

誤りパターン埋込み型ステガノグラフィに
関する一考察

**A study on steganography
based on embedding error patterns**

研究者：索手 一平
Researcher : Ippei NAWATE

指導教員：福岡 久雄
Supervisor : Hisao Fukuoka

松江工業高等専門学校情報工学科
Department of Information Engineering, Matsue College of Technology

Abstract

本論文は、テキスト情報をグレースケール画像に埋め込むステガノグラフィ技術を対象とする。データの埋め込み手法の一つである誤りパターン埋め込み法は、テキスト情報を冗長かつハミング重みの小さいビット列（これを誤りパターンという）に変換し、画像中の LSB 平面との排他的論理和で LSB 平面を置き換える。本研究では、誤りパターン埋め込み法における画質劣化等について考察する。また、Shalkwijk の数え上げ符号を用いた誤りパターンの動的生成方法を提案する。

Keywords

ステガノグラフィ, セキュリティ, 誤りパターン

目次

1. はじめに	2
2. ステガノグラフィとは	2
3. 誤りパターン埋め込み法	3
4. 誤りパターンの生成方法	4
4.1 Slalkwijk の数え上げ符号	4
4.2 誤りパターンの動的生成	5
5. 実験	5
5.1 実験手順	5
5.2 実験結果	5
5.2.1 誤り率と埋め込み率	5
5.2.2 SSIM と誤り率	6
5.2.3 2 ビットプレーン以降の埋め込みでの実験結果	6
5.2.4 メッセージ長が同じ場合の劣化について	7
6. 実験環境	7
7. 画像の入手元	8
8. おわりに	8

1. はじめに

近年のネットワーク通信の増加に伴い、安全に通信を行うための技術の重要性が高まってきている。特に秘密情報の通信においては重要なものとなる。安全に通信を行う手段として主なものに送信内容の暗号化がある。暗号化により、送信内容を第三者に読み取られない状態とすることで、第三者による盗聴、なりすましといった妨害行為を防ぐことができる。しかし、通信行為そのものは第三者に認知されていることから通信経路の遮断などといった妨害行為をうける可能性を排除できない。この点に対し、ステガノグラフィでは送信内容を別のデータに埋込むことで、第三者から秘密情報の存在そのものを隠ぺいする。つまり、「秘密データの通信を行っている」という事実そのものを隠ぺいすることができる。

本論文ではステガノグラフィ技術の中で最も埋め込みに利用される画像、特にグレイスケール画像に対し、テキスト情報を埋め込むものとして、誤りパターン埋め込み法における埋め込み率と誤り率、画質劣化とのトレードオフ関係を実験的に明らかにする。なお、画質劣化の指標には SSIM[1] を用いる。また、誤りパターンへの変換手法として Shalkwijk の数え上げ符号 [3] を用いたどう適正性手法を提案することで、誤りパターンテーブル法における問題に対する解決案を示す。

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媒体に埋め込む技術、研究の総称である。ステガノグラフィでは一般的に埋め込み対象となる画像をカバーデータ、埋め込みによって生成されたデータをステゴデータと呼ぶ。ステガノグラフィを用いた通信は図 1 のように、送信者がステゴデータを生成することで秘密データの存在を隠蔽し、それを送信する。受信者は送信されたステゴデータから埋め込みに対応するアルゴリズムを用いて秘密情報を取り出す。第三者にとってはこの通信はあくまで「何の変哲もない画像通信」であり、送信内容を確認できたとしても秘密情報の存在に気づくことはできない。

しかし、「別の媒体に埋め込む」という特性からカバーデータによっては多くの情報を埋め込むことが困

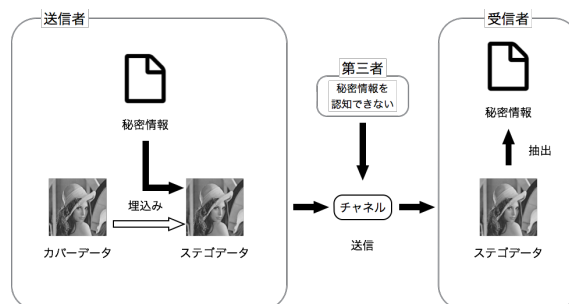


図 1 ステガノグラフィの通信モデル

難となる。また、一般的に多くの情報を埋め込むほどにステゴデータはカバーデータと比べ劣化し、劣化が大きければ第三者から秘密情報の存在を認知される可能性が高まるためステガノグラフィは意味を成さなくなる。このような特性からステガノグラフィでは以下の 2 点を同時に満たすことが強く望まれる。

1. できるだけ多くの情報の埋め込みが可能である
2. 埋め込みが主観的・客観的に認知されない

本論文では後者についてステガノグラフィにおける隠蔽性（以下隠蔽性）と呼ぶ。

埋め込み媒体には主にメディアデータが用いられる。ほとんどのメディアデータはいくらかの冗長性を有しており、これらを利用した埋め込みが主流である。本実験で扱う画像、この冗長性とは画像中の各ピクセルにおける LSB などの下位ビットである。これらのビットはそれぞれが持つ情報量が少なく、変化させたとしても視覚的变化がほとんど発生しない。特に LSB は情報量が最も少ないことから、埋め込み利用されることが多い。実際、この特性を利用した埋め込み手法として LSB 法が提案されており、ステガノグラフィにおける最も一般的な手法として知られている。

LSB 法とは画像の各ピクセルにおける LSB のみを埋め込み対象とすることで、埋め込みによる画像の劣化を抑えた手法である。また、埋め込みはカバーデータ中の LSB に対しテキスト情報のバイナリ表現をそのまま置き換えることで行われる。（図 2）

埋め込み時に LSB をテキスト情報のバイナリ表現でそのまま置換することから、LSB のビット列をそのまま抽出することでテキスト情報を画像から抽出することができる。（図 3）

単純なアルゴリズムであり実装が容易である反面、

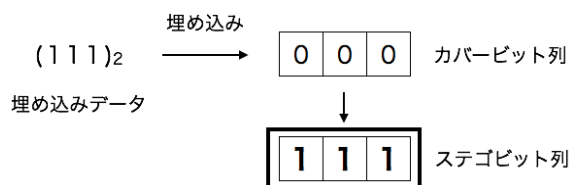


図2 LSB 法での埋め込み

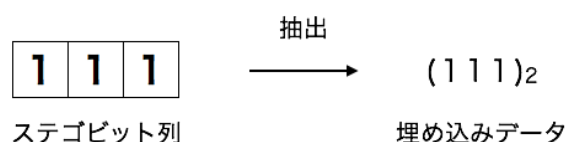


図3 LSB 法での抽出

埋め込み後のビット誤りが起きやすく、図2のようにすべてのビットが反転してしまう場合もある。このため、ステゴデータの画質が劣化しやすく、視覚的に隠蔽性に問題を引き起こす可能性がある。

このような問題から、これまでLSB法におけるビット誤りを改善した手法が多数提案されてきた。それらの中でも本論文で扱う誤りパターン埋め込み法はビット誤りを大きく改善した手法として知られている。これについて章3.にて述べる。

本論文ではカバーデータのうち、埋め込みに対象となるビット列をカバービット列、ステゴデータ中のデータが埋め込まれたビット列をステゴビット列と呼ぶ。また、カバービット列とテキスト情報のバイナリ表現のビット列長をそれぞれ n , m , ステゴビット列中の誤りビットの数を d として、 $\frac{m}{n}$ を埋め込み率、 $\frac{d}{n}$ を誤り率とする。

埋め込み率、誤り率は埋め込み評価指標として利用される。埋め込み率はいかに効率よくテキスト情報を埋め込んでいるかを表しており、高いほどに多くの情報を埋め込むことができる。また、誤り率は埋め込みによるビット誤りの発生頻度を表しており、一般的に誤り率が高いほど画質が劣化する傾向にある。LSB法では埋め込み率は常に100%であるが、一方でビット誤りが起きやすいことから誤り率が高い。

3. 誤りパターン埋め込み法

LSB法をもとに、より低い誤り率での埋め込みを実現した手法として誤りパターン埋め込み法が知られ

ている。この手法では後述する変換方式(章4.)を用いてテキスト情報のバイナリ表現を、より長くハミング重みの小さいビット列である誤りパターンに変換する。そして、カバービット列をそのまま置き換えるのではなく、カバービット列と誤りパターンとの排他的論理和でカバービット列を置き換える(図4)。

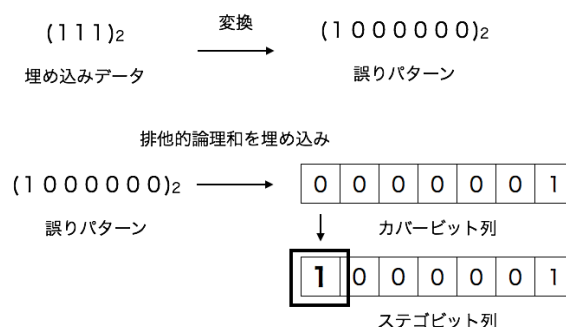


図4 誤りパターン埋め込み法での埋め込み

テキスト情報の抽出時は、カバービット列とステゴビット列との排他的論理和をとることで誤りパターンを抽出し、その誤りパターンを逆変換することでテキスト情報を抽出することができる(図5)。

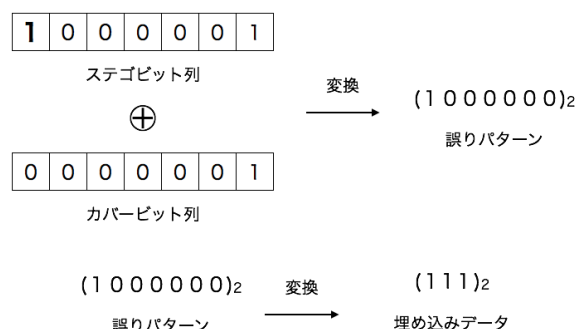


図5 誤りパターン埋め込み法での抽出

排他的論理和を用いることから、誤りパターンにおける「1」の対応するビットのみがカバービット列中で置き換わるため、ビット誤りを大幅に抑えることができる。一方でより長いビット列を使用することから必然的に埋め込み率は減少する。

この手法ではステゴビット列中で発生するビット誤りは誤りパターンのハミング重みと同じであり、誤りパターンの発生は埋め込まれるテキスト情報に依存することから、誤り率はテキスト情報の内容に依存する。そのため同じテキスト情報を埋め込みデータとした場

$n = 6, k = 2$ の 2 進数列 x の集合は 10 進数 $i(x)$ が表 2 のように割り当てられる.

表 2 $n = 6, k = 2$ の場合の対応付け

x	$i(x)$	x	$i(x)$
000011	0	010100	8
000101	1	011000	9
000110	2	100001	10
001001	3	100010	11
001010	4	100100	12
001100	5	101000	13
010001	6	110000	14
010010	7		

4.2 誤りパターンの動的生成

動的生成のアルゴリズム中ではテキスト情報の各文字のバイナリ表現を 2 進数列 x として与えることで、パスカルの三角形を用いて 10 進数 $i(x)$ へと変換する. このとき, x は一意の値となるが $i(x)$ は同じ値が割り振られてしまう. 例えば, 表 2 で $x = 000011$ に割り当てられる $i(x)$ は 0 であるが, $x = 000000$ に割り当てられる $i(x)$ も同様に 0 である. そこで x の長さ n , ハミング重み k を元に式 (1) で求められる offset_k を $i(x)$ に加算することで一意の誤りパターンとする.

$$\text{offset}_k = \sum_{i=0}^{k-1} n C_i \quad (1)$$

$$\text{offset}_0 = 0$$

この方法を用いることで誤りパターンを動的に生成し, 強いメモリ制約下での誤りパターン変換を可能にすることができる.

5. 実験

5.1 実験手順

実験手順の概要を図 7 に示す. 以下に示す手順で実験を行った. 実験には $256 \times 256 \text{px}$ の 8 ビットグレイスケール Bitmap である SIDBA 画像 30 枚を使用し, 埋め込みに使用するテキスト情報は当確率で発生する 8bit コードの列とした. テキスト情報の生成には 623 次元に分布する乱数発生器である SFMT を用いた.

(1) テキスト情報の各コードを章 4.2 にて述べた手

法で動的に誤りパターンへと変換し, 変換した誤りパターンと画像の LSB 平面との排他的論理和を画像へと埋め込む.

- (2) 埋め込み前後の画像を比較し, 誤り率, SSIM を算出する.
- (3) 誤りパターン長を 8bit から 256bit まで変化させ (1), (2) を繰り返す.
- (4) 画像を入れ替えて (3) を繰り返す.

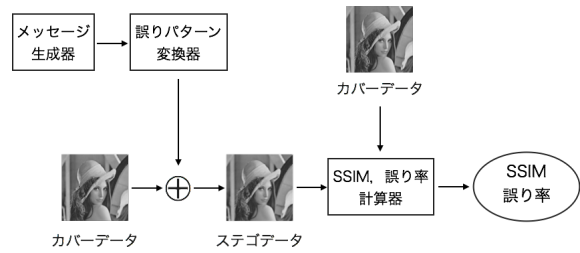


図 7 実験概要

5.2 実験結果

5.2.1 誤り率と埋め込み率

誤り率の計測結果と文献 [2] において示されている誤りパターン埋め込み法における誤り率の理論的下限曲線を図 8 に示す. なお, 誤りパターン埋め込み法における誤り率は埋め込まれるテキスト情報にのみ依存するため, 同じテキスト情報が埋め込まれたすべての画像について計測される誤り率は等しい.

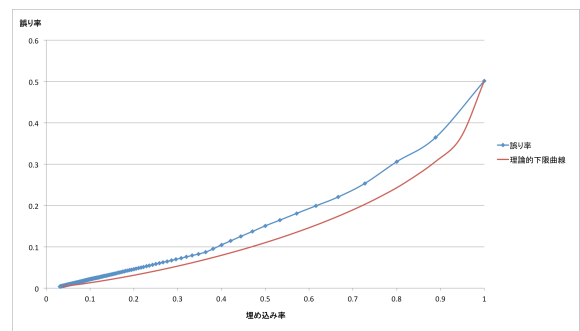


図 8 埋込率に対する誤り率の変化

図 8 より, 実際に計測した誤り率は理論的下限曲線と同様, 埋め込み率が増加するとともに誤り率も増加し, 理論的下限曲線に比べ曲率の低い曲線を描いた.

5.2.2 SSIM と誤り率

30 枚の SIDBA 画像のうち、SSIM の最も高い画像 10 枚と最も低い 10 枚の埋込率に対する SSIM の変化を図 9 に示す。

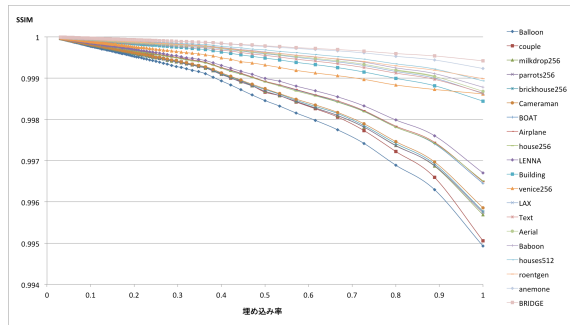


図 9 埋込率に対する SSIM の変化 (画像ごと)

図 9 よりすべての埋込率について SSIM が 0.99 を上回っていることがわかる。一般的に SSIM は 0.98 以上で比較された画像間の見分けがつかないと言われていることから、どのような埋込率に対しても画質が大きく劣化することはないと考えられる。このことから、埋込みを LSB 平面に限定した場合、埋込率、誤り率によって画質が大きく劣化することはない、画質劣化の面でステガノグラフィ技術の隠蔽性に大きく影響を与えることはないということがわかる。同時に図 9 より、画像ごとに SSIM の変化の様子が異なることがわかる。これについて、実験に使用した画像を主観的に観察したところ、図??のように画像全体の複雑度が高い画像ほど SSIM の変化が小さく、一方で図 14 のように複雑度の低い大きな領域を含む画像ほど SSIM の変化が大きくなるという傾向が見られた。ここで複雑度とは画像全体における画素間の明暗の変化の多さを表しており、複雑度が高いほどにノイズ画像のようになる。これは、テキスト情報中の 0,1 の発生はランダムであり、埋込みによる画像の劣化がノイズ上になることから図 13 のように複雑度が高い画像であれば画像中にノイズが溶け込んでしまうためであると考えられる。

5.2.3 2 ビットプレーン以降の埋込みでの実験結果

章 5.2.2 の結果から、隠蔽性に影響を及ぼさない範囲で 2 ビットプレーン以降への埋込みも可能なのではないかと考え、2~4 ビットプレーンまでの埋込み

を行った。実験手順はこれまでと同様の手順で行い、実験対象となるビットプレーン以下のビットプレーンについては埋込率 100 % で埋込みを行った。実験結果をそれぞれ図 10~12 に示す。

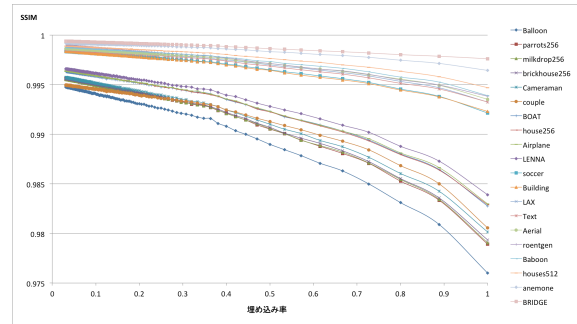


図 10 埋込率に対する SSIM の変化 (2 ビットプレーン使用)

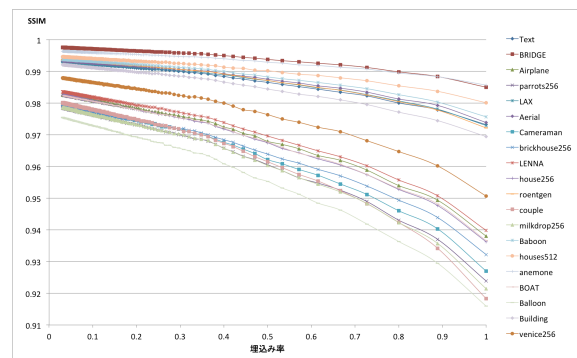


図 11 埋込率に対する SSIM の変化 (3 ビットプレーン使用)

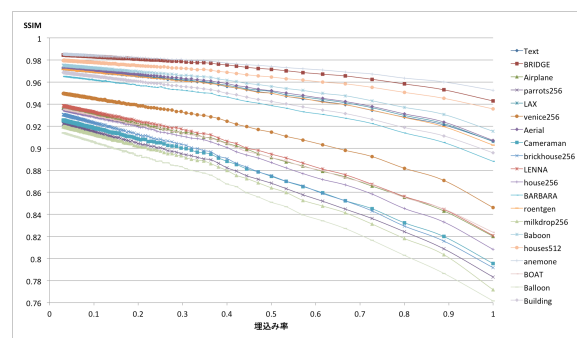


図 12 埋込率に対する SSIM の変化 (4 ビットプレーン使用)

図 10 より埋込率 0.9 前後で SSIM が 0.98 を下回り始めていることがわかる。このことから、LSB へ

の埋め込みを 100 % として 2 ビットプレーンまで埋め込みを行うことで、ほとんどの画像に対し、ステガノグラフィの視覚的な隠蔽性に影響を及ぼさない範囲で、約 1.9 倍のテキスト情報の埋め込みが実現できるといえる。

図 11 より 3 ビットプレーンまで埋め込み率 100 % の埋め込みを行ったとしても SSIM が 0.98 を上回る画像があることがわかる。また、図 12 においても最大で埋め込み率 0.2 前後までテキスト情報を埋め込むことができることがわかる。ここで、図??、14 のステゴデータをそれぞれ図 14、14 に示す。ステゴデータは 3 ビットプレーンにまで埋め込み率 100 % で埋め込みを行ったものである。これらの画像から明らかに図 14 はもとの画像に比べ視覚的に大きく劣化が生じている一方で図 13 は劣化が小さく元の画像を知らなければほとんど劣化に気づかないレベルであるといえる。これらのことから適切な画像を選択することでより LSB のみへの埋め込みに比べ 3 倍以上のテキスト情報の埋め込みが可能になるといえる。



図 13 BRIDGE.bmp のステゴデータ

5.2.4 メッセージ長が同じ場合の劣化について

埋め込み範囲を広げて同じメッセージ量を埋め込む場合、より長い誤りパターンを用いることができることから、ステゴデータの誤り率を下げるができる。

例えば、LSB のみへ埋め込み率 100 %、つまり誤りパターン長を 8 ビットとしてで埋め込んだ場合、



図 14 Balloon.bmp のステゴデータ

256×256px の画像であれば 8192 文字の埋め込みが可能である。これを 2 ビットプレーンにまで埋め込み範囲を拡張し 8192 文字を埋め込んだ場合、単純に埋め込み範囲が倍になることから誤りパターン長を 2 倍の 16 ビットとして埋め込みを行うことができるため、理論上誤り率を半減させることができる。

このことから、メッセージ長を固定し LSB のみへ埋め込みを行った場合と 2 ビットプレーンまで埋め込んだ場合の SSIM について、同様の実験手順で比較を行った。

30 枚の SIDBA 画像のうち BRIDGE.bmp (図??) を使用した場合の実験結果を図 15 に示す。この結果から LSB のみへ埋め込みを行った場合の SSIM が埋め込み率にかかわらず、常に 2 ビットプレーンにまで埋め込み範囲を拡張した場合を上回っていることがわかる。このことから埋め込み範囲を拡張することによる画質劣化の抑制は基本的に不可能であるといえる。しかし、この図において SSIM は 0.98 を上回っており、視覚的な隠蔽性に問題がないことから、誤りによる埋め込みの検出を回避する目的に利用する x という面では有用であるといえる。

6. 実験環境

- OS : Mac OS X 8, 9, Windows 7, Ubuntu 13.10
- IDE : IntelliJ IDEA 13.0

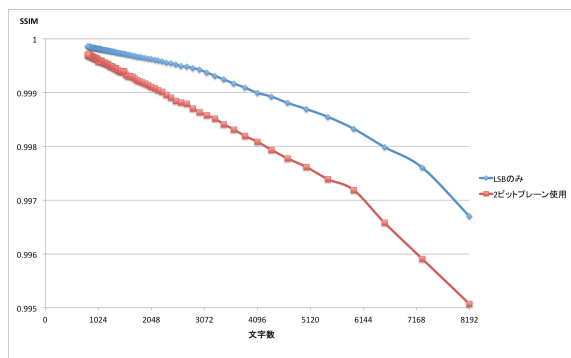


図 15 埋込率に対する誤り率の変化

7. 画像の入手元

1. 神奈川大学
http://www.ess.ic.kanagawa-it.ac.jp/app_images-j.html
2. 京都大学
http://vision.kuee.kyoto-u.ac.jp/IUE/IMAGE_DATABASE/STD_IMAGES/index.html
3. Ashi-LAB
<http://assy.sakura.ne.jp/idba.html>
4. Rensselaer Polytechnic Institute <http://www.cipr.rpi.edu/resource/stills/index.html>

8. おわりに

本研究では誤りパターン埋め込み法における埋め込み率と誤り率、画質劣化とのトレードオフ関係を実験的に明らかにした。これによって、埋め込みを LSB 平面に限定した場合、埋め込み率、誤り率によって画質が大きく劣化することはなく、ステガノグラフィ技術の隠蔽性に大きく影響を与えることはないということがわかった。さらに、この結果から埋め込み範囲を広げての SSIM の計測を行い、2 ビットプレーンを使用することでほとんどの画像に対し 1.9 倍近くのテキスト情報の埋め込みが可能であること、画像を適切に選択することで 3 倍以上ものテキスト情報の埋め込みが可能であることを示した。

また、Shalkwijk の数え上げ符号を用いた誤りパターンへの動的な変換方法を提案することで、強いメモリ制約下における誤りパターンテーブルの実装問題に対する解決策を示した。しかし、本実験で使用した環境

は決してメモリ制約の強い環境ではないため、今後実際に強いメモリ制約下での実験を行う必要がある。

参考文献

- [1] Z.Wang, A.C.Bovik, H.R.Sheikh, E.P.Simoncelli. Image quality assessment: From error visibility to structural similarity. *IEEE TRANSACTIONS ON IMAGE PROCESSING*, Vol. 13, No. 4, pp. 600–612, April 2004.
- [2] 合田翔, 渡辺峻, 松本和幸, 吉田稔, 北研二. コスト付き符号化を用いたステガノグラフィ. 信学技法 IT, Vol. 113, No. 153, pp. 5–9, 7 2013.
- [3] J.P.M.Shalkwijk. An algorithm for source coding. *IEEE TRANSACTIONS ON INFORMATION THEORY*, Vol. IT-18, No. 3, pp. 395–399, May 1972.