

# 画像ステガノグラフィの Java による初歩的実装

島根大学 総合理工学部 数理・情報システム学科

計算機科学講座 田中研究室

S083005 荒牧 敬祐

## 第1章. はじめに

- 1.1. 研究背景
- 1.2. 研究目的
- 1.3. 研究概要

## 第2章. ステガノグラフィ

- 2.1. ステガノグラフィとは
- 2.2. ステガノグラフィの種類と分別
- 2.3. ステゴデータ隠匿方法

## 第3章. 実装したステガノグラフィ

- 3.1. 作成したステガノグラフィプログラムの概要
- 3.2. 画素置換型ステガノグラフィ
  - 3.2.1. 画素置換型ステガノグラフィについて
  - 3.2.2. 本研究で追加した内容
- 3.3. 周波数特性利用型ステガノグラフィ
- 3.4. 元画像と情報を埋め込んだ画像の差について

## 第4章. 研究成果と今後の課題

- 4.1. ステガノグラフィプログラム
- 4.2. 残された課題

## 文献

# 第1章 はじめに

## 1.1 研究背景

近年、SNS サイトの普及により、個人で撮影した写真、作成したイラストなどの画像データをネット上にアップロードする機会が増えてきた。

そんな中、アップロードされた画像は不特定多数が活動する SNS サイト、個人ブログなどを通して、アップロードした本人が与り知らない所で勝手に流用されるケースなども、それに応じて増えている。

しかし、いつ、誰が、どこで自分のアップロードした画像が使われるかを把握できるかは、追跡の困難なネット上において容易にできるものではない。例えできるとしてもパソコンをネットや資料作成などだけに使う人が多い中、手軽にはできないことではない。

そこでアップロードされる画像そのものに何らかの保護データを埋め込み、かつその技術を容易に使用できる環境があれば、誰でも画像の著作権を保護することができるようになる。

## 1.2 研究概要

本研究では、ステガノグラフィと呼ばれる技術を使用して、著作権を保護できるプログラムを作成することを目的とする。

また、本研究で目的にするのは、bmp 形式の画像データである。

## 第2章 ステガノグラフィ

### 2.1 ステガノグラフィとは

ステガノグラフィとは、あるデータを他のデータの中に埋め込んで、そのデータの存在を隠し秘密状態でやりとりする、情報ハイディング技術の一つである。[1]

データを秘密裏にするには暗号化するのが望ましいが、暗号化した情報は容易に人の目についてしまう。

しかしその暗号化したデータを他のデータに埋め込んで、データそのものを隠してしまうことで、秘密データの露見を抑えることが可能となる。これがステガノグラフィの基本である。

また、一つの特徴として、ステガノグラフィは主にデジタルコンテンツのデータの中に埋め込まれるが、表から見えるデータには、ほとんど変化はみられないというものがある。これにより、秘密データを埋め込んだデータと、秘密データを埋め込んでいないデータを判別することは難しく、例えば誰かに表データを見られても、中に埋め込んでいるデータが露見する心配は少ない。

また類似技術として電子透かしというものがあり、デジタルコンテンツを不正利用されないために著作権情報を示すための情報を埋め込み、そのデジタルコンテンツを保護することを主な目的にした技術である。[2]

例えば画像や音声データが流出しても、埋め込まれた透かしを使って著作権を主張することができ、古くから情報ハイディング、情報セキュリティの技術としてあらゆる世界で使われていた技術である。

これだけ見れば類似技術である電子透かしを利用したほうが有用ではないか、と思うかもしれないが、電子透かしとステガノグラフィは、その目的と保護するデータが異なっている。

以下、表1はそれをまとめた表になる。[3]

	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技術	外に現れた情報(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.1-1. ステガノグラフィと電子透かしの違い

電子透かしはデータを埋め込んだ画像や音声などのデータに価値を置くのに対し、ステガノグラフィはむしろ画像や音声データに埋め込んだ秘密データそのものに価値をおく技術である。

位置づけを示すと、以下の図で表される。

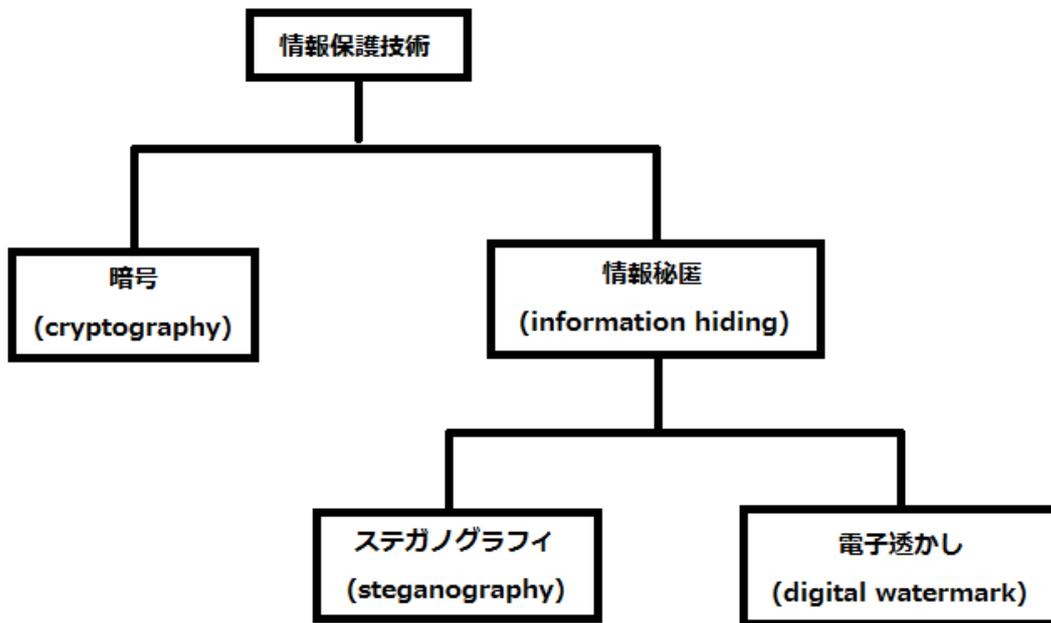


図 1-1. ステガノグラフィと電子透かしの関連性

著作権保護の観点から見れば電子透かしの技術のほうが望ましいと思えるが、本研究では埋め込んだ秘密データに価値をおく構造になっているため、ステガノグラフィ技術の研究と称することにした。

## 2.2 ステガノグラフィの種類と分類

デジタルデータに秘密データを埋め込むにしても、ただそのままデータに手を加えただけでは、埋め込んだ画像や音声データが変化してしまい、すぐにデータを埋め込んでいることが露見してしまう。

ステガノグラフィでは、秘密データを埋め込んでも、簡単には画像データや音声データが大きく変化しない手法をとり、情報を隠匿する。

その手法は大きく分けて、以下の2種類に分類される。[4]

### ① コンテンツの中の冗長性を含むデータ内に埋め込む手法

画像データ、音声データ、映像データなどのデジタルコンテンツの中には、変更しても表にはあまり変化が見られないデータ、特に意味を含まないデータ、人間が知覚できないデータなど、冗長性を含むデータが存在する。

それらのデータは、まったく別のデータと置き換えたり、余分な情報を追加しても表データにはほとんど影響は見られない。

この特性を利用して秘密データを埋め込むのが、冗長性にデータを埋め込む手法である。

デジタルコンテンツの標本値を置き換えたりする手法などが、これに該当する。

### ② 人間の生理的特性を利用した手法

人間の感覚は非常にルーズであり、ある条件下で特定の刺激に鋭くなったり鈍くなったりするなどの特徴がある。

これにより、特定の条件を満たしていれば、秘密データを埋め込んで音声や画像が乱れても、人間からは知覚ことはできず気付くことがない。

例えば輝度値の大きいデータと小さいデータが隣り合っていた場合、直前、あるいは直後の小さい刺激に対しては、人間の視覚は鈍感になる。複雑な情報の中で、細かな変化は人間は知覚できない、などの特性が存在する。

これら特性を利用したのが、生理的特性を利用した手法になる。

後述する周波数成分を使用したステガノグラフィによく使われる手法である。

## 2.3 ステゴデータの隠匿方法

ステガノグラフィや電子透かしは、これらを利用して情報を埋め込んでいる。しかし、上記した特性は、あくまでどういう部分に秘密データを隠匿するかであって、実際に埋め込む手法は別に存在する。

本研究では画像ステガノグラフィに限定しているが、画像に対するステガノグラフィ、も大まかに分けて、以下の2つに分類することができる。

### ① 画素情報を利用したステガノグラフィ

画像データを構成するピクセルデータのの一つ一つに含まれる輝度、色度などの標本値を利用したステガノグラフィ。

直接標本値に秘密データを埋め込んだり、置き換えたりする手法で、標本値の中でも冗長性のあるデータを選び、そこにデータを隠匿する。

複雑な手続きを踏まないため、後述する周波数成分を利用したステガノグラフィに比べて埋め込みが容易であり、処理時間や開発コストが小さくて済むというメリットがある。

一方で隠匿されたデータは標本値としてそのまま画像のデータとして残るため、画像の変質には弱く、画像の圧縮、加工などによって埋め込んだデータが破損してしまうというデメリットがある。

また、このような埋め込み方式は通常、「定まった場所」に情報を埋め込むため、秘密データを埋め込んだという事実が比較的容易に見破られやすく、同時に埋め込んだデータを抜き取ったり、すり替えたりされやすいという点もデメリットとして挙げられる。

これらの具体例として画素置換型ステガノグラフィや、色差情報を利用したステガノグラフィなどが存在する。

### ② 周波数成分を利用したステガノグラフィ

近年主流とされているステガノグラフィで、一旦画像を周波数成分に変換し、その中で画像に影響の少ないとされる部分に周波数を埋め込んでいく手法。

周波数成分に変換すると、その画像を構成するデータの特徴を把握しやすくなり、どこが重要なデータで、どこに冗長性があるかなどが分かりやすくなる。

画像を周波数成分に変換する方法としては、フーリエ変換(FT)、離散コサイン変換(DCT 変換)などの手法が挙げられる。

周波数成分に変換し、その中で特定の領域にのみ周波数を埋め込んだ後に逆変換で再び元に戻すという手法をとるため、画素情報利用型のステガノグラフィと比べて、処理時間も開発

コストも大きくなりがちである上、埋め込める情報も場所を選ぶ分、どうしても少なくなってしまう。

しかし意図して冗長性のあるデータや、人間が知覚しにくいデータを選んで秘密データを埋め込めるので、画像自体への影響は少なく、また手法が複雑な分、秘密データが埋め込まれているのかどうかを見破られにくい。

加えて圧縮、加工などの画像の変質にも強く、ある程度の変化であれば中に埋め込んだデータが壊れることが少ないというメリットがある。

上に挙げた2種類のステガノグラフィは、それぞれメリットとデメリットが真逆であり、手法に応じて使い分けていく必要がある。

また、大まかに分けて2つに分類したが、これ以外の情報を利用したステガノグラフィ技術が次々開発されているため、ミクロな視点から見ると、これ以上の種類に分類できるようになると考えている。

## 第3章 実装したステガノグラフィ

### 3.1 作成したステガノグラフィ

本研究では、bmp 画像に対するステガノグラフィを目的としており、前の章で説明した2種類の手法に対応するステガノグラフィをそれぞれ1つずつ作成した。

本章では作成したステガノグラフィプログラムについて記述していく。

### 3.2 画素置換型ステガノグラフィ

#### 3.2.1 画素置換型ステガノグラフィについて

画素置換型ステガノグラフィとは、画像を構成するビットプレーンそのものを秘密データと置き換える手法である。

濃淡画像やフルカラーbmp 画像は、 $2^0$  から  $2^7$  の8つのビットプレーンから構成されており、 $2^7$  を表すビットプレーンを最上位ビット(MSB)、 $2^0$  を表すビットプレーンを最下位ビット(LSB)という。(図 3-1)

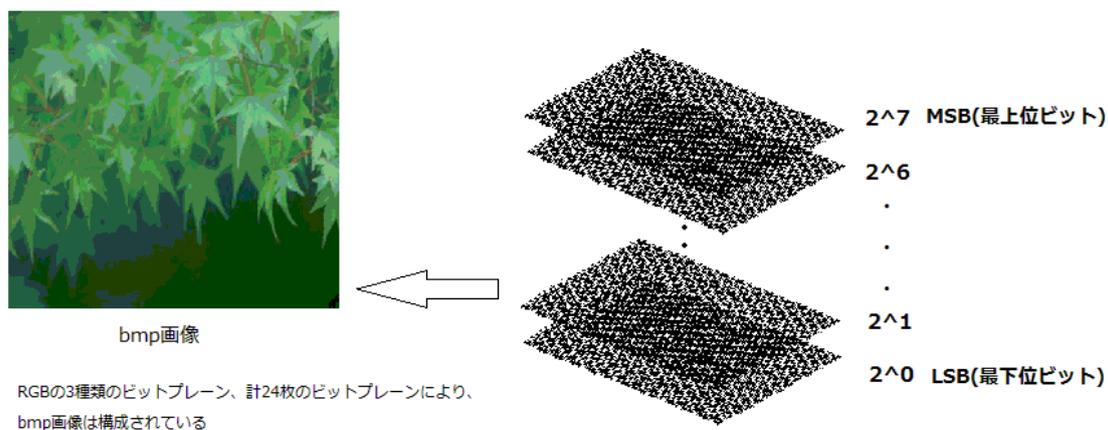


図 3-1. bmp 画像を構成するビットプレーン

最下位ビットは、数値を変更しても画像全体に影響する割合は非常に少なく、例え全てを変更しても、画像への視覚的影響はほとんどないに等しい。

この特徴を利用して、最下位ビットを隠匿する秘密データと置き換えることによって、画像への影響を最小限にしてデータを埋め込むことが可能になる。

また最下位ビット以外にも、 $2^1$  のビットプレーンまでなら画像への影響は比較的少なく、下位2ビットまでを使用するステガノグラフィなら、従来の画素置換型ステガノグラフィの倍の情報

を埋め込むことが可能となる。しかし今回は都合上、最下位ビットのみを使用したステガノグラフィで作成している。

埋め込める大きさは、1画素につき、RGB成分の3つのビットプレーンの最下位ビットである計3ビットである。

よって1文字を8ビットと考え、3画素を使用して1文字を埋め込める計算になる。

### 3.2.2 本研究で追加した内容

この方式は典型的なステガノグラフィとして知られており、初歩的なステガノグラフィといえ、この画素置換型が挙げられる。

しかしこの画素置換型のステガノグラフィは、前述した画素情報利用型のステガノグラフィのデメリットに加え、埋め込める数、埋め込み位置がほぼ固定化されてしまう、という欠点が存在する。

通常これら为了避免するには、ファイルのヘッダ情報を使用するなどして、埋め込み文字数や散らばせた場所などを別ファイルとして保存する必要が出てくる。

今回作成した画素置換型ステガノグラフィは、埋め込んだ文字数や散らばせた位置をヘッダ情報を使用せずに、画像を読み込むことで判別させる方式をとっている。

今回作成した画素置換型ステガノグラフィを使って埋め込む秘密データは、二つの部分に分割することができる。

埋め込み情報を記載した情報部と、実際に埋め込む秘密データについて記載したステゴデータ部の二つである。

以下、図3-2.に簡易説明を用意した。

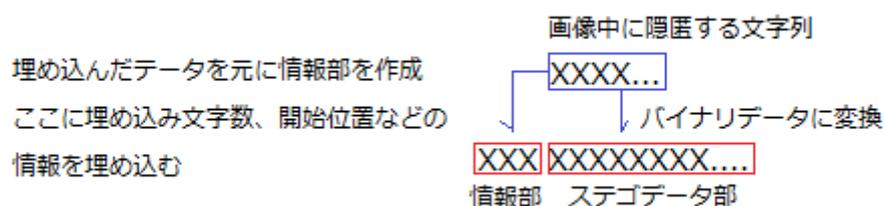


図3-2. 実際に埋め込むデータ

まず前半部の情報部には、埋め込むステガノグラフィの文字列の数と、後述する埋め込みを散らばらせる機能についての情報をつめてある。

この情報部分は全部で9ビットの大きさであり、いかなる場合でも先頭3画素の部分に埋め込まれる。また、この情報部が拡大したり縮小することはない。

まず先頭部分の2bitで埋め込んだ際に使用した機能について調べ、その後続く7bitで

埋め込んだ情報量の長さを測定する。

これにより、最大 127 文字のデータを自由に埋め込むことが可能となり、ステガナリシス(複合化)を行う際に、過不足なく埋め込んだ情報を取り出すことができる。

後半のステゴデータ部は、隠匿する文字列を 2 進数に変換した情報であり、実質このデータが隠匿データそのものである。

これらデータを画素置換型の方法を用いて、bmp 画像に埋め込む。

隠匿するデータは、通常画像情報の先頭から順次埋め込まれていくことになる。

しかしその場合、埋め込みデータを分散させることができず、第三者の手で容易に情報を抜き取られてしまう可能性が出てくる。

そこで、埋め込むステゴデータを分散できるよう、以下の 2 つの機能を追加した。

#### 1. 先頭から順にカウントしていき、偶数番目にのみステゴデータを埋め込む手法

この手法の仕組みは単純で、データ埋め込み部分前の処理を以下のように変更する。

一つの画素を読み込む度に数字をカウント。その際にカウント数が奇数の時は処理をスキップし、次の画素を読み込む。そして偶数の時は埋め込み処理を続行する。

```
for (y=0; y<image.getHeight(); y++) {
    for (x=0; x<image.getWidth(); x++) {
        if(count%2==0) Steg(x,y);
        count++;
        if(Pass[i]==null) break;
    }
    if(Pass[i]==null) break;
}
```

これにより埋め込み容量は従来の 1/2 になってしまうものの、埋め込む画素データを間隔的に散らせることが可能になる。

## 2. 輝度が 170 以上の画素データにのみステゴデータを隠匿する手法

この手法は、画素データを読み込んだ際にその輝度値が  $170(10101010)_2$  以上だった場合にのみ埋め込み処理を行い、それ未満の時は処理をスキップする仕組みである。

通常人間の目は、刺激や周波数の高い部分での僅かな変化に鈍感になるという特性をもっている。

これを利用して、輝度情報がより高めの部分にのみ隠匿データを埋め込むことにより、画像中に埋め込んだステゴデータに気づかれにくくすると共に、ステゴデータの埋め込み位置を分散させることができる。

なぜ輝度が 170 であるかという、輝度値が比較的高めであるということ、あまりに高い値で設定してしまうと、埋め込む容量が極端に小さくなってしまうこと、バイナリデータの 1bit 目が 0 であることに由来する。

もし 1bit 目が 1 である輝度値に設定した場合、埋め込み後に値が 0 になった時に、ステガナリシスにて埋め込んだ画素データをスキップしてしまう可能性があるからである。

この機能は前者の分散プログラムに比べ、ランダム性のある散らばらせ方ができるものの、画像全体の輝度値が低い場合など、ステゴデータを埋め込むことができなくなる可能性もある。

### 3.3 周波数特性利用ステガノグラフィ

しかし前述した画素置換型のステガノグラフィは、頑健性の部分に関しては未だ脆弱であり、画像の加工や圧縮を行えば情報部も壊れてしまい、正常な情報を画像から抜き出すことができなくなる。

そこでその頑健性カバーさせる形で作成したのが、この周波数特性利用型のステガノグラフィである。

このステガノグラフィでは、DCT (Discrete Cosine Transform) 変換と呼ばれる変換方式を利用している。これは画像データを周波数成分に変換する直交変換技術のひとつで、jpeg 画像などの基底技術として使われている。

以下(式 3.1)が、その DCT 変換の数式である。

$$F(u,v) = 2/N c(u)c(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\{(2x+1)un/2N\} \cos\{(2y+1)vn/2N\}$$

$u=0$  または  $v=0$  のとき  $c(u)=c(v)=1/\sqrt{2}$

$u \neq 0, v \neq 0$  のとき  $c(u)=c(v)=1$

$F(u,v)$  : 求めるDCT係数

$f(x,y)$  : 画像信号  $x,y$  : 画像の座標

$\sum_{x=0}^{N-1} \sum_{y=0}^{N-1}$  : 画素数

(式 3.1) DCT 変換式

まず情報を埋め込む画像内の画素データを、 $8 \times 8$  の画素ブロックで分割し、そのブロックごとに DCT 変換を行う。

$8 \times 8$  で分ける理由は、この数が一番ノイズの少なさと、実行時間のバランスが優れているからである。[2]

ここでいうノイズとは、 $8 \times 8$  画素のブロック単位で周波数成分を計算し、不要な部分が削除されるので、この削除の程度がブロック毎によって異なっていることを指す。この差が目立ってしまうことをノイズいう。

この分割した画素を DCT 変換することで出力  $F(u,v)$  が得られるが、この出力のうち、 $F(0,0)$  の出力成分を DC 係数と称し、 $8 \times 8$  で区切った画素ブロック全体の明るさを表している。

そして残りは AC 成分といい、その画素ブロック内の周波数成分を示している。この周波数成分は、 $(u,v)$  の値が小さいほど低周波成分を表し、逆に高ければ高いほど高周波成分を表している。(図.5)



図 3-3. DCT ブロックの各成分

さて、前述したとおり、人間の生理的特性として、高周波成分の刺激には鈍感になってしまうという特性がある。そこで、この画素ブロックのもっとも高い周波数を表している、右下隅の AC 成分に情報を埋め込むことで、画像データにほとんど影響させることなく、ステゴデータを埋め込むことが可能になる。

今回の場合、各ブロックを  $8 \times 8$  で分割しているので、 $F(7,7)$ 成分が、埋め込まれる AC 成分にあたる。

これを画像全体の各ブロック毎に施し、すべてのステゴデータを埋め終えることができれば、逆 DCT 変換(式 3.2)で周波数成分から元画像に変換し、周波数特性利用型のステガノグラフィは完了する。

$$f(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c(u,v) F(u,v) \cos\{(2x+1)u\pi/2N\} \cos\{(2y+1)v\pi/2N\}$$

$f(x,y)$  : 画像信号       $F(u,v)$  : DCT係数

(式.3.2) 逆 DCT 変換

この方式だと、頑健性がある程度あり、画像の圧縮にも対応できるようになる上、一度周波数成分へと変換させてからでないと、画像内に秘密データが隠匿されているか否かを判断するのは難しい。

しかし一方で、 $8 \times 8$  のブロックの画素に 1bit しか埋め込めないという容量上の欠点もあり、機能を使わなかった通常の画素置換型のステガノグラフィと比較して、 $1/192$  の容量しか埋め込むことができないというデメリットも存在する。

### 3.4 元画像と情報を埋め込んだ画像の差について

以上が今回作成したステガノグラフィプログラムになる。

では実際動かしてみて、どのような画像が出るのか。本当に元画像と比べて差が出たりはしないのかについてここで説明する。

以下の bmp 画像は、これからステガノグラフィを行う前の元画像である。



図 3-4.ステガノグラフィ前 元画像[7].出典

これをステガノグラフィを使用して変換してみる。また、埋め込む文字列は双方とも「Steganography」である。以下その結果である。



図 3-5. 画素置換型ステガノグラフィ[7].出典

これが画像置換型ステガノグラフィで処理した後の画像である。分散させる機能などは使っていない。

標本値を直接変更しており、画像の一部を拡大してみない限りには、画像に変化があるかは分からない。しかし元画像と比較し、差分を求めるプログラムなどで検査した場合はその限りではない。



図 3-6. 周波数成分利用型ステガノグラフィ[7]. 出典

上図は周波数成分を利用したステガノグラフィである。

こちらは画素置換型とは違い、影響は各ブロックごとに現れて入るので、ノイズの影響下一部画像が荒れているようにも見える。

しかし些末な影響であり、一目見た限りではどこになにの影響があるかはまったくわからないため、仮に判別できたとして、情報が埋め込まれている場所や方法は判断される心配は少ないと思われる。

これは、複雑な刺激の中でのわずかな変化に対して人の視覚は鈍感になるという特性によるところもあり、逆に平坦な画像。それも輝度の非常に低い値の画像に対しては、違う結果が出るのではないかとの疑問もある。

そこで、色度 0 の平坦な画像に対しステガノグラフィを行っても、画像に変化はないかを調べてみた。

以下の画像がその結果である。

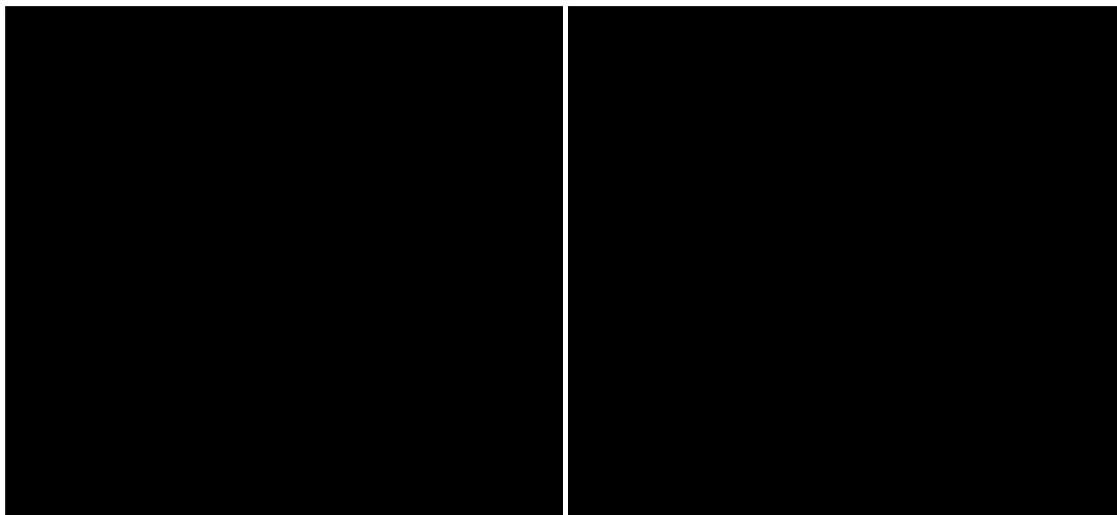


図 3-7 - 図 3-8. 埋め込み前画像と埋め込み完了後の画像

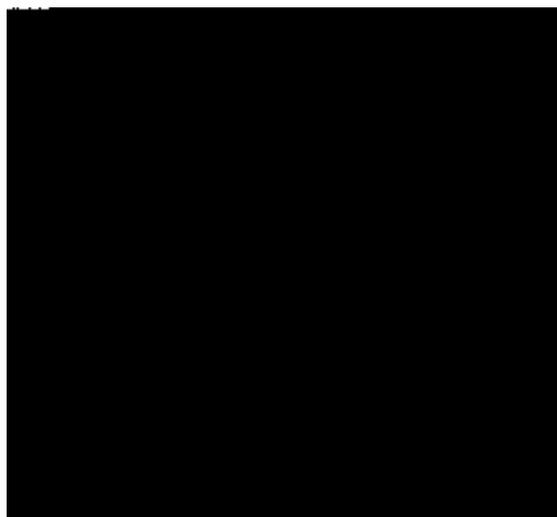


図 3-9.画像差分

使用したステガノグラフィは画素置換型で、左上の画素データが僅かながらに書き換えられている。

しかし人間の特性の一つとして、隣り合う同じ刺激が微小の変化をしても、その変化を感じ取れないというものがあるため、見ての通り視覚的变化は少なく、例え色度の低い平坦画像であっても、最下位ビットの変更などの僅かな変化だけであると、画像の変化に気づかれる心配は少ないと思われる。

## 第4章 研究の成果と今後の課題

### 4.1 ステガノグラフィプログラム

本研究で作成したプログラムは、ステガノグラフィプログラムとステガナリシスプログラムの2種類あり、操作方法としては画像 URL を入力と埋め込む文字を入力し、ボックスなどでステガノグラフィの種類を選択。



図 4-1. ステガノグラフィプログラム動作例

その後、ステガノグラフィ処理を行った画像データが `out.bmp` の形で出力されて、ステガノグラフィは完了する。

その後、この画像をステガナリシスプログラムに入力し、そのステガノグラフィプログラムにあった方式を選択すると、以下の様な `txt` ファイルが出力される。

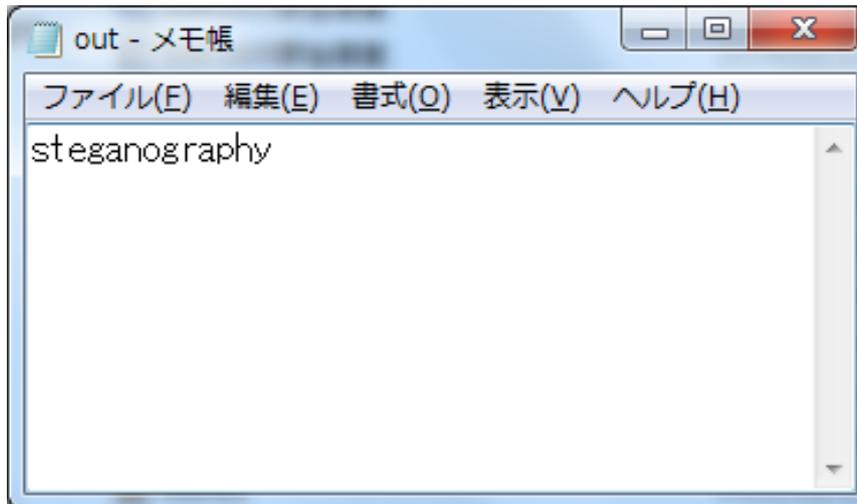


図 4-2. 出力ファイル

なお、一度情報を埋め込んだ画像データは、ステガナリシスプログラムにかけたとしても情報は保存されたままである。

そのため、不必要になった画像データは削除を自力で行う必要がある。

## 4.2 残された課題

本研究で作成したステガノグラフィプログラムは、その双方とも頑健性に問題があり、外からの攻撃には脆弱なままである。

また、bmp 画像にのみ対応しているため、今日多く使われている jpeg、png などにはこのプログラムは使えない。また、他の画像形式に変換した場合、即座に壊れてしまう上、twitter など、特別な変換方式を行いアップロードされるものなどにも弱いという問題を残している。

このため、頑健性の強化のほか、他の画像方式に対応できるステガノグラフィを作るという課題が挙げられる。

## 謝辞

本研究にあたり、最後まで熱心な御指導をいただきました田中章司郎教授には、心より御礼申し上げます。

また、田中研究室皆様には、本研究に関して数々の御協力と御助言をいただきました。厚く御礼申し上げます。

なお、本論文、本研究で作成したプログラム及びデータ、並びに関連する発表資料等のすべての知的財産権を、本研究の指導教官である田中章司郎教授に譲渡致します。

## 参考・引用文献

- [1] 電子情報通信学会知識ベース: [http://www.ieice-hbkb.org/files/01/01gun\\_03hen\\_13.pdf](http://www.ieice-hbkb.org/files/01/01gun_03hen_13.pdf)
- [2] 電子透かし技術とステガノグラフィ技術 SBINS Developer Center :  
[http://dev.sbins.co.jp/digital\\_watermarking/04b.html](http://dev.sbins.co.jp/digital_watermarking/04b.html)
- [3] 「デジタル・ステガノグラフィ技術について」、野田秀樹、新見道治、河口英二著、画像電子学会誌
- [4] 画像内暗号を用いた C/S 型ログインモジュールの開発、島根大学、田中研究室、田辺知里
- [5] 「電子透かしとコンテンツ保護」、小野 東 著、オーム社
- [6] 「電子透かしの基礎」、松井 甲子雄 著、森北出版株式会社
- [7] フリー素材写真集 <http://sozai-free.com>: