BMP ファイルを使った Steganography

A Steganography Using A BMP File

野崎　剛一（長崎大学　総合情報処理センター）
Koichi NOZAKI (Information Science Center, Nagasaki University)
nozaki@net.nagasaki-u.ac.jp
新見 道治，野田 秀樹，河口 英二（九州工業大学 工学部）
Michiharu NIIMI, Hideki NODA and Eiji KAWAGUCHI(Kyushu Institute of Technology)
{niimi,noda,kawaguch} @kawa.comp.kyutech.ac.jp

本論文は，カラービットマップ(BMP)ファイルをダミー画像とする情報非可視化技術(Steganography)に関する新方式の提案について述べたものである．本論文で提案する新方式の特長は，人間の視覚特性を利用した情報の埋め込みであり、画像の複雑さの定義とコンジュゲーション操作により，ダミー画像の 40-50%の部分に秘密情報を埋め込むことを可能としたことである．この方式は，他の Steganography 技術と比較して，3 倍以上の情報埋め込み能力を持つものでり，インターネットを利用した情報通信の新たなセキュリティ技術としての応用が見込まれる。

キーワード ： 画像深層暗号、情報非可視化、BMP ファイル、セキュリティ

A new steganography (information hiding technique) is proposed. It uses a color image as the information hiding dummy image. This new technique is not based on a programming technique, but is based on a property of human vision system such that human can not see the effect of the data change, even if the "noise-like" portions in the bit-planes of a multi-valued image are all changed to other noise-like patterns. In order to assure this property, we made a replacement experiment of noise-like portions of a color photo with random binary patterns. This human vision property is the key to the large capacity steganography which uses a color image in a BMP file format.

Keywords ： Information Hiding, Steganography, Image Bit-Plane, Image Perception, Image Complexity

1．はじめに

近年，インターネットは急速な勢いで社会に浸透し，インターネット上でビジネスを行う企業も増加し，セキュリティの確保がますます重要となってきている．既に信頼性の高い暗号方式が利用されているが，暗号化された情報内容は第３者には解読できないとしても，何かの秘密が隠されている，との事実は容易に露見してしまい，逆に不都合が生じることがある．従って，暗号技術とは異なる秘密情報を見えなくする Steganography（非可視化）技術は，情報の機密保護に有効と思われる．本研究は，そのような一つの試みとして，「ダミー画像データの中に秘密情報を埋込み，秘密情報そのものの存在を見えなくする」技術に関するものである．

2．BPCS-Steganography 方式

Steganography とは，簡単に言えば，コンピュータ・データ に関する「あぶりだし絵」技術のことである．すなわち，他人に見られた

くない秘密情報を何か別のデータ（ダミー情報）の中に埋め込み，その秘密の存在そのものを隠してしまう技術のことである．埋め込んだ秘密を取り出すには，特別な鍵（実際にはプログラム）を使う．この技術は情報化社会において益々重要になる「情報セキュリティ」技術の一つとして注目され始めている．

我々の提案するシステム BPCS(Bit-Plane Complexity Segmentation)-Steganography は，複雑さによる領域分割を利用した新たな方式であり，ダミー画像ファイル(Windows での BMP フルカラーの画像データファイル)の中に情報を埋め込む．この原理は，現在知られている技術とは異なる原理であり，大容量のデータに対応可能である．今日の Steganography における電子データの隠し場所(Carrier, Container, 或いは Dummy data 等の呼び方がある)としては，画像データが利用されることが多い．その理由は，画像データは大容量であり，冗長な部分が多く含まれているからである．

しかしながら，これまでに公表されている Steganography 技術の弱点は，隠せる(或いは「埋め込める」)情報容量が小さく，Dummy 画像データ量の 5～15%程度にとどまっている．

3．画像ファイルへの情報の埋め込み

最近では，インターネットやディジタル情報を取り扱う分野の拡大に伴い，カラー画像，動画像，音声などのマルチメディア作品の著作権保護や所有権の主張という観点から，「電子透かし」技術が俄かに注目を浴びている[1]．この技術は，或る見えにくい「固有情報」をディジタル作品に埋め込み，権利を主張するものであり，その特徴は以下の通りである．

- 透かし情報は，人間が目や耳で知覚し難いノイズという形でディジタルデータに埋め込まれ，所在が分かり難い．
- 透かし情報を多く入れ過ぎると，著作物の品質の劣化を招くので，埋め込み量は少量である．
- 透かしが埋め込まれたデジタルデータ(著作物)の小片からでも，透かし情報は抽出できる．

一方，我々の提案する「自然画像をダミー・データとする BPCS-Steganography 方式」は，電子透かし技術と似てはいるが，目的と用途が全く異なるものである．我々の埋め込み方式は，かなり多量の秘密データをダミー画像に埋め込んでも，その画像の見た目が変わらないというものである．データを埋め込んでも，見た目が変わらなければ，埋め込まれた画像を他人に盗まれても，秘密が隠されている事に気付かれることもない．

3．1 多値画像のビットプレーン分解

各画素が n ビットの値を持つ多値画像 (P) は，それぞれのビット毎に分解して取り出せば，n 枚の２値画像の組として考えることができる．すなわち，モノクロ画像では P=(P1, P2, . . . , Pn) と表され，カラー画像については，R(赤)，G(緑)，B(青)の３成分に分解して，

$$P = (PR1, PR2, \ldots, PRn, PG1, PG2, \ldots, PGn, PB1, PB2, \ldots, PBn)$$

と表される．ただし，P1 が最上位ビット，Pn が最下位ビットである．通常の画像データは，純２進数表現(Pure Binary Code，PBC と略記)によっているが，その他の表現によるビットプレーンも可能である．例えば，グレイコードの一種である Canonical Gray Code(CGC と略記)を用いて画像データを表してもよい[2]．各ビットプレーンは，普通，上位プレーンから下位プレーンに向かって徐々に複雑なパターンとなる．もし，このような傾向を示さない画像があれば，それは人工的に加工，合成したものである．特に，最下位ビット（カラーの場合は R，G，B 成分の最下位ビット）は，殆どノイズ状のパターンとなる．

次に，レオナルド ダビンチの「最後の晩餐」の BMP カラー24 ビット画像とその RGB のビットプレーン分解した R(赤)成分の第３，第４の各ビットの画像を示す．G(緑)成分と B(青)成分についても，同様の画像となる．

図１　24 ビット画像

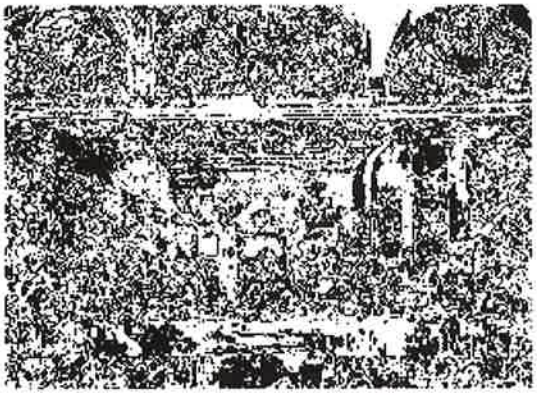


図２　R の第３ビットプレーン

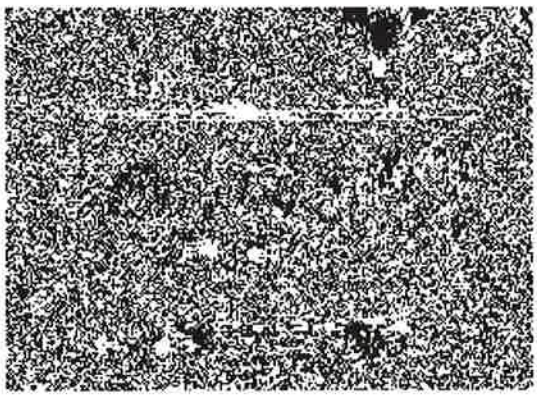


図３　R の第４ビットプレーン

このように，多値画像のビットプレーン分解で得られる２値画像には，形の情報が認められる領域(有意味な領域)と，ノイズ状の領域(無意味な領域)がある[2)3)4)]．一般に，意味の有る領域は簡単であるが，無意味な領域は複雑である．

次にR(赤)成分第５ビット目の画像を示す．多くの自然画像の BMP カラー24 ビット画像の場合，第５ビット目以降のビットプレーンの画像はこの例のように，ノイズ状の領域(無意味な領域)がほとんどである．

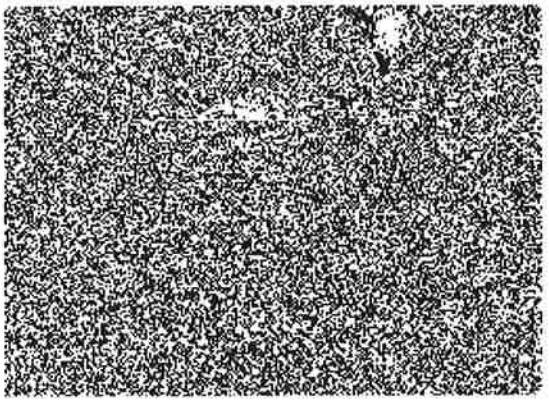


図４　R の第５ビットプレーン

4．画像の複雑さの定義

画像データに関して，視覚的に複雑であるか否か(形の情報が認められるか否か)を数値で表現したいが，２値画像の複雑さの標準的な定義は存在しない．河口等は画像の閾値処理に関して議論し，３つの複雑さを提案しているが，本稿では，境界線の長さによる複雑さを利用する．

ここで，２値画像における，白黒の境界線の長さとは，近傍の定義を４連結とする場合，色の変わり目を縦方向と横方向で足し合わせたものである．例えば，白画素で囲まれた孤立した１個の黒画素の境界線長は４である．今，$2^m \times 2^m$ 画素からなる画像を考え，その画像内において色が変わる個所を数える．境界線の最小値は０である(全て白，又は全て黒の場合)．一方，境界線の最大値は

$$2 \times 2^m \times (2^m - 1)$$

である(市松模様の場合)．この境界線の長さを利用して，「複雑さα」を以下の式で定義する．

$$\alpha = \frac{k}{2 \times 2^m \times (2^m - 1)}$$

ここで，k は画像内の実際の境界線長である．この式において複雑さの値の範囲は，

$$0 \leq \alpha \leq 1$$

となる．このような複雑さは，全画面について定義してもよいが，局所的に小領域で定義してもよい．

4.1 自然画像におけるノイズ

次に，2つの自然画像を示す．

(512×512 カラー画像 ： 原画像)

図5　ダミーの自然画像

図5はダミーとなる自然画像(何も埋め込んでいない R, G, B 各8ビット 512×512 のカラー画像)である．

図6　秘密情報埋め込み後の画像

図6は，図5のダミー画像に，「眼鏡橋」JPEG カラー画像(154KB)，音声データ(66KB)(子供の声「先生さようなら」3.04秒)および図1の「最後の晩餐」(512×371 ピクセル JPEG 圧縮カラー画像)の画像(76KB)，合計 296KB のファイルを埋め込んだものである．これらの 2 つの画像を比べて分かるように，両者の画質には，大きな差異は見られない．

「眼鏡橋」JPEG データ(154KB)

「先生さようなら」音声データ(66KB)

図1の「最後の晩餐」の JPEG データ(76KB)

図7　埋め込んだデータ

4.2 パターン情報に対する人間の視覚特性

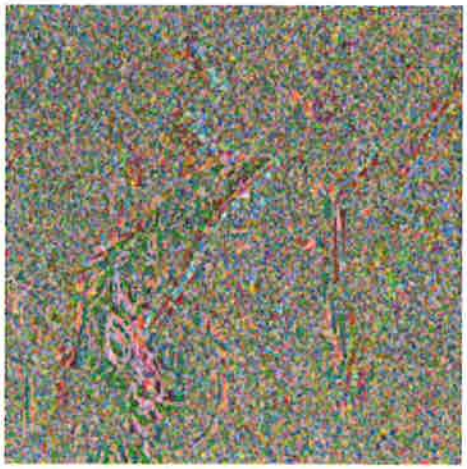
我々の提案している Steganography 技術は，パターン情報に対する人間の特異な視覚特性を利用したものである．既に述べたように，画像ビットプレーン上の意味のある領域は「簡単」であるが，ノイズ状の領域は複雑である．図 8 はこのことを示す実験例である．

まず，図8の(a) は Lena と呼ばれるカラー画像である(257×257 画素，R，G，B 各8 ビット)．図8の(b)と(c)は，これをそれぞれのビットプレーンに分解（Canonical Gray Code による[2) 12) 13)]し，複雑さの尺度 α について，各プレーン上で、それぞれ $0.125 < \alpha$ 及び $\alpha \leqq 0.125$ なる全ての 8×8 領域をランダムパターンと置き換えたものである． 8×8 の2値パターンの分布を正規分布と見なせば[3)]，$\alpha = 0.125$ とは，標準偏差値 σ では $\alpha = 0.5 - 8\sigma$ に相当する．これは，この値より簡単なパターンの総数は 全体 (2^{64} 個) の 6.66×10^{-14} % にしか過ぎないことを示している．図8の(b)は，$\alpha = 0.5 - 8\sigma$ より複雑な部分をランダム化しても Lena の視覚情報は大部分保存されることを示している．しかしながら，図8の(c)はそれより簡単な部分(パターン全

体からは極めて希少なもの)をランダム化するだけで Lena は殆ど見えなくなることを示している.

(a)原画

(b)複雑な部分の置き換え



(c)簡単な部分の置き換え

図8 ランダムパターンの置き換え例

以上のことから次の結論を得る.

「人間には極めて簡単な視覚的パターンしか認識できない」

このことを利用すれば「ランダム化できる全ての情報ファイルは画像データの中に隠せる」ことになる.

5. 複雑さを利用したデータ埋め込み法

5.1 基本原理

これまで述べたように,自然画像のビットプレーンでは,ノイズ状の領域を,別のノイズ状のデータで置き換えても,視覚的にほとんど影響を受けない.このことを利用すると,ダミー画像中のノイズ状の領域を秘密データで置き換えることが可能となる.ノイズ状の領域であるか否かの判定基準は,前述の実験により,8×8 を局所領域サイズとした場合, $\alpha = 0.5 - 8\sigma$ 程度に定めておけばよいと思われる.つまり,2 値画像上で上記の値よりも複雑な領域は秘密データの埋め込み場所となる.秘密データファイルをダミー画像に埋め込むには,まず,ファイルを 8 バイト毎に区切り(8×8 画素に対応),それらの各ファイル小片を順次ノイズ領域の 8×8 領域に埋めていけばよい.しかしながら,すべてのファイル小片がノイズ状で(つまり複雑で)あるわけではない.そこで,そのような小片についてはコンジュゲート演算[5]により複雑化する.このような操作をすれば,どんな秘密ファイルも画像に埋め込むことが可能となる.ただしこの場合,秘密ファイルを完全に復元するために,画像のどの領域がコンジュゲートされたデータであるかを記録する「コンジュゲートマップ」を保存しなければならない[5].

5.2 データの埋め込み容量

鍵を用いた暗号技術を Cryptography と呼び,それに対して本稿で述べている技術は暗号らしくない暗号技術であり,Steganography と呼ぶ.この Steganography の発想をコンピュータと画像通信に移植した松井等の研究[7]や,最近ではインターネット上に以下のようなシステムが公開されている.

HideSeek
http://www.cypher.net/products/hideseek.html
S-Tools
http://www.iquest.net/~mrmil/stego.html
Steganos for Windows95
http://www.demcom.com/english/steganos/

我々の BPCS-Steganography は，これらの技術とその原理が異なっている．図 5 のカラー画像をダミーとして，テキストのみのファイルを埋め込んでみると，S-Tools では，その内部でデータの圧縮処理を行うために 200KB のファイルを 100KB 程度に圧縮し，(我々が実験を行ったところ，99.06KB に圧縮)，jpeg，gif のみのファイルの場合，99KB までのファイルを埋め込むことができた．従って，ダミーファイルの 13%程度が埋め込み容量の限界であることが分かった．松井等が行っている「画像を周波数分解し，中間領域の成分を別の情報に置き換える」方式の場合[6) 7) 8) 9)]，原画像データ量の 12%程度までしか別の情報は埋め込めないと報告されている．このように現在公開されているツールでは，いずれもダミー量の 10%強程度までのファイルしか埋め込むことができなく，この程度では秘密情報の保管場所としては不十分である[10) 11)]．

一方，我々が考案した本方式では，通常の自然画像の場合，そのデータの 50%程度までを別の情報と入れ替えてもよいことが判明した．即ち，現在公開されている他の方式に比べ，我々の方式での容量は非常に大きいと言える．

5.3 埋め込みデータ

本システムでダミー画像に埋め込む秘密情報は，どんなファイルであってもよいが，埋め込む容量を大きくするためにはランダム化しなければならない．これは「圧縮ファイル」にすることで解決できる．本研究では圧縮ファイル化技術については既存の方法を用いている．

6 BPCS-Steganography の応用について

BPCS-Steganography のプログラムは，Encoder 部 Decoder 部からなり，"Encoder・Decoder"一体として利用したり，"Encoder・Decoder" と "Decoder"に分割して利用することが可能である．また，本システムをインストールする時，カスタマイズしておけば，互いに動作する一つの Encoder と 一つの Decoder を唯一に定められる．

次に BPCS-Steganography 技術の応用可能性を検討する．

6.1 Encoder・Decoder だけでの利用

(1) カスタマイズした Encoder・Decoder を自分だけで持つ場合

画像ファイル(主としてパソコン上の)を他人には見えない自分だけの秘密情報金庫として利用できる．

(2) カスタマイズした Encoder・Decoder を特定の相手(グループ)と共有する場合

- 秘密を埋め込んだダミー画像データを E-Mail の添付ファイルとして送信し合うことにより，相互に安全な秘密通信ができる．
- 互いのホームページから，秘密情報を埋め込んだダミー画像をダウンロードして，相手(またはグループ)からのメッセージを受け取る．

(3) 一人のリーダが多数の会員別にカスタマイズした Encoder・Decoder を持つ場合

この形態は，インターネットでのカタログショッピングに利用できる．リーダ(インターネットストア)は，会員 (顧客) に対して，個別にカスタマイズした Encoder・Decoder を会員証として配布しておく．会員はストアのホームページの商品の写真をダウンロードし，「注文書」を埋め込んでストア側に E-Mail する．会員の Encoder が会員証であり，「商品」の中に注文書が入れられているので間違いが生じにくい．会員が脱会するときは，ストア側が保管していた Decoder を破棄するだけでよい．

6.2 Encoder･Decoder と Decoder を分けての利用

グループ・リーダとグループ員からなる特定グループ内で利用する場合

リーダー(本社)は，グループ員(支社)毎にカスタマイズした Encoder･Decoder をグループ員のそれぞれに配布し，同時に全ての Decoder 部を一括して保管する．このようにしておけば，各グループ員からのダミー画像に隠された秘密メッセージを E-Mail として受信できる．逆に，それぞれにカスタマイズした Decoder だけを配布しておけば，リーダーは E-Mail によって個別に秘密指令が出せる．いずれの場合もグループ外には秘密通信の存在がわかりにくい．

このように，BPCS-Steganography は，秘密情報をダミーファイルに直接埋め込むため，画像再生のプラットホームが変わっても，ダミーデータが保存されている限り，埋め込んだ情報を取り出すことができ，可逆圧縮には耐えられる．我々の研究の目指すところは情報の暗号化(どう秘匿するか)ではなく，どう情報を埋め込んだ媒体と一体化するか，即ち「画像データに秘密を埋込み，その秘密の存在を他人に気付かせない」ということである．本方式では，2 値化情報なら，どんなものでも埋め込むことができるので，暗号コードを埋め込めば，その暗号のキャリアとして画像を利用することや小さなプログラムを埋め込むことなど多くの分野への適用が考えられる．

7. おわりに

本研究は秘密情報の保存と通信を安全なものにする一種の暗号化技術の研究である．これまでの暗号化が秘密情報を隠す技術であったのに対して，本技術は，秘密の存在を「気付かせない」技術であり，両者は互いに補完し合える技術である．すなわち，暗号化した情報を非可視化することにより，情報の安全性は格段に高まるはずである．本方式を使ったアプリケーションソフトに，秘密を埋込む際に，カスタマイズ機能を設定できるようにしておくことで，同じソフトでも他のユーザから自分の秘密は完全に守られる．例えば，ディジタルカメラによる自分のアルバムに，カスタマイズしたプログラムで自分用に秘密情報を埋込んでおけば，秘密情報の存在を他人に全く気付かれずに済む．従って，本研究による情報非可視化応用ソフトは，パソコンユーザにこそ手軽に利用できる最適の暗号化ソフトとなる．何故なら，パソコンは秘密情報をあからさまに隠せない状況での使用が多いからである．

参考文献

(1) 中村, 松井, "離散的直交変換を用いた濃淡画像とテキストデータの合成符号化法", 電子情報通信学会論文 D-II, Vol. J72-D-II, No. 3, pp. 363-368, 1989.

(2) Eiji Kawaguchi, et al: Depth-First Picture Expression Viewed from Digital Picture Processing, IEEE Trans. on PAMI, Vol.PAMI-5, No.4, pp.343384, July, 1983.

(3) 野崎, 新見, 野田, 河口, "自然画像をダミーデータとする大容量 Steganography 方式について", 信学技法, IE97-43, pp. 17-23(1997).

(4) Kamata,Kawaguchi,et al,"Depth-First Coding for Multi-Valued Pictures Using Bit-Plane Decomposition", IEEE Trans. Communications, Vol.43, No.5, pp.1961-1969, 1995.

(5) 新見, 野田, 河口, " 複雑さによる領域分割を利用した画像深層暗号化法", 信学技法, IE97-14, pp. 39-44(1997).

(6) 櫻井幸一監訳, "暗号理論の基礎", 共立出版 1996

(7) 松井甲子雄, "画像深層暗号", 森北出版(1993).

(8) 中村, 松井, "離散的直行変換を用いた濃淡画像とテキストデータの合成符号化", 信学論 DIIJ72-DII,3,pp.363-368(1989).

(9) 中村, 荻原, 横矢, "DCT を用いた画像深層暗号における歪み低減手法", 信学技法, IE95-121, pp. 1-6 (1996.

(10) 小出, 荻原, 金田, "誤差拡散法および平均濃度近似法を用いた画像深層暗号方式の提案", 信学技法, IE95-122, pp. 7-14 (1996).

(11) Maragos,P., "Pattern spectrum and multiscale shape representation", IEEE Trans. on PAMI, vol.11, no.7, pp.701-716,1989.

(12) Kawaguchi, E. and Taniguchi R., "Complexity of binary pictures and image thresholding - An application of DF-Expression to the thresholding problem", Proceedings of 8th ICPR, vol.2, pp.1221-1225,1986.

(13) Kawaguchi, E. and Taniguchi, R.., "The DF-Expression as an image thresholding strategy",IEEE Trans. on SMC,vol.19,no.5,pp.1321--1328, 1989.

(14) 野崎, 新見, 野田, 河口, "自然画像をダミーデータとする大容量 Steganography の利用形態について", 平成 9 年度電気関係学会九州支部連合大会講演論文集, p. 79 (1997)

著者略歴

野崎 剛一

昭和 50 年 九州大学・工学部電気工学科卒. 同年 長崎大学助手・電子計算機室. 昭和 55 年 長崎大学講師・情報処理センター. 昭和 61 年～62 年 米国テネシー州立大学客員研究員. 平成元年 長崎大学総合情報処理センター研究開発室長. プログラミングツールとコンピュータネットワーク, 情報処理教育システム環境の研究, 画像処理の研究に従事. 情報処理学会, ACM 各会員

新見 道治

平成 4 年 九工大・工・電気・計算機工学コース卒. 平成 6 年 同大・工・大学院博士前期課程了. 同年 長崎総合科学大学助手. 平成 8 年 九工大工学部助手, 現在に至る. 画像解析, 画像表現, 自然言語理解の研究に従事. 情報処理学会, IEEE 各会員.

野田 秀樹

昭和 48 年 九州大学・工・電子卒. 昭和 50 年 同大大学院修士課程了. 同年 第二精工舎 (現セイコー電子工業) 入社. 昭和 53 年 警察庁科学警察研究所入所. 平成元年 郵政省通信総合研究所入所. 平成 7 年 九州工業大学工学部助教授, 現在に至る.

河口 英二

昭和 39 年 九州大学・工・通信卒. 昭和 44 年 同大学院博士課程了. 同年 九州産業大学講師. 昭和 48 年 九州大学工学部情報工学科助教授. 昭和 54 年 同大学院総合理工学科情報システム学専攻助教授. 昭和 63 年 九州工業大学工学部教授, 現在に至る. 昭和 59 年～60 年米国テネシー大学訪問教授. 工学博士. 画像理解, 情報圧縮, Steganography, 自然言語理解等の研究に従事. 情報処理学会, 人工知能学会各会員.