ステガノグラフィにおける埋め込みデータ量の限界についての調査と研究

2000MT003 安藤 百恵　　2000MT011 福田 幸子
指導教員　真野 芳久

1　はじめに

急速な勢いでインターネットを使った情報通信が我々の身近な存在になりつつある今日、重要なデータ、例えば秘密データをインターネットで他人に気づかれることなく通信したいという願いが自然と生まれてくるであろう。そこで注目されているのがステガノグラフィという技術である。ステガノグラフィ技術では、メディアデータ中に秘密データを隠し、他人に気づかれることなく保存したり相手に伝えたりする。画像に秘密データを隠すことが多く、秘密データを隠す画像のことをダミー画像と呼ぶ。ダミー画像の 36% 程度を埋め込むことができるという報告 [4] がある。

本研究では、扱うダミー画像は白黒濃淡画像とし、非圧縮画像 (BMP 形式) と圧縮画像 (JPEG2000 形式) に対しての既存の埋め込み方法 [1][3][4][5] を調査し、既存の埋め込み方法や応用した埋め込み方法を作成して実際に埋め込んだデータ量について調査研究を進める。

2　ステガノグラフィとは

ステガノグラフィとは、秘密データを別のデータに隠し持たせ、他人に気付かれることなく保存、伝送する技術である。

類似する技法として、電子透かしと呼ばれる技術がある。これはデジタルデータに対しての著作権や真正性を立証するための証拠を知覚できないようにデータに付加する技術のことで、ステガノグラフィとともに情報秘匿技術に属するが、二つの技術は用途も使用方法も異なる [2]。例えば、電子透かしで重要視されるのは、様々な画像処理に耐久をもつことだが、ステガノグラフィでは埋め込む情報が重要で、大量の情報を埋め込むことが求められる。また暗号とは全く別物である。暗号は秘密の内容は保護するが、存在を強調することになる。これに対してステガノグラフィは、秘密データを別のデータに隠し持たせる。秘密情報をあらかじめ暗号化して、それを秘匿すれば極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 [2]。

3　画素置換型

基本概念となる画素置換型の方法 [3] を示す。

3.1　方法

1 画素当たり 8 ビットの濃淡画像で表現したとき、画像を 8 枚のビットプレーンにわけることができる。この各ビットプレーン上の画素は二値で表現されているので、その二値データの一部をそっくり秘密データと置換する。ここで 8 枚のビットプレーンを最下位から順にビットプレーン番号 0,1,....,7 と呼ぶ。

3.2　検証結果

ダミー画像として自然画像と人工画像を用い、最下位ビットプレーンから順に二値の画像を埋め込んでいく。肉眼では最下位からビットプレーン番号 3 までは埋め込まれているのが認識できなかったが、ビットプレーン番号 4 になると埋め込まれているのが画像によってわかるものも現れた。肉眼での検証では曖昧となるため、さらに詳しく画質を評価するために信号対雑音比 (S/N 比) を求めた (**図 1** 参照)。

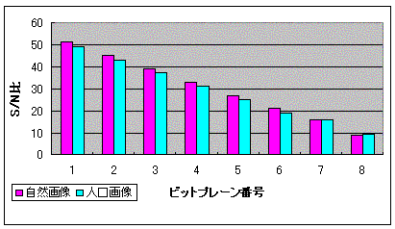

図 1　画素置換型で埋めた場合

S/N 比とは、原画像と埋め込み後の画像の劣化比のことで数値は高いほうがよく、埋め込んだ画像の冗長度も考慮すると、35dB 前後までの埋め込み後の画像は原画像との差を認めにくい。上位のビットプレーンに埋め込むと埋め込みデータが出現し、S/N 比も激しく低下するのに対し、下位ビットプレーンに埋め込むことは画像にあまり影響を与えない、それは S/N 比が高い数値を示していることからわかる。秘密データを下位のビットプレーン上に置き換えても元の画像に与える影響は少ない。この埋め込み方法は 1 枚のビットプレーン毎に埋め込めば、ダミー画像の 12.5% まで埋め込むことができた。しかしビットプレーン上の画像データを秘密データでそっくり置換しているため第三者に 1 枚ずつビットプレーンを取り出して調べられると、すぐに埋め込みデータは容易に探知することができる。

4　画素空間利用型

前節の欠点をふまえ、視覚的な影響も考慮しつつ、さらに埋め込み位置もわからないように、複数枚のビットプレーンを使った画素空間利用置換型の方法 [3] を示す。

4.1　方法

画像を $n \times n$ の小領域のブロックに分割し、小領域ごとに異なる特定のビットプレーン上に秘密データを分割配置していく。

画像を $n \times n$ 画素のブロックに分割する。画像の位置

情報に依存してビットプレーン番号を決定し、そこのブロック内から m $(1 \leq m \leq n \times n)$ bit 選択し、秘密データを埋め込む。この方法をうまく利用できれば、第三者からは埋め込み位置はわからず全体的に画質劣化も抑えることができる。

この方法では画質が局部的に著しく劣化するおそれがあるため、輝度補正処理を導入する。これは桁上りによってダミー画像に影響しない範囲で一つ上のビットや下位ビットの画素値を増加、減少させて原画素の値にできるだけ近づける処理である。

4.2 検証結果

$n = 1, m = 1$ についてダミー画像として自然画像と人工画像を使って試してみた。ビットプレーン番号 0〜0,1,...,7 まで埋め込み実験した。0〜6,7 は埋め込みデータが出現する場合はあったが、S/N 比は前節に比べ上がっている (**図 2** 参照)。しかしながら、埋め込みデータ量は最大でもダミー画像の 12.5% である。この方法では、埋め込み位置が容易に探知されず、S/N 比の向上も期待できるが埋め込みデータ量の向上は期待できない。

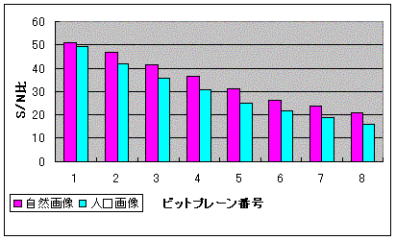

図 2　画素空間利用型 $(n = 1, m = 1)$ で埋めた場合

5　ビットプレーンの複雑さ利用型

ビットプレーン分解で得られる二値画像は「画像に対して有効な情報を保有している領域と保有していない（ノイズ状ともいわれる）領域」に分割できることを利用した方法である [4]。

5.1 方法

以下の手順で行う [2]。

1. 各 8 枚のビットプレーンを $2^m \times 2^m$ 画素の小領域に分割し、小領域の「複雑さ α (以下に定義)」が、閾値 α_0 (≤ 0.5) よりも大きい時、小領域は複雑と判断し、埋め込み用の場所となる。

$$\alpha = \frac{k}{2 \times 2^m \times (2^m - 1)}$$
$$(0 \leq \alpha \leq 1,\ k \text{ は } 0 \text{ と } 1 \text{ の境界線の長さ})$$

2. 秘密データを $2^m \times 2^m$ ビットの小ブロックに分割し秘密データが「閾値 α_0」よりも小さい時、複雑なパターンに変換する (コンジュゲート演算という)。コンジュゲート演算は、その画像と市松模様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. 複雑な小領域を秘密データの小ブロックと順次置き換えていく。秘密データの小ブロックがコンジュゲート演算を行ったか否かの情報 (コンジュゲートマップ) は記憶しておき、秘密データと同様に埋め込む。埋め込まれた情報の取り出しは、複雑さの閾値 α_0 とコンジュゲートマップを基に埋め込み手順と逆の手順を行う。

5.2 検証結果

自然画像と人工画像を使って (256 × 256 画素)、閾値を 0.312 として [4]、実験を行った。横軸に 埋め込みデータ量 (%)、縦軸に S/N 比 (dB) のグラフを示す。**図 3** より、人工画像は前節に比べ埋め込みデータ量が大幅に減少しているのに対し、自然画像では大幅に増加している。それは人工画像には複雑な領域が少なく自然画像のように下位のビットプレーンにも複雑なものが現れないからである。そのことから人工画像はこの方法ではダミー画像として不向きであるといえる。自然画像ではダミー画像の約 41.9% を S/N 比が 34.3dB、つまり視覚的に見劣りしない程度で埋め込むことができた。

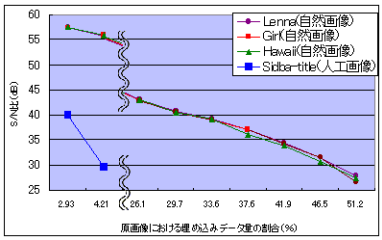

図 3　ビットプレーンの複雑さ利用型で埋めた場合

5.3 閾値の検証

複雑さを利用することで、より多くの埋め込みデータ量を得ることができた。しかし、埋め込みデータ量をさらに増加させさせられないかを考える余地がある。この方法では全ビットプレーンに対し、複雑か複雑でないかの閾値を一定にしていたが、前の方法からもわかるようにビットプレーン毎に画像に対して有効な情報量が違う。そのことから閾値をビットプレーン毎に操作することで埋め込みデータ量の増加をはかる。

5.3.1 方法

無条件で最下位ビットプレーンから 3 枚全てに埋め込むこととし、ビットプレーン番号 3 から 5 までは閾値を操作する。埋め込みデータ量を調べる目的からランダムなビット列を埋め込む。これにより画質の劣化が抑えられることにより、下限を 32dB とした。

5.3.2 検証結果

閾値 (0.312) を一定にして得たものと閾値を変動させて得たものの埋め込みデータ量、S/N 比を比較した (**表 1** 参照)。閾値一定のよりもビットプレーン毎に閾値を変動した方が埋め込みデータ量の割合 (%) が 2〜10 程度増加した。

また、ビットプレーン番号 3 まで埋め込んだ画像とビットプレーン番号 4 や 5 まで埋め込んだ画像の埋め込みデータ量や S/N 比を比較したところ、どの画像もビッ

表 1　閾値の操作による埋め込みデータ量 (%) と S/N 比 (dB)

画像	閾値一定		閾値変動	
	S/N 比	埋め込みデータ量	S/N 比	埋め込みデータ量
couple	32.7	39.5	32.7	47.0
milkdrop	32.6	37.0	32.5	47.7

トプレーン番号 3 まで埋め込む方がより多くの埋め込みデータ量と安定した S/N 比を得ることができた。そこで埋め込むビットプレーンを最下位から 4 枚とし、最下位から 3 枚のビットプレーンは無条件に埋め込み、ビットプレーン番号 3 では閾値を操作して最適な閾値を探索するプログラムを作成したところ、埋め込みデータ量の割合 (%) が 5〜10 程度増加した。

6　圧縮画像への応用

世の中で非圧縮画像を使われることは少なく、圧縮画像を使うことの方が多い。そこで圧縮画像に対して、多くの情報を埋めることができる方法について考える。

本研究ではステガノグラフィの実現のため、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る非可逆圧縮画像を用いる。逐次近似型の圧縮法は知覚的に重要な情報を順に符号化する方法で、その基本アルゴリズムは JPEG2000 で採用されている。そこで JPEG2000 における埋め込み方法について考える。

JPEG2000 とは JPEG 規格委員会が設定した新しい JPEG のことで ISO15444 で国際規格に設定されている。従来の JPEG と比較すると高品質で高圧縮であるなど様々な利点がある [6]。

7　JPEG2000 における複雑さ利用型

非圧縮画像において複雑さ利用型埋め込み法で大容量の秘密データを埋め込むことができた。そこで複雑さ利用型を JPEG2000 の圧縮画像にも適用する [2][5]。

7.1　方法

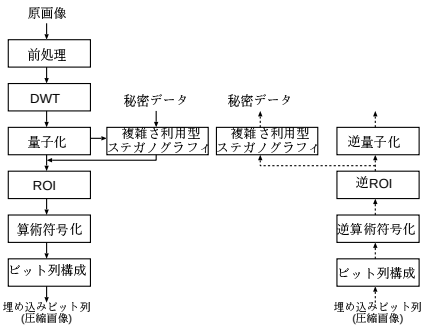

図 4　JPEG2000 における複雑さ利用型の手順

JPEG2000 符号化は、前処理、離散ウェーブレット変換 (DWT)、量子化、算術符号化、ビット列構成から構成される (**図 4** の左側参照)。DWT の後、ウェーブレット係数は量子化され、その後、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る。量子化ウェーブレット係数 (以下係数と呼ぶ) は、コードブロックと呼ばれる小ブロックを、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、指定の圧縮率でビット列が生成される。

JPEG2000 符号化と統合した複雑さ利用型の手順を**図 4** に示す。JPEG2000 の有する優れた圧縮率制御機能を考慮して、符号化する途中の ROI の直前に埋め込む。JPEG2000 における複雑さ利用型による埋め込みは、**図 4** の実線の矢印に従って行われる (**図 4** 左側)。矢印に従って量子化まで行うと、一旦符号化を中断し、係数からビットプレーンを構成し、複雑さ利用型によって情報の埋め込みを行う。情報が埋め込まれた係数は、ROI から符号化処理を受け、情報が埋め込まれた JPEG2000 ビット列が得られる。また、埋め込めれた情報の取り出しは、破線矢印に従って行われる (**図 4** 右側)。

7.2　検証結果

8bpp (bit/pixel) であるダミー画像を用い、埋め込みの単位となる小画像の大きさは 4×4 画素、圧縮率は 1.0bpp で、秘密情報として二値乱数を用いた。Lenna を用いた場合の実験結果を**図 5** に示す。左図は閾値を 0.5 とし最下位 1 ビットのみに埋めた場合で、右図は閾値を 0.5 とし最下位から 3 ビットに埋めた場合である。S/N 比とデータ量の関係を**表 2** に示す。埋め込めるデータ量はごくわずかで我々が試みたこの方法では、複雑さ利用型の良さをいかすことができなかった。[5] に示されている数値 (15% 程度) とは異なるので改善の余地はあると思われるが、今後の課題として残された。

図 5　左図 ： 埋め込み率 0.4%, 33.7dB、右図 : 埋め込み率 0.5%, 30.7dB

表 2　JPEG2000 における複雑さ利用型の埋め込み実験結果

画像 (512 × 512 画素)	埋め込みなし		埋め込みあり	
	圧縮率	S/N 比 (dB)	埋め込み率 (%)	S/N 比 (dB)
Lenna	1/8	38.0	0.4	33.7
Barbara	1/8	37.6	3.8	33.0

8　JPEG2000 におけるレイヤ構造利用型

複雑さ利用型では、量子化後に情報を埋め込んでいたため、後に続くエントロピー符号化に影響を与え、符号化列の長さを変化させてしまっていた。そして何よりも埋め込めるデータ量がごくわずかであった。そこで JPEG2000 の機能の一つであるレイヤ構造をデータ埋め込みのために利用する [1]。

8.1　方法

レイヤとは、複数の画質で順次再生できるように算術符号を明示的にグループ分けしたものである。符号列は最上位から最下位までいくつかのレイヤと、各レイヤの位置、長さを記録したヘッダ部から成る。各レイヤは、各コードブロックの算術符号の一部とその位置と長さを記録したヘッダ部から構成される。この時、画質への寄与が高い情報ほど、上位のレイヤに含まれるようになる。つまり、一般に各コードブロックにおいて上位ビットの情報ほど上位レイヤに含まれるよう構成される。

JPEG2000 符号列の最下位レイヤに秘密データを埋め込む。**図 6** は、レイヤが 4 層存在する場合に、データを埋め込む例である。まず、秘密データのサイズを見積もり、2 層以上のレイヤを構成し、JPEG2000 符号化を行う。その際、最下位レイヤのサイズは、見積もられたサイズ以上とする。そして、最下位レイヤに順に秘密データを埋め込む。この時、埋め込むデータのサイズが最下位レイヤと同一でない場合、埋め込むデータのサイズ情報も保存する。また、秘密データの取り出しは埋め込み手順と逆の手順を行う。

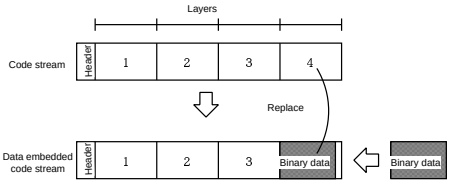

図 6　最下位レイヤへのデータ埋め込み ([1] より引用)

8.2　検証結果

8bpp であるダミー画像を用いた。圧縮率は 1.0bpp、秘密情報は二値乱数を用いた。Lenna を用いた場合の実験結果を**図 7** に、S/N 比とデータ量の関係を**表 3** に示す。画像によって埋められるデータ量は大きく異なるが 15〜50% 程度の埋め込み率を得ることが確認された。

表 3　JPEG2000 におけるレイヤ構造利用型の埋め込み実験結果

画像 (512 × 512 画素)	埋め込みなし		埋め込みあり	
	圧縮率	S/N 比 (dB)	埋め込み率 (%)	S/N 比 (dB)
Lenna	1/8	38.0	24.5	33.1
Milkdrop	1/8	42.6	53.7	32.9

図 7　左図 :　埋め込み率 19.6%,34.0dB、右図 : 埋め込み率 24.5%,33.1dB

9　おわりに

画素置換型、画素空間利用型いずれの方法でも改善の余地はあり、埋め込みデータ量を伸ばすことは可能であるが、複雑さ利用型による埋め込み結果 (約 40〜45%、34dB 前後) 程度の向上は望めない。複雑さ利用型では閾値や埋め込むビットプレーンを制限することで埋め込みデータ量の割合 (%) を 5〜10 程度伸ばすことができた。圧縮画像については、[5] による複雑さ利用型における埋め込み方法を試みたが、我々はわずか数 % で、失敗に終わった。そこで新たに試みたレイヤ構造を利用した埋め込み方法 [1] では、圧縮画像のデータ量の 15〜50% 程度もの埋め込み率を確認できた。これにより、画像によっては、圧縮画像でも非圧縮画像と同程度の埋め込み率を得られることが確認できた。

今後の課題としては、まず [5] が提案する埋め込み方法を実現できなかったことが挙げられる。また他の圧縮画像、さらにカラー画像においての埋め込み方法についての調査も挙げられる。

謝辞

本研究を進めるにあたり多大な助言を頂き、また熱心に御指導下さいました南山大学情報通信学科の真野芳久教授に深く感謝いたします。

参考文献

[1] 安藤勝俊, 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データ埋め込み法”, 信学論, Vol.J85-D-ll, No.10 (2002).

[2] 河口英二, 野田秀樹, 新見道治 : “画像を用いたステガノグラフィ”, 情報処理, Vol.44, No.3 (2003).

[3] 松井甲子雄 : “電子透かしの基礎–マルチメディアのニュープロテクト技術”, 森北出版 1998.

[4] 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画像深層暗号法, 電子情報通信学会論文誌, Vol.J81-DII No.6 (1998).

[5] 野田秀樹 : “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”, 電気通信普及財団研究調査報告書第 17 号 (2002).

[6] 小野定康, 鈴木純司 : “わかりやすい JPEG2000 の技術”, オーム社 2003.