

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

索手イッペイ†

福岡久雄†

松江高専†

1 はじめに

ステガノグラフィとは秘密データをメディアデータに埋め込む技術、研究分野の総称である。一般的な通信では秘密データを暗号化し、それを相手に送信する。しかし、この方法では秘密データの内容そのものを隠蔽することはできるが、通信行為そのものは他者に認知されてしまうため通信妨害をうける可能性がある。一方ステガノグラフィではメディアデータ内に秘密データを埋め込むため、第三者に秘密データの存在を知覚されずに通信を行うことができる。

ステガノグラフィでは基本的にメディアデータの冗長性を利用して秘密データを埋め込みを行う。しかし、埋め込む秘密データの容量が増加するほどにメディアデータの質は劣化する。ステガノグラフィではその性質から多くのデータを埋め込むことが可能であること、そしてそれと同時に埋め込みが主観的・客観的に認知されないことが求められる。

本研究ではグレースケール画像にテキスト情報を埋め込むようなステガノグラフィ技術を対象とし、誤りパターン埋込み法における画質劣化と埋め込み率とのトレードオフ関係を実験的に明らかにする。

2 誤りパターン埋込み法の概要

ステガノグラフィ技術における代表的な埋め込み方式の一つに LSB 法がある。この手法では秘密データのバイナリ表現をメディアデータの LSB 平面とそのまま置換することによって埋め込みを行う。この手法はアルゴリズムが単純であり多くの情報をメディアデータに埋め込むことができるほか、LSB のみへ埋め込みを行うことからメディアデータの品質劣化が少ない。一方で LSB との置換を無加工で行うことから埋め込み後のビットの変化が起りやすいため画質劣化が大きくなりやすいという問題がある。ここで、埋め込みに使用したビット列

長 n に対し、埋め込んだデータ量 $n_{embedded}$ との割合を埋め込み率、変化したビット数 $n_{inverted}$ との割合を誤り率といい、それぞれ以下の式で表される。

$$\text{埋め込み率} = \frac{n_{embedded}}{n}, \quad \text{誤り率} = \frac{n_{inverted}}{n}$$

これまで LSB 法の誤り率を改善したいいくつか手法が提案されてきた。その一つとして誤りパターン埋め込み法が知られている。この手法は秘密データをより冗長で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し、誤りパターンと画像の LSB 平面との排他的論理和で LSB 平面を置き換える。こうすることで、埋め込み後のビットの変化を少なくし、LSB 法に比べ優れた誤り率を実現している。しかし、1 データの埋め込みにより長いビット列を必要とすることから埋め込み率は LSB 法に劣ってしまう。

3 誤りパターンの生成

誤りパターンへの変換方法の一つに秘密データ内に出現するビットパターンと誤りパターンの対応を表すテーブルを用意する方法が知られている。しかし、秘密データの大きさを m とすると 2^m 個の要素を対応付けたテーブルが必要となり、テーブルが膨大となりやすいことからメモリ制約の大きい環境での実装が困難になるという問題点があげられる [1]。そこで本研究では Shalkwijk の数え上げ符号 [2] を用いた埋め込みデータから誤りパターンを動的に生成する手法を提案する。Shalkwijk の数え上げ符号とは、長さ n 、ハミング重み k の 2 進数の集合に対し nC_k 種類の 2 進数を一意に割り当てる符号化方式であり、これを用いて各ビットパターンに対して誤りパターンとの相互変換を行うことができる。

4 実験方法

実験手順の概要を図 1 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 8bit グレースケール Bitmap である自然画像 100 枚を使用し、埋め込みに使用するメッセージはほぼ当確率で発生する 8bit コードの列とした。

A study on steganography based on embedding error patterns

†Ipppei Nawate Hisao Fukuoka

†Matsue College Of Technology

- (1) メッセージの各コードを Shalkwijk の数え上げ符号を用いて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[3]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。

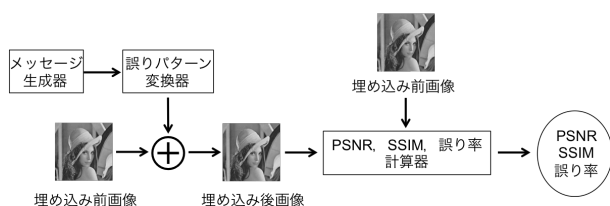


図 1 実験概要 1

5 実験結果

誤り率に対する埋め込み率と参考文献 [1] の式 (4) で表される 2 値エントロピー関数 $H(\Delta)$ の変化のグラフを図 2 に、埋め込み率による画像ごとの SSIM の変化のグラフを図 3 に示す。

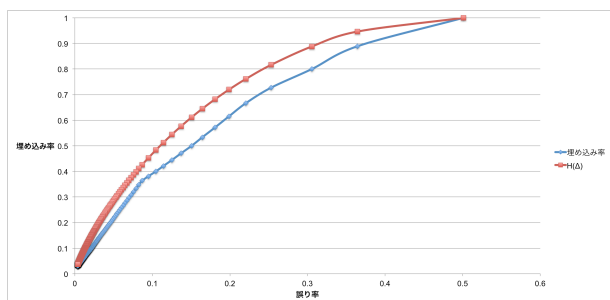


図 2 誤り率に対する埋め込み率と $H(\Delta)$ 変化

図 2 より、埋め込み率に対する誤り率の遷移が参考文献 [1] の図されたグラフと同様緩やかな曲線となった。このことから Shalkwijk の数え上げ符号を用いて誤りパターンテーブルを用いた場合の誤りパターン埋め込み法と同等の機能を実現できたことがわかった。

また、図 3 より SSIM が最低でも約 0.996 と SSIM の基準値である 0.98 を上回っていることがわかる。これは画質劣化が許容される範囲で LSB だけでなく 2bit 列目への埋め込みが可能であることを示しており、また画

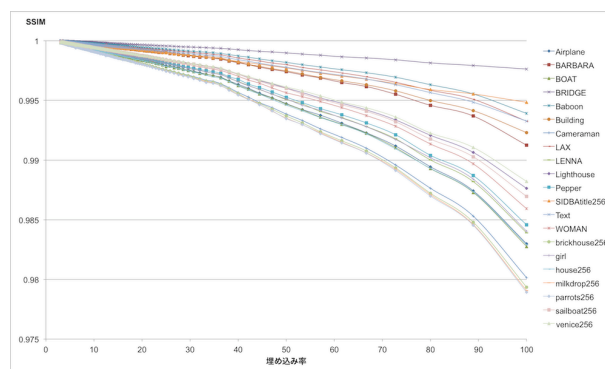


図 3 画像ごとの SSIM の変化

像ごとに同じ埋め込み率に対する SSIM が異なることから、画像によっては 3bit 目 4bit 目への埋め込みも可能であると考えられる。

6 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画質劣化のトレードオフ関係を実験的に明らかにし、これによって画質劣化という観点においてほとんどの画像で LSB 以降への埋め込みが有効であることがわかった。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、誤りパターンテーブルの肥大化問題を解決した。

参考文献

- [1] 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.
- [2] J.PIETER M.SHALKWIJK. An algorithm for source coding. *IEEE TRANSACTIONS ON INFORMATION THEORY*, Vol. IT-18, No. 3, pp. 395–399, May 1972.
- [3] Zhou Wang, Alan Conrad Bovik, Hamid Rahim Sheikh, and Eero P.Simoncelli. Image quality assessment: From error visibility to structural similarity. *IEEE TRANSACTIONS ON INFORMATION THEORY*, Vol. 13, No. 4, pp. 600–612, April 2004.