J-020

BPCS ステガノグラフィにおける複雑領域分割のための閾値設定と下位ビット置換に関する評価

阿部　美智子†　　山本　富士男†　　宮崎　剛‡
Michiko Abe　　Fujio Yamamoto　　Tsuyoshi Miyazaki

1. はじめに

機密情報を安全に保持する方法として現在幅広く使われている技術に暗号化がある。暗号化は“鍵”と呼ばれる数字や記号が不規則に並んだ文字列と、データの順序を入れ替えるアルゴリズムを組み合わせて行う。通信分野で使用される暗号化鍵としては、共通鍵暗号の DES や公開鍵暗号の RSA が有名である。しかしこれらの方法では暗号化された内容が人には理解できない文字の羅列となるため、第三者はそれが機密情報ではないかということを容易に判断できてしまう。そこで、機密情報の存在そのものに気付かれないよう保存・やり取りする技術にステガノグラフィがある。ステガノグラフィは秘密にしたい情報をダミーデータと呼ばれる別の情報（文章・画像・音楽等）に埋め込むことで、秘密情報の存在そのものを第三者から隠してしまう技術である。情報を埋め込む手法については既にいくつか提案されているが、本研究では画像を用いた情報秘匿を取り上げる。画像を用いた情報秘匿は情報を埋め込む際、可逆圧縮を利用した場合[1]などを除いた殆どの場合で画像の劣化が生じる。画質と埋め込んだ情報量とはトレードオフの関係にあるため、どちらか一方を断念せざるをえないのが実情である。

本研究では、BPCS（Bit-Plane Complexity Segmentation：ビットプレーン複雑さ領域分割に基づく）ステガノグラフィ[2][3]の複雑領域を分割する際に使用する閾値と、下位ビット置換法についての評価を行った。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 値画像のうち、複雑とされる領域を利用するもので、画質を保ちつつ大量の情報を埋め込むことができる情報秘匿技術である。情報を埋め込む際には、原データに影響しない値に閾値を固定したものや、LSB（Least Significant Bit：最下位ビット）置換法等がある。今回は新たに変動する閾値と、下位ビット置換を 3，4 ビットに拡張した方法を追加し、それぞれの埋め込み方法を実験し、有効性の評価を行った。

2. 画像深層暗号化法

2.1 BPCS ステガノグラフィ

まず BPCS ステガノグラフィの特徴について説明する。画像深層暗号を実現する方法はこれまでいくつか提案されてきたが、殆どの場合ダミーデータに対して僅かな情報しか埋め込むことが出来なかった。これに対し BPCS ステガノグラフィは画像の冗長性に着目し、ダミーデータの 40～50%程の機密情報を埋め込むことに成功している[3]。情報を埋め込む際はダミー画像をビットプレーンに分解して得られる 2 値画像を利用する。この 2 値画像のうちノイズ状の部分を別のデータで置き換えることで大量データの埋め込みが可能になる。

†神奈川工科大学大学院工学研究科，‡神奈川工科大学情報学部情報工学科

2.1.1　ビットプレーン分解

本実験ではフルカラーBMP を使用する。BMP 画像は 1 画素を表現するのに RGB それぞれ 8 ビットと光度の、合計 32 ビットを用いている。このうち色を表す 24 ビットを 3 色に分解し更に色ごとに桁で分解していくことで、合計 24 枚の 2 値画像（ビットプレーン画像）を得ることができる。通常、画像は純 2 進数表現（Pure Binary Code、以下バイナリコード）で表されるが、グレイコードによる表現も可能であり、今回あわせて実験を行う。

ビットプレーンは各画素を表現する値のうち、同じ桁の成分だけを取り出したものである。その特徴は、生成されたプレーンデータのうち上位桁ほど原画像に与える影響が強く、下位桁に進むにつれて原画像に与える影響が少なくなることである。そのため上位桁を加工すると、下位桁を同じように加工した場合に比べ変化が顕著に現れる。

2.1.2　複雑領域

複雑領域とは、2 値画像を小領域に分割した際、一定以上の複雑さを持った小領域だけを選り分けた部分である。2 値画像の複雑さを表す標準的な定義は存在しないということなので、論文[3]で提案されている白と黒の境界線の長さを利用した方法を使うことにする。白と黒の境界線とは 2 値画像における白と黒の境目のことで、長さはその合計である。複雑さ α は次式で与えられる。

$$\alpha = \frac{\text{実際の境界線の長さ}}{\text{境界線の最大長}} \quad (0 \le \alpha \le 1)$$

又、境界線の最大長は市松模様で与えられ、最小値は真白もしくは真黒の画像のときの 0 である。

一定以上の複雑さを持っているか否かの判断には閾値 α_0 を使用する。$\alpha_0 \le \alpha$ となる小領域が複雑領域とみなされ、秘匿情報を埋め込む場所となる。

実験ではビットプレーン分解された 2 値画像を更に 8×8 ピクセルの小領域に分割する。その小領域の複雑さを測定し、得られた複雑さと閾値との大小関係により小領域を複雑な領域とそうでない領域とに分けていく。

2.1.3　コンジュゲート演算

複雑さが α_0 以上である領域にデータを埋め込む場合、埋め込むデータの複雑さも α_0 以上である必要がある。そのための方法としてコンジュゲート演算[3]がある。コンジュゲート演算は複雑でない画像に対し市松模様との排他的論理和を計算することで、画像に簡単に複雑さをもたせることが出来る。又、演算前と演算後の画像の複雑さの和が 1 になる特徴を持っている。

2.2 LSB 置換法

LSB 置換法は最下位ビットを利用した情報秘匿技術であり、電子透かしなどにも利用されている。画像であれば、1 画素を現すデータの最下位部分に情報を埋め込む。今回行う実験の都合上、下位ビット置換は閾値に 0 を指定しているものとして扱う。

3. 閾値の設定

閾値α_0として、全てのプレーンで値を固定したもの、下位桁から上位桁に向けて値が上昇するもの、下位ビットを置換するものを用意した。下位ビット置換については 2.2 で触れたように、秘匿に使用するプレーンの値を 0 に固定した閾値として扱っている。

3. 1 一般的な閾値

普通閾値は固定したまま使用する。画像の劣化を抑えつつ最大限に秘匿領域が得られる値α_0を特定し、それを全てのプレーンで使用するのが一般である。又、閾値が 0.5 を超えることは無い。これはコンジュゲート演算の性質である、演算前と演算後の複雑さの和が 1 になることが関係している。次のような場合、埋め込んだ情報を取り出せなくなることがある。

仮に閾値をα_0'(>0.5)に設定した場合、埋め込む秘匿情報の複雑さαがα_0'以上にならないことがある。それは秘匿情報の複雑さαが$1-\alpha' < \alpha < 0.5$ もしくは $0.5 < \alpha < \alpha'$となったときである。情報を取り出す際は設定された閾値を頼りに走査を行うが、この場合演算を施しても$\alpha_0' \leq \alpha$となることは無いので、このまま情報を埋め込んでもα_0'を頼りに情報を取り出すことは出来ないのである。

このようにα_0が 0.5 を超えると、閾値を頼りに秘匿情報を取り出せる保障がなくなってしまうためα_0の上限は 0.5 となる。

3. 2 新たに提案する閾値

今回新たに提案するのは変動する閾値である。これは閾値を変化させることで、情報を埋め込んだ後の画像の劣化を抑える、もしくはより多くの秘匿領域を得ようというものである。

複雑さにより領域分割を行う場合、まず 8×8 ピクセルの小領域に分割する。そして各小領域の複雑さを測定し、閾値との大小関係から複雑な小領域とそうでない小領域とに分けていく。この際使用する閾値には特定の値を設定し、全てのプレーンにおいてその値を使うのが普通である。しかしビットプレーン分解で生成したデータは、原画像に与える影響の少ない下位桁のほうが埋め込みに適している。そこで下位桁での閾値を低くし、上位桁に行くにつれて閾値が上がるように設定する。こうすることで原画像への影響が少ない下位桁に秘匿情報の大部分を埋め込むことが可能になる。

3. 3 小領域の構造

本実験でも画像を分割する際は 8×8 ピクセルの小領域を利用する。よって埋め込む秘匿情報も 8×8 ピクセルの 2 値画像に変換される。この小領域は次の内容で構成されている。

- 秘匿情報本体
- コンジュゲート操作の有無
- 秘匿情報のバイト数
- 最後の領域か否か

3. 4 0.5 をこえる閾値への対応

今回提案した変化する閾値は 0.0～1.0 の値をとる。しかし閾値が 0.5 を超えるとコンジュゲート演算との兼ね合いから、埋め込んだ情報を取り出せなくなる可能性がある。そこで 3.3 で説明したものとは異なる構造の小領域を作成する。その小領域は以下の内容で構成される。

- 秘匿情報本体
- コンジュゲート演算の有無
- 最後の領域か否か
- 最後の領域か否か
- 次の小領域を指すポインタ

閾値が 0.5 を超えた場合は、閾値を頼りにせず次の小領域を指すポインタをたどって秘匿情報を取り出していく。このポインタは次の小領域が埋め込まれている場所を、色・桁・2 値画像内における位置で与える。又、情報を埋め込む際は埋め込むデータの複雑度が 0.5 以上になるようコンジュゲート演算を行っている。

4. 実験

用意した閾値を評価するため、テスト画像に対して各閾値で得られる秘匿領域全てにテキストデータを埋め込む実験を行う。評価方法は、埋め込み後の画像の劣化具合と埋め込んだデータの量を数値化したものを使用する。更にバイナリコードとグレイコード(今回は反転グレイコードを使用)それぞれに対してビットプレーン分解を行った場合の情報秘匿も試みた。2 種類のコード表現を使用した理由は、秘匿容量や情報埋め込み後の画質を比較し、どちらがより高い効果を得られるか検証するためである。

4.1 使用するデータ

(1) ダミー画像

実験では、ダミー画像として JISX9201:1995 による標準カラー画像(8 枚)を高さと幅が 360 ピクセル以下になるよう縮小し、RGB で保存したものを使用する。

(2) 秘匿データ

秘匿データには「理工系の Java プログラミングテキスト」(著者：山本富士男　出版：技術評論社)の画像を省いたテキスト部分のみを使用する。

4.2 評価方法

各閾値の評価は、どれだけ多くの情報を埋め込むことができたかと、埋め込んだ後の画質を測定することで行う。評価のために次の値を定義する

(1) 埋め込み率(RATIO)

ダミーデータである画像に対しどれだけのデータを埋め込むことが出来たかを次の式で定義する。値が大きいほど 1 画素あたりに埋め込んだデータが多いことを示す。単位は[bit/pixel]で示し以後[b/p]と表記する。

$$RATIO = \frac{volume}{WH} \quad [bit/pixel]$$

- volume：秘匿情報の量(単位：bit)
- WH：画素数(高さ×幅)

(2) ピーク信号対雑音比(PSNR)

ピーク信号対雑音比は画像の信号と混入したノイズを測定する際に使用される。通常は濃淡画像で計算するのが普通であるが、実験ではカラーに拡張したものを使用する。

PSNR は値が小さいほどノイズの混入が多いことを示し、ノイズが全く混入していなければ値は無限大となる。一般に、値が 40[dB]以上であれば視覚的に原画像との区別は困難とされ、値が 20[dB]付近まで下がると見るに耐えない画像となる。利用目的から、それほど高い画質を必要としているわけではないため、目視による確認により 37[dB]以上であれば使用に耐えると判断する。

$$MSE = \frac{1}{WH}\sum_{w=0}^{W-1}\sum_{h=0}^{H-1}\sum_{c=r,g,b}\{c(w,h)-c'(w,h)\}^2$$

$$PSNR = -10*\log_{10}\frac{MSE}{\max R^2+\max G^2+\max B^2} \quad [dB]$$

- MSE：平均二乗誤差
- c'：原画像
- c：埋め込み後の画像
- maxR,maxG,maxB：各色成分の最大値(255)

尚、本研究は人の視覚特性を利用したものなので本来ならば主観評価を行うべきだが、主観評価のみではばらつきがあり信憑性に欠けると判断し、客観的な尺度としてPSNR を使用した。

4.3 使用する閾値

用意した閾値を用いて情報の埋め込み実験を行う。実験で使用する閾値は次の 7 種類である。括弧内の値は左が下位桁、右が上位桁の閾値である。値が 2.0 に設定してあるところはその桁の 2 値画像に対して埋め込みを行わないことを意味する。また値に 1.0 が設定してあるところは、小領域が市松模様になっている場合のみ埋め込みの対象にすることを示している。

- k1 = {0.5, 0.5, 0.5, 0.5, 0.5, 0.5, 0.5, 0.5}
- k2 = {0.4, 0.4, 0.4, 0.4, 0.4, 0.4, 0.4, 0.4}
- h1 = {0.0, 0.2, 0.4, 0.6, 0.8, 1.0, 2.0, 2.0}
- h2 = {0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.8, 1.0}
- s1 = {0.0, 2.0, 2.0, 2.0, 2.0, 2.0, 2.0, 2.0}
- s3 = {0.0, 0.0, 0.0, 2.0, 2.0, 2.0, 2.0, 2.0}
- s4 = {0.0, 0.0, 0.0, 0.0, 2.0, 2.0, 2.0, 2.0}

k1 は値を 0.5 に固定、k2 は値を 0.4 に固定、h1 は値が急激に変化、h2 は値がなだらかに変化、s1 は最下位ビット置換、s3 は下位 3 ビット置換、s4 は下位 4 ビット置換を表している。

5. 結果

2 種類のコード表記に対して実験を行った結果、図 5.1、5.2 のようになった。縦軸は 1 画素にどれだけ情報を埋め込むことができたかを示す埋め込み率を表している。横軸は画像にどれだけノイズが混じっているか(劣化具合)を示すピーク信号対雑音比を表している。又、グラフは右上へ行くほど評価が高いことを表している。k1，k2，h1，h2，s1，s3，s4 はバイナリコードでの閾値、k1g，k2g，h1g，h2g，s1g，s3g，s4g はグレイコードでの閾値を表しているが、内容は同じである。

下位ビット置換(s1，s3，s4)を行った場合、ダミーに使用した画像による結果に大差は見られない。2 種類のコード表記に対する結果を比較しても、殆ど違いは無い。閾値を固定した k1，k2，k1g，k2g は埋め込み率、画質共にかなり評価が低い。それに対して、閾値を変化させる方式では、埋め込み率は同程度の場合でも画質がかなり保たれることが判った。この閾値変動方式では、グレイコードを使用すると(h1g，h2g)、バイナリコードを使用した場合(h1，h2)に比べ埋め込み率は落ちるが画質が良くなることも判明した。

6. おわりに

本研究では画像深層暗号化法として複雑領域を利用した方法、最下位ビットを利用した方法に加え、新たに変動する閾値と下位 3，4 ビットまで拡張した下位ビット置換を追加し実験を行った。その結果、下位ビット置換は下位 3 ビットまでなら使用に耐えることが判った。又、提案した閾値変動方式では閾値固定方式に比べ、画像の劣化が少ないという効果を確認できた。今回、目視による確認からPSNR が 37[dB]以上であれば使用可能と判断したが、複雑な画像の場合であれば 32[dB]付近まで画質が落ちても違和感がなかった。このことから、単純に数値のみの評価で画質を判断することは難しいことが判る。今後の課題として、PSNR 値が同じであってもコード表記によって目視による画質に違いが出る可能性もあるのでその確認等があげられる。

参考文献

[1] 武久 泰夫，坂無 英徳：JPEG-LS への秘匿情報の組み込み方式の提案，長野県情報技術試験場 1999 研究報告，http:// www.nagano-it.go.jp/jyouhou/report/1999/9904.pdf (1999)

[2] BPCS-Steganography へのお招き，http://www.know.comp.kyutech.ac.jp/BPCS/

[3] 新見 道治，野田 秀樹，川口 英二：複雑さによる領域分割を利用した画像深層暗号化法，電子情報通信学会論文誌，Vol.J81-D-II，pp1132-1140 (1998)

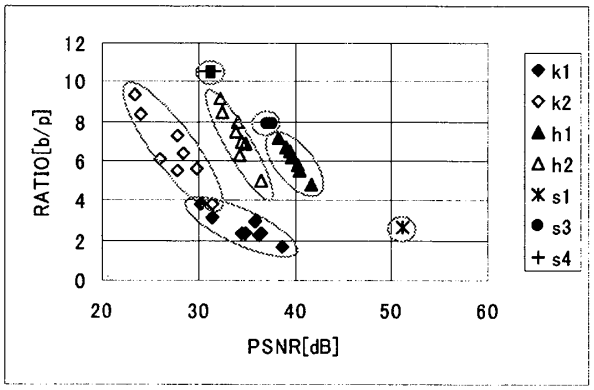

図 5.1 バイナリコードでの実験結果

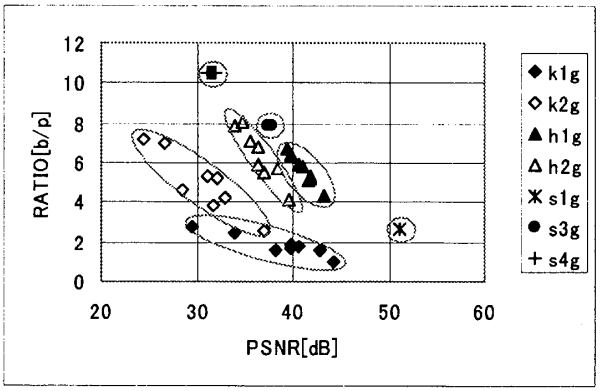

図 5.2 グレイコードでの実験結果