよく用いられている[1,2]。そこでは通常，視覚的に最も影響が少ない最下位プレーンの２値データが秘密情報と入れ換えられている[1]。一方，ビットプレーン分解と人間の視覚特性を考慮した優れたステガノグラフィとして，BPCS（bit-plane complexity segmentation）ステガノグラフィが提案されている[3]。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[2]。BPCS ステガノグラフィは，８ビット濃淡画像[3]，24ビットカラー画像[4]，８ビット限定色カラー画像[5]，16ビット音響データ[6]等をダミーデータとして用いることができ，ダミーデータの30%～50%もの大量のデータを秘匿できることが確認されている。

しかし，これまでの BPCS ステガノグラフィは，非可逆圧縮されたメディアデータへの適用はできなかった。非可逆圧縮によってデータ値が変化することは，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形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[7,8,9]は少ない。文献[7]では，適応型離散コサイン変換による圧縮画像への情報埋め込み法を，文献[8]では，JPEG 符号化列への埋め込み法を提案している。しかしながら，いずれの方法でも埋め込み量は，圧縮ファイルのデータ量の２%程度のようである。文献[9]では，特異値分解とベクトル量子化に基づく画像データの埋め込み法を提案しているが，この方法は，１枚のダミー画像中に１枚の画像データを埋め込む場合にしか適用できない。

本研究では，ウェーブレット変換を用いた逐次近似型の情報圧縮法の併用により，非可逆圧縮されたメディアデータを用いたステガノグラフィを実現する。逐次近似型の圧縮法は，知覚的に重要な情報から順に符号化する方法であり，その基本アルゴリズムは JPEG2000[10]で採用されている。逐次近似型の圧縮アルゴリズムでは，ウェーブレット係数が，ビットプレーン構造を有する形で量子化表現されるため，BPCS ステガノグラフィが適用可能となる。各種メディアデータとして，静止画像，ビデオデータ，音響データを取り上げ，それぞれに対して圧縮データを用いる BPCS ステガノグラフィを実現する。

2 BPCS ステガノグラフィの概要

静止画像をダミーとする 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

[1]例えば，８ビット画像をビット分解すると，８枚の２値画像が得られる。
[2]そうでない場合に対しては，簡単な（ノイズ状でない）パターンを可逆な複雑な（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[3]。

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 のとき，複雑さ α を次式で定義する。

$$\alpha = \frac{k}{2m(m-1)},\ 0 \le \alpha \le 1 \tag{1}$$

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，以下の手順で行われる。

⑴ 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。

⑵ 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。

⑶ 秘密データを $m \times m$ ビット毎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[3]。

⑷ 順次，ノイズ状の小画像を秘密データの小ブロックと入れ換えていく。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。

式⑴の複雑さは，２次元データである静止画像に対するものであり，１次元データである音響データと３次元データであるビデオデータに対する複雑さは，それぞれ式⑵，⑶で与えられる。

$$\alpha = \frac{k}{m-1},\ 0 \le \alpha \le 1 \tag{2}$$

$$\alpha = \frac{k}{3m^2(m-1)},\ 0 \le \alpha \le 1 \tag{3}$$

式⑵における k は，m 個の２値１次元データ中の，０，１の境界点の数を，式⑶における k は，$m \times m \times m$ 個の２値３次元データ中の，０，１の境界面の面積を表す。

3　逐次近似圧縮データを用いた BPCS ステガノグラフィ

ウェーブレット変換を用いた逐次近似型の圧縮法では，圧縮データ自体がビット分解構造を有するため，圧縮データをダミーとする BPCS ステガノグラフィが実現できる。

3.1　静止画像を用いる場合

3.1.1　EZW-BPCS ステガノグラフィ

はじめに，逐次近似型の画像圧縮法として最初に提案された EZW（embedded zerotree wavelet)。アルゴリズム[11]を用いる場合について述べる。この場合の方法を，EZW-BPCS ステガノグラフィと呼ぶ。EZW 符号化では，ウェーブレット係数の絶対値 w は次のように２進表現される。

$$w = T(a_0 + a_1 2^{-1} + \cdots + a_n 2^{-n}),\ a_i \in \{0, 1\} \tag{4}$$

ここで，T は，$T > 0.5 w_{max}$（w_{max} はウェーブレット変換画像中のウェーブレット係数の絶対値の最大値）を満足する定数である。通常は，$T = 2^{\lfloor \log_2 w_{max} \rfloor}$ とする場合が多い。$(a_0 + a_1 2^{-1} + \cdots + a_n 2^{-n})$ は２進表現であることから，ウェーブレット変換画像においてもビットプレーン構造を考えることができ，BPCS ステガノグラフィが適用できることになる。

EZW 圧縮に組み込んだ情報秘匿法のブロック図を**図１**(a)に示す。EZW 圧縮は，⑴原画像を離散ウェーブレット変換（図中の DWT）する，⑵EZW 符号化で，ウェーブレット係数を量子化する，⑶量子化ウェーブレット係数を表す符号列を算術符号化する，という手順で行われる[11]。情報の埋め込みは，⑵の EZW 符号化と⑶の算術符号化の間で，**図１**の破線で囲まれた部分で行われる。EZW 復号化によって得られた量子化ウェー

[3]コンジュゲート演算は，市松模様の画像との画素毎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[3]。

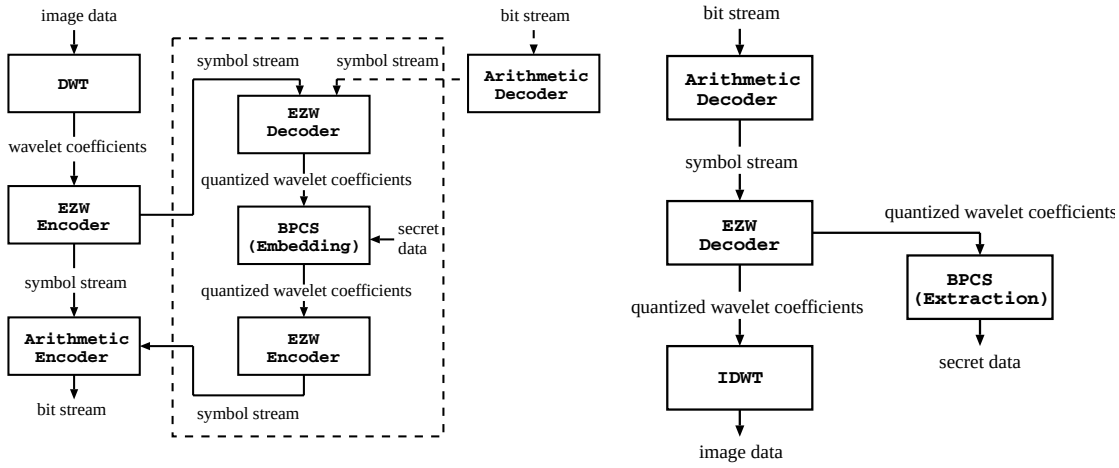

図１：EZW-BPCS ステガノグラフィによる情報埋め込みのブロック図（(a)），及び情報抽出のブロック図（(b)）

ブレット係数から，ビットプレーンが構成される．情報の埋め込みは，このビットプレーン上で BPCS ステガノグラフィによって行われ，情報が埋め込まれた量子化ウェーブレット係数が得られる。このウェーブレット係数が EZW 符号化され，その後，算術符号化が行われる。圧縮済みの画像ファイル(ビット列)中への情報埋め込みも行うことができる。ビット列の算術復号化によって得られる符号列をEZW号化すれば（**図１**(a)の右上の破線矢印の流れに従う），それ以降は，前述のとおりに行えばよい。

逆に，情報が埋め込まれた圧縮画像ファイル（ビット列）から情報を抽出する方法を**図１**(b)に示す．ビット列を算術復号化し，得られた符号列を EZW 復号化して量子化ウェーブレット係数を得る。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 ステガノグラフィによる情報の抽出を行う。

3.1.2 JPEG2000-BPCS ステガノグラフィ

JPEG2000 符号化[10]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（DWT）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毎に，ビットプレーン毎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 符号化と統合した BPCS ステガノグラフィ（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 の有する優れた圧縮率制御機能を考慮して，復号化途中の ROI 逆スケーリングの直後に情報秘匿を行うこととした。

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 ROI 逆スケーリング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 ROI 逆スケーリング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。

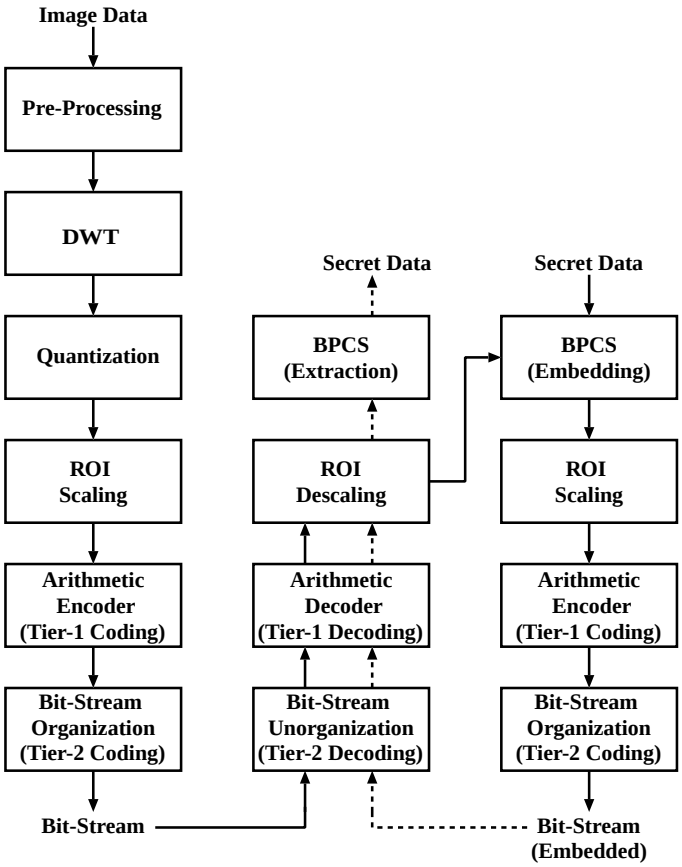

図2：JPEG2000-BPCS ステガノグラフィによる情報埋め込み，及び情報抽出のブロック図

3.2　ビデオデータや音響データを用いる場合

ビデオデータに対する圧縮法として，3-D SPIHT アルゴリズム[12]を用いた。3-D SPIHT は，静止画像圧縮のための SPIHT アルゴリズム[13]（SPIHT は EZW と並ぶ逐次近似型情報圧縮の代表的手法）を，３次元データであるビデオに適用するために拡張されたアルゴリズムである。3-D SPIHT アルゴリズムと BPCS ステガノグラフィを統合した，圧縮ビデオデータを用いた情報秘匿と情報抽出の方法は，**図１**の EZW-BPCS ステガノグラフィの場合と同様である。

音響データに対する圧縮法としては，Srinivasan らによるウェーブレットパケット変換を用いた逐次近似型の音響データ圧縮法[14]を用いた。この方法では，圧縮アルゴリズム自体は EZW を用いている。従って，BPCS ステガノグラフィとの統合は，静止画像に対する EZW-BPCS ステガノグラフィの場合と同様にして実現できる。

4　情報埋め込み実験

4.1　静止画像を用いる場合

4.1.1　EZW-BPCS ステガノグラフィ

“ Lena ”を含む３枚の標準画像をダミー画像として用いた。いづれもモノクロ画像で，8bit/pixel(bpp)，512×512 画素である。Daubechies 9/7 フィルタを用いた５レベルのウェーブレット変換を行った。EZW 圧縮におけるビットプレーンの数（式(4)における n）は８と９とし，その内，上位５つのプレーンには情報を埋め込まないこととした。

“ Lena ”を用いた場合の実験結果を**図３**に示す。ここでは，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。**図３**(a)と(d)は，EZW 圧縮におけるビットプレーン数を８と９とした圧縮画像であり，それぞれ 0.59bpp，1.15bpp に圧縮されている。**図３**(b)と(c)は，(a)を用いて埋め込みを行った

(a) (b) (c)

(d) (e) (f)

図３：Lena を用いた実験結果

(a) **EZW 圧縮画像（0.59bpp）** (b) (a)**への21%埋め込み結果**
(c) **33%埋め込み結果** (d) **EZW 圧縮画像（1.15bpp）**
(e) (d)**への26%埋め込み結果** (f) **38%埋め込み結果**

結果であり，(e)と(f)は(d)を用いた結果である。**図３**(b)と(e)は，埋め込みに際しての複雑さのしきい値 $\alpha_0 = 6/24$ とした結果であり，埋め込みによる劣化は殆ど知覚されない。一方，**図３**(c)と(f)は $\alpha_0 = 2/24$ とした結果であり，埋め込みによる劣化が認められる。３枚の画像を用いた実験結果を総合すると，画像の劣化が殆ど知覚されることなしに，圧縮画像ファイルサイズの25%位までの量の情報を秘匿できることが確認された。

4.1.2 JPEG2000-BPCS ステガノグラフィ

ここでは，JJ2000 プロジェクト[15]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１**に示す。画像は 1.0bpp，すなわち 1/8 に圧縮し，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，複雑さのしきい値は $\alpha_0 = 8/24$ とした。それ以外は，EZW-BPCS ステガノグラフィの場合と同様の条件で行った。

表１　JPEG2000 圧縮画像を用いた情報埋め込み実験結果

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”	1/8	40.5	14.0	37.1
“Barbara”	1/8	37.1	16.9	31.9

表２　3-D SPIHT 圧縮ビデオデータを用いた情報埋め込み実験結果

ビデオ	埋め込みなし		埋め込みあり	
	圧縮率	PSNR(dB)	埋め込み率 (%)	PSNR(dB)
“Claire”	1/32	44.3	15.4	43.6
“Diskus”	1/11	39.6	16.0	38.1

表３　EZW 圧縮音響データを用いた情報埋め込み実験結果

音楽	埋め込みなし		埋め込みあり	
	圧縮率	PSNR(dB)	埋め込み率 (%)	PSNR(dB)
1	1/5	43.8	16.0	40.8
2	1/3	46.4	19.2	42.4

4.2　ビデオデータや音響データを用いる場合

実験に用いたビデオデータは，256×256 画素，32フレームのモノクロビデオである。3-D SPIHT 圧縮におけるビットプレーン（実際はキューブ）数は10，埋め込みに使用したのは最下層のみ，埋め込みの単位となる小キューブの大きさは 4×4×4，複雑さのしきい値は $\alpha_0 = 0.3$ とした。実験結果を**表２**に示すが，この場合，埋め込みによる劣化は知覚されなかった。

音響データとして，標本化周波数 44.1kHz，量子化精度 16bit のモノーラル音楽データを用いた。EZW 圧縮におけるビット数は14，その内，最下層から２つのビットを埋め込みに用い，複雑さのしきい値は $\alpha_0 = 0.3$ とした。実験結果を**表３**に示すが，この場合，埋め込みによる劣化は知覚されなかった。

5　むすび

本研究では，ウェーブレット変換を用いた逐次近似型の情報圧縮アルゴリズムと BPCS ステガノグラフィを統合して，圧縮データに適用可能なステガノグラフィを実現した。各種メディアデータとして，静止画像，ビデオデータ，音響データを取り上げ，それぞれに対して圧縮データを用いる BPCS ステガノグラフィを実現した。本研究によって，BPCS ステガノグラフィ等のビットプレーン分解を用いたステガノグラフィ技術が，情報圧縮されたメディアデータに対して適用可能になり，ステガノグラフィの利用利便性や安全性を飛躍的に向上させることができる。各種メディアデータは情報圧縮された形で通信されるのが普通であり，そのような自然な形でのステガノグラフィが本研究ではじめて実現された。

参考文献

[1] Katzenbeisser Katzenbeisser, S. and Petitcolas, F.A.P.: *InformationHiding Techniques for Steganography and Digital Watermarking,* Artech House (2000).

[2] Wang Wang, R.Z., Lin, C.F. and Lin, J.C.: Image Hiding by Optimal LSB Substitution and GeneticAlgorithm, *Pattern Recognition,* Vol.34, pp.671-683 (2001).

[3] 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，電子情報通信学会論文誌，Vol.J81-D-II, pp.1132-1140 (1998)。

[4] Kawaguchi Kawaguchi, E. and Eason, R.O.: Principle and Applications of BPCS-Steganography, *Proc. of SPIE,* Vol.3528, pp.464-473 (1998).

[5] Ouellette Ouellette, R., Noda, H., Niimi, M. and Kawaguchi, E.: Topological Ordered Color Table for BPCS Steganography using Indexed Color Images, *IPSJ Journal,* Vol.42, pp.110-113 (2000).

[6] 草津郁子，新見道治，野田秀樹，河口英二：音響信号をダミーとする大容量 steganography, 電子情報通信学会技術研究報告, EA98-69-78, pp.27-32 (1998)。

[7] 片岡利幸，田中清，中村康弘，松井甲子雄：適応型離散コサイン変換符号化におけるカラー画像への記述情報の埋込み，電子情報通信学会論文誌，Vol.J72-B-I, pp.1210-1216 (1989)。

[8] 小林弘幸，野口祥宏，貴家仁志：JPEG 符号化列へのバイナリデータの埋込み法，電子情報通信学会論文誌，Vol.J83-D-II, pp.1469-1476 (2000)。

[9] Chung, K.L., Shen, C.H. and Chang, L.C.: A Novel SVD- and VQ-Based Image Hiding Scheme, *Pattern Recognition Letters,* Vol.22, pp.1051-1058 (2001).

[10] Rabbani, M. and Joshi R.:An Overview of JPEG 2000 Still Image Compression Standard. *Signal Processing: Image Communication,* Vol.17, pp.3-48 (2002).

[11] Shapiro, J.M.: Embedded Image Coding Using Zerotrees of Wavelet Coefficients, *IEEE Trans. Signal Process.,* Vol.41, pp.3445-3462 (1993).

[12] Kim, B.J., Zixiang, X. and Pearlman, W.A.: Low Bit-Rate Scalable Video Coding with 3-D Set Partitioning in Hierarchical Trees (3-D SPIHT), *IEEE Trans. Circuits and Systems for Video Technology,* Vol.10, pp.1374-1387 (2000).

[13] Said, A. and Pearlman, W.A.: A New, Fast, and Efficient Image Codec based on Set Partitioning in Hierarchical Trees, *IEEE Trans. Circuits and Systems for Video Technology,* Vol.6, pp.243-250 (1996).

[14] Srinivasan, P. and Jamieson, L.H.: High-Quality Audio Compression Using An Adaptive Wavelet Packet Decomposition and Psychoacoustic Modeling, *IEEE Trans. Signal Process.,* Vol.46, pp.1085-1093 (1998).

[15] http://jj2000.epfl.ch/index.html

〈発　表　資　料〉

題　　名	掲 載 誌 ・ 学 会 名 等	発 表 年 月
Application of BPCS steganography to wavelet encoded images	第3回日本ファジイ学会九州支部学術講演会論文集，pp.73-76	2001年12月
BPCS steganography using EZW encoded images	電子情報通信学会技術研究報告，Vol. 101, No. 524, PRMU 2001-155, pp.13-20	2001年12月
ビットプレーン分解ステガノグラフィーのウェーブレット圧縮画像への適用	情報処理学会論文誌，Vol.43, No.5, pp.1548-1551	2002年５月
BPCS steganography using EZW lossy compressed images	Pattern Recognition Letters, Vol.23, pp.1579-1587	2002年10月