

BMP 画像に対するステガノグラフィの検討と実験

2001MT015 福田 奈美

2001MT036 井上 歩美

2001MT103 鳥居 正浩

指導教員 真野 芳久

1 はじめに

ステガノグラフィ技術とはメディア内に秘密の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ものである。秘密データを隠すメディアをダミーデータという。

ステガノグラフィは、暗号化とは異なり秘密データの存在自体を隠す技術である。この2つは協調できる技術であり、秘密データをあらかじめ暗号化させそれを秘匿すれば、極めて強力な情報保護技術となる。

2 画像評価の方法

本研究では、ダミー画像に秘密データを埋め込んだ後の画像の劣化の度合いを計るのに S/N(Signal/Noise) 比を用いる。S/N 比はデシベル (dB) 単位であらわし、この値が大きいほど劣化が少なく高画質ということがいえる。S/N 比が 40dB を超える画像であれば画質の劣化はほとんどみられない。

しかし、視覚的に劣化したことがわかりやすいパターンのある雑音があっても、S/N 比は比較的高い数値を返すこともある。そのため画像の劣化を評価する際には、S/N 比での評価と視覚的な評価の2つを用いて評価することにする。

また、ビットプレーンや画素ごとに分解されて見たときにも解読が困難な埋め込み方法を実現することにも重点をおいて研究を進める。

3 ビットマップとは

3.1 特徴

ビットマップはウィンドウズが標準でサポートしている画像形式のひとつである。2 値の画像からフルカラーまであり、それぞれファイルの各属性のデータを格納するためのヘッダと使用する色のパレットデータ、実際のグラフィックイメージデータからなっている。

3.2 ビットプレーンとは

1 画素あたり 8 ビットの濃淡画像で表現したとき、画像全体でビットごとにみることによって 8 枚の 2 値画像として考えることができる。この 1 枚 1 枚をビットプレーンと呼び、最下位のビットプレーン (LSB) から最上位のビットプレーン (MSB) まで順に、ビットプレーン番号を 0, 1, …, 7 と呼ぶ。

3.3 ビットマップへのステガノグラフィ

ビットマップは冗長度が高く、画像にとって重要な部分以外の変更は人間の目にはほとんど見分けがつかない。それを利用してできるだけ多くの秘密データを埋め込んでいく。また、本実験で使用されるビットマップは 8

ビット 256 階調表示の白黒濃淡画像である。

4 画素置換型

ビットマップのビットプレーンを利用した埋め込み方法に画素置換型がある。これはビットプレーンのうち 1 枚をそのまま秘密データと置き換える。下位のビットプレーンに埋め込んだ場合は画像に違いはほとんど見られない。しかし、この方法ではビットプレーンを 1 枚ずつ分解すると秘密データを簡単に取り出されてしまう恐れがある。そのため、それを改善するために画素空間利用型が考えられた。

5 画素空間利用型

画素空間利用型では、ダミー画像 $n \times n$ の小領域に分割し、その小領域ごとに異なる特定のビットプレーンを選択し m ビットの埋め込みを行うことで秘密データを分散配置する。

5.1 埋め込み方法

小領域ごとにランダムにビットプレーンを選択し、選択したビットプレーンの中から秘密データを埋め込む画素をランダムに決定する。 $n=1$ と $n=3$ のとき $m=1$ での S/N 比の変化は図 1 のようになる。

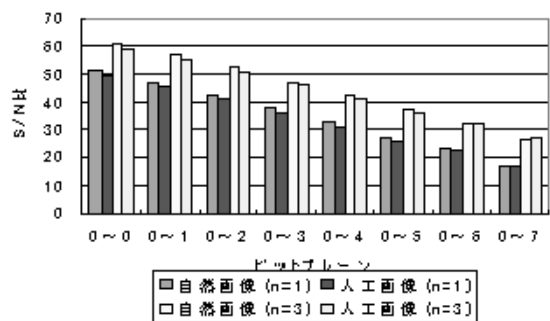


図 1 画素空間利用型の埋め込みの S/N 比の変化

5.2 輝度補正

輝度補正とはダミー画像に秘密情報を埋め込んだときに起こる画素情報の変化を、埋め込み位置以外のビットを変更することや、埋め込み位置の周辺の画素情報を変更することによって、輝度を原画像の明るさに近づけたり、まわりの画素との輝度の差を少なくすることで画像の劣化を抑え、埋め込みの形跡を視覚的にわかりにくくする補正のことである。本研究では、前者の秘密データを埋め込まれた画素に対する輝度補正を取り扱う。

輝度補正は、原画像の輝度と埋め込み後の輝度の差がもっとも小さくなるように行う。具体的に、ビットプ

レーン番号を k ($k = 0, 1, 2, \dots, 7$) として、秘密データをビットプレーン k に埋め込んだとき、 $k-1$ の値が秘密データと異なった場合 k より上のビットで秘密データと値が等しくなるビットを見つけ値を反転させ、そのビットより下の値をすべて秘密データと同じ値に書き換える。そこで、上位のビットに利用できるビットが見つからなかった場合と $k-1$ と秘密データが等しかった場合、 $k-1$ 以下のビットを全て秘密データと異なる値に書き換え、下位ビットのみを利用して輝度補正を行う。

輝度補正を用いた埋め込みでは、画素空間利用型で秘密データを埋め込んだ画素に対して、原画像と埋め込み後の画像の輝度の差がもっとも小さくなるように輝度補正を行う。 $n=1$ 、 $m=1$ で埋め込んだ際の S/N 比の変化は図 2 のようになる。

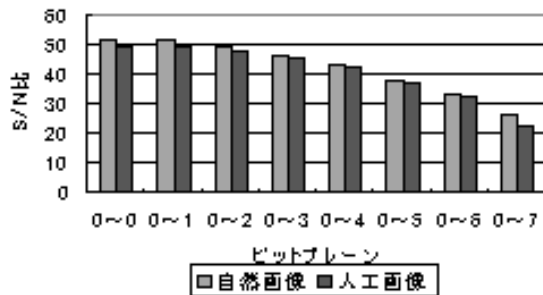


図 2 埋め込み時に輝度補正を行った場合の S/N 比の変化

輝度補正を行わなかったときと比べて S/N 比が上がっている。極端に明るい画素や暗い画素が減ったため、視覚的に評価した場合でも画質が向上した。

5.3 埋め込み位置を画像に依存させる方法

埋め込み位置の決定を画像に依存する場合、それぞれの画像に対して最適な埋め込み位置に秘密情報を埋め込むことができるので、画質劣化を小さく抑えることができる。一方画像に変更を加えられると、埋め込み位置の情報を失い取り出しができなくなる恐れがある。

5.3.1 小領域のパリティを用いた埋め込み

画像を $n \times n$ の小領域に分割しランダムにビットプレーンを選択し、そのビットプレーン上では画像に依存して秘密データを埋め込む。埋め込みには小領域の 1 の数が奇数か偶数かというパリティを利用し、埋め込みたい秘密データとダミー画像のパリティが一致しなければ、最も輝度の差が少なくなる画素を選択し値を反転させる。埋め込み後の S/N 比の変化は図 3 のようになる。

S/N 比が格段に向上しているのがわかる。画質がよいとされる 40dB にビットプレーンの 0~6 と使用したときも達していて、そのとき視覚的に評価しても埋め込みは一見しただけではわからない。

5.3.2 小領域のパリティを用いた埋め込み 2

小領域の大きさを 4×4 に設定し、その中に 2 ビットの秘密データを埋め込む。これによって、埋め込むことのできる秘密データの量は 1.125 倍になる。また、最適

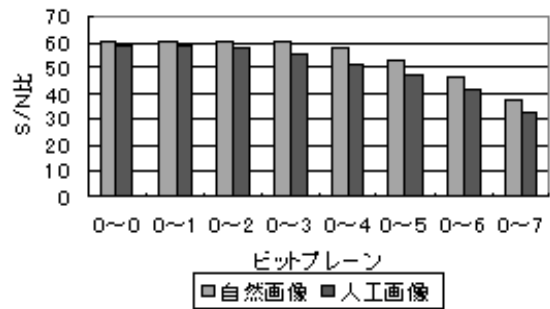


図 3 パリティを利用した埋め込みの S/N 比の変化

な埋め込みを行うための画素の候補が 3×3 のときより増えているので画質の向上も期待できる。

実験をした結果、前述の $n=3$ 、 $m=1$ のパリティに比べて S/N 比が落ちていた。そのため埋め込める容量は増えるものの、S/N 比という点からみると $n=3$ のパリティ埋め込みに劣る。

5.4 輝度補正を利用した複数ビットプレーンに対するパリティを用いた埋め込み

ダミー画像に秘密データを埋め込む際、輝度補正をすることによって秘密データを埋め込むビット以外のビットの値も変化し、それに伴って他のビットプレーンのパリティの値が変化することを利用し、最小限のビットを反転させ輝度補正を行い複数枚のビットプレーンのパリティをすべて秘密データと一致させる。埋め込み後の S/N 比の変化は図 4 のようになる。

前述の $n=3$ 、 $m=1$ のパリティに比べると S/N 比は落ちているが、 $m=6$ の時にも 40dB 以上を達成できた。そのため、埋め込む秘密データの量が多い際には適していると言える。

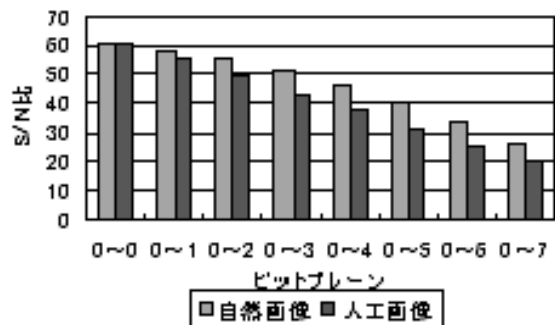


図 4 輝度補正を利用した埋め込みでの S/N 比の変化

6 輝度補正の問題点

輝度補正を行うことにより輝度の劣化を小さくできるので、S/N 比が向上する。また、視覚的な劣化もある程度抑えることができる。しかし、輝度補正を行うと画素を 2 値情報に置き換えたとき、下位ビットから上位ビッ

トに向かって0、1の連続を数えると、連続数の多いものの割合が多くなる。これがなんらかの不自然さを引き起こせば、輝度補正自体が埋め込みの存在を検知される原因になりかねない。

画像サイズ 256×256 の256色白黒濃淡画像を用い、全画素に秘密情報を埋め込んだ。埋め込むビットプレーンの最下位を BP_m 、最上位を BPM とし、埋め込む秘密情報はランダムなビット情報である。 $BP_m = 0$ 、 $BPM = 0 \sim 7$ で検証を行った。全画素について、最下位ビットから上位ビット方向に0または1の連続個数を数え出現回数ごとにまとめ、横軸に連続数、縦軸に出現回数をとり二次関数近似する。このとき、自然画像は二次係数がほぼ全て1100~1300に収まった。秘密情報を埋め込んだ場合では BPM が0または1であるとき二次係数は元の自然画像のものと変化があまり見られない。しかし、 $BPM = 2 \sim 7$ では二次係数が大きく変化し、全て1000未満となった。

3×3 の小領域の固定位置に情報を埋め込んだ場合では、小領域の各位置ごとに連続数を数え、(全画素数/小領域数) 倍し二次関数近似した場合、埋め込み位置のみ二次係数が大きく変化する為、上記と同じ結果が得られる。他の小領域サイズでも同じであると考えられる。

画素の下位から0、1の連続個数と出現回数を使い、二次関数近似しただけでは確実に埋め込みの有無を決めることはできない。しかし $BPM = 0, 1$ 以外では埋め込みを検知できてしまう。これではプログラムによる埋め込み検知に対する耐性が高いとはいえない。よって、視覚的な埋め込みの検知、プログラムによる埋め込み検知の2つから埋め込みの存在がわからなくなるような新たな輝度補正が必要である。

6.1 秘密データが埋め込まれた画像の解析

画素空間利用型 ($n=1, m=1$) で輝度の差が最小になる輝度補正を用いて埋め込みを行ったとき、輝度補正を行ったことによってできた不自然なビットの並びを利用して、秘密データを取り出そうとしたとき、どの程度取り出せるのかを検証した。

表1は特定のビットプレーンのみに秘密データを埋め込んだ際に、Aは上位ビットも利用した輝度補正を行ったと仮定し正しく取り出せた秘密データの割合(%) Bは下位ビットのみを利用したと仮定したときに取り出せた割合(%)である。

複数のビットプレーンに分散して秘密データを埋め込んだ場合、その秘密データを取り出せる割合は、埋め込みに利用したビットプレーンそれぞれから取り出せる割合の平均になるため、利用するビットプレーンの枚数が多くなるほど秘密データを取り出せる割合は減る。

7 ビットプレーンの複雑さ利用型

7.1 ビットプレーンの複雑さ利用型

画像をビットプレーンに分解すると、その状態はノイズ状態のもの、意味のある状態のものに分けることができる。この特徴を利用してノイズ領域に秘密データ

表1 埋め込んだビットプレーン番号と取り出した秘密データの割合(%)の変化

番号	1	2	3	4	5	6	7
A	49.6	49.2	48.4	46.9	43.4	37.5	25.0
B	50.8	51.2	52.0	53.5	56.6	62.9	75.4

の埋め込みを行うのがビットプレーンの複雑さ利用型である[3]。

7.1.1 埋め込み方法

1. ダミー画像の各ビットプレーンを $2^m \times 2^m$ (本研究では $m = 3$ とする) の小領域に分割する
2. 小領域の複雑さ α (以下に定義) を計算し、 α の値が閾値 (0.5 以下) よりも大きい場合、小領域は複雑であるとし埋め込みを行う対象とする。

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

3. 秘密データを $2^m \times 2^m$ の小ブロックに分割する。(秘密データとして、画像、0、1の乱数を用いる。画像を扱う場合は1次元に変換して扱う)
4. 秘密データの複雑さを計算し、その値が閾値よりも小さかった場合コンジュゲート演算を行い複雑なものに変換する。コンジュゲート演算は、複雑ではない2値の秘密データと、市松模様になった2値データとの排他的論理和をとるものである。(コンジュゲート演算は複雑でないものを複雑なものに、複雑なものを複雑でないものに変換する)
5. 秘密データの埋め込みを行う。まず秘密データの大きさ、秘密データがコンジュゲート演算されたかどうかを保持するコンジュゲーションフラグを埋め込む。つづいて、ダミー画像の複雑な小領域に複雑な秘密データを埋め込んでいく。

7.1.2 検証結果

自然画像は下位のビットプレーンのほとんどがノイズ状態になっているものが多いため大容量の秘密データの埋め込みを実現できた。埋め込み量、S/N比については次節の埋め込み方法の結果とともに表2に示す。

しかし、秘密データの大きさ、コンジュゲーションフラグをコンジュゲート演算することなく固定領域に埋め込むため、埋め込み後の画像の最下位ビットプレーンに不自然な状態が見られる。

7.2 コンジュゲーションフラグを画像全体に分散させるステガノグラフィ

この埋め込みは、固定領域に埋め込んでいたコンジュゲーションフラグを画像全体に分散させることによって、最下位ビットプレーンの不自然な状態を改善する埋め込み方法である[4]。

7.2.1 埋め込み方法

1. 秘密データを $2^m \times 2^m$ の小領域に分割する。

2. 小ブロックの1画素をコンジュゲーションフラグとし、秘密データのコンジュゲート演算の有無を保持する。
3. ダミー画像の複雑な小領域に複雑な秘密データを埋め込んでいく。

7.2.2 検証結果

この方法でも大容量の埋め込みを実現できた。また、コンジュゲーションフラグを分散させたことにより最下位ビットプレーンの不自然な状態は改善された。埋め込み量と S/N 比を表 2 に示す。

表 2 Lenna における埋め込み量に対する S/N 比の比較

埋め込み量	複雑さ利用型 (フラグ分散なし)	複雑さ利用型 (フラグ分散あり)
12.5KB	45.88dB	45.86dB
18.75KB	40.61dB	40.53dB
25KB	35.21dB	35.08dB

7.3 複雑さの他の尺度について

[5] では、二値画像の複雑さを定義する際、以下の 3 つの尺度を用いることができるのと述べている。

1. 連結成分数による尺度
2. 境界線の長さによる尺度
3. DF-表現における複雑度

[3]、[4] の埋め込みでは、2 の尺度を用いている。本研究では 1、3 の尺度も用いて埋め込みを行うことができるか $2^m \times 2^m$ の小領域を用いて検証を行なったところ、3 の尺度が実際に利用できると分かった。3 の尺度を用いて埋め込みを行った場合の埋め込み量と S/N 比について検証を行った。

7.3.1 連結成分数による尺度

ある画素とその縦横で隣接する画素との値が等しい場合、この 2 つの画素は連結しているという。連結成分の数を数え、複雑さ α を以下のように定義する。

$$\alpha = \frac{\text{連結成分数}}{4^m}$$

7.3.2 DF-表現における複雑度

素画数 (2 値画像を 4 分木で表現した時の葉ノードの数) を用いた複雑さの尺度である。素画数を数え、複雑度 α を以下のように定義する。

$$\alpha = \frac{\text{素画数}}{4^m}$$

7.3.3 検証結果

この尺度を用いて埋め込みを行い、埋め込み後の画像を比較した。埋め込み量と S/N 比は表 3 である。尺度の違いによる S/N 比の違いは見られなかったことから、DF-表現における複雑度も埋め込みに利用できるといえる。

表 3 尺度の変更における埋め込み量に対する S/N 比の比較

埋め込み量	DF-表現	境界線
12.5KB	45.90dB	45.90dB
18.75KB	40.57dB	40.71dB
25KB	35.15dB	35.29dB

8 おわりに

輝度補正を行った場合、何もしない場合と比較すると S/N 比でも視覚的な評価でもかなり向上した。さらに埋め込み位置を画像に依存する方法を組み合わせた埋め込みでは、画質の劣化を抑えるのにかなり高い効果があることがわかった。小領域の大きさを 4×4 にし、埋め込む秘密データの量を 2 ビットとしたとき、埋め込むデータ量は 1.125 倍となったが、S/N 比は落ちた。

画素空間利用型での埋め込み後の画像を、下位ビットからの同じ値の連続を解析して秘密データを取り出すのは、秘密データが複数枚のビットプレーンに分散配置されていると画素ごとにビット列の並びを分析して取り出す方法では難しい。

ビットプレーンの複雑さ利用型は、ビットプレーンごとの画像の特徴を効果的に利用し、大容量の秘密データの埋め込みと高い S/N 比を実現している。コンジュゲーションフラグを画像全体に分散させる埋め込み方法では、最下位ビットプレーンの不自然な状態を防ぐことができた。また埋め込み量、S/N 比に関してもコンジュゲーションフラグ分散の有無に関わらず高い値を示しているためとても効果的な埋め込み方法である。

2 値画像の複雑さの尺度を変更しても、埋め込み、取り出しを実現できた。この場合も、大容量の埋め込みに対して高い S/N 比を示したことから、ビットプレーンの複雑さ利用型では 2 種類の複雑さの尺度を用いることができるとわかった。

参考文献

- [1] 安藤百恵 福田恵子：“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”，南山大学数理情報学部情報通信学科 卒業論文 (2004.1).
- [2] 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).
- [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 D- Vol.J81-D- No.6(1998.6).
- [4] 新見道治，野田秀樹，河口英二：“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め込み方法”，電子情報通信学会 論文誌 D- Vol.J87-D- No.2(2004.2).
- [5] 谷口倫一郎，河口英二：“二値画像の複雑さと多値画像の閾値処理に関する考察”，電子情報通信学会 論文誌 D Vol.J70-D No.1(1987).