

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

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[†]

本論文では, EZW (embedded zerotree wavelet) アルゴリズムを用いた画像圧縮と BPCS (bit-plane complexity segmentation) ステガノグラフィを組み合わせた情報秘匿法を提案する. 本提案によって, 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, 非可逆圧縮された画像データに対して適用可能になる. 提案法によると, 画像の劣化が知覚されることなく, 圧縮画像ファイルサイズの 25% 位もの大量の情報を秘匿できることが確認された.

Application of Bit-plane Decomposition Steganography to Wavelet Compressed Images

HIDEKI NODA,[†] JEREMIAH SPAULDING,[†] MAHDAD NOURI-SHIRAZI,^{††}
MICHIHARU NIIMI[†] and EIJI KAWAGUCHI[†]

This paper presents a steganography method based on an embedded zerotree wavelet (EZW) compression scheme and bit-plane complexity segmentation (BPCS) steganography. The proposed steganography enables us to use lossy compressed images as dummy files in bit-plane-based steganographic algorithms. Large embedding rates of around 25% of the compressed image size were achieved with almost no obvious degradation in image quality.

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

解がよく用いられている^{1),2)}. ここでは通常, 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. 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

たとえば, 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.

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, コンジューグート演算と呼ばれる操作を用意している³⁾.

[†] 九州工業大学工学部

Faculty of Engineering, Kyushu Institute of Technology

^{††} 総務省通信総合研究所

Communications Research Laboratory

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、一般的に、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)~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%程度のものである。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。

本論文では、ウェーブレット変換を用いた逐次近似型の画像圧縮法を用いて、圧縮画像に適用可能なBPCSステガノグラフィを提案する。本論文では、そのような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¹⁰⁾を用いる。EZWアルゴリズムでは、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。本提案によって、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。

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。

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

ここで、 $2m(m-1)$ は、市松模様のように得られる、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。

- (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。
- (4) 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。

3. EZW圧縮画像への情報埋め込み

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。

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

ここで、 T は、 $T > 0.5w_{max}$ (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、 $T = 2^{\lceil \log_2 w_{max} \rceil}$ とする場合が多い。 $(a_0 + a_1 2^{-1} + \dots + a_n 2^{-n})$ 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に示す。EZW圧縮は、(1)原画像を離散ウェーブレット変換(図中のDWT)する、(2)EZW符号化で、ウェーブレット係数を量子化する、(3)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¹⁰⁾。情報の埋め込みは、(2)のEZW符号化と(3)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

コンジュゲート演算は、市松模様の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³⁾。

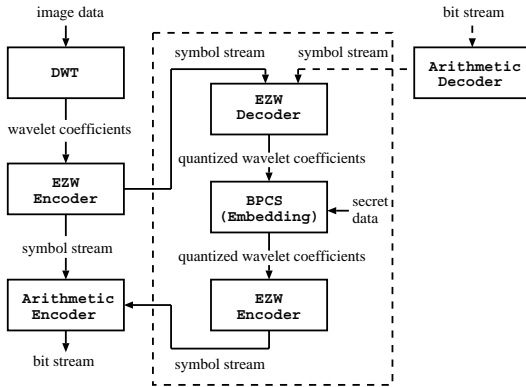


図 1 提案法による情報埋め込みのブロック図

Fig. 1 A flowchart of embedding secret data by the proposed method.

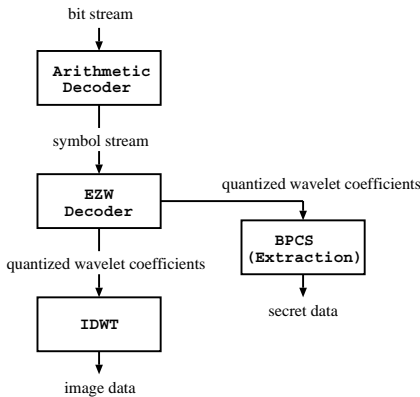


図 2 提案法による情報抽出のブロック図

Fig. 2 A flowchart of extracting secret data by the proposed method.

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 復号化すれば(図 1 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 2 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。

4. 情報埋め込み実験

Lena を含む 3 枚の標準画像をダミー画像として用いた。いず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 (2)における n)は 8 と 9 とし、そのうち、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 0.59 bpp, 1.15 bpp 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ほとんど知覚されない。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。

5. むすび

本論文では、EZW アルゴリズムによる画像圧縮と BPCS ステガノグラフィを組み合わせ、圧縮画像に適用可能なステガノグラフィを実現した。提案法によると、画像の劣化が知覚されることなしに、圧縮画像ファイルサイズの 25%位も大量の情報を秘匿できることが確認された。

提案法は、SPIHT (set partitioning in hierarchical trees) アルゴリズム¹¹⁾ や JPEG2000 のような、他のウェーブレット変換を用いた逐次近似型画像圧縮法にも適用可能であると考えられる。標準規格である JPEG2000 圧縮画像への適用は特に有用であることから、現在その実現を目指して検討中である。

謝辞 本研究の一部は電気通信普及財団の助成による。

参考文献

- 1) Katzenbeisser, S. and Petitcolas, F.A.P.: *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House (2000).
- 2) Wang, R.Z., Lin, C.F. and Lin, J.C.: Image Hiding by Optimal LSB Substitution and Genetic Algorithm, *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



図3 Lenaを用いた実験結果：(a) EZW 圧縮画像 (0.59 bpp)，(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 (1.15 bpp)，(e) (d) への26%埋め込み結果，(f) 38%埋め込み結果

Fig. 3 Experimental results for "Lena": (a) EZW compressed image (0.59 bpp), (b) 21% embedded and, (c) 33% embedded into (a), (d) EZW compressed image (1.15 bpp), (e) 26% embedded and, (f) 38% embedded into (d).

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, E. and Eason, R.O.: Principle and Applications of BPCS-Steganography, *Proc. SPIE*, Vol.3528, pp.464-473 (1998).
- 5) 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め込み, 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め込み法, 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) Shapiro, J.M.: Embedded Image Coding Using Zerotrees of Wavelet Coefficients, *IEEE Trans. Signal Process.*, Vol.41, pp.3445-3462 (1993).
- 11) 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).

(平成 13 年 9 月 28 日受付)

(平成 14 年 2 月 13 日採録)