ソーラス符号を用いた電子透かしの提案
Proposal of digital watermarking using Sourlas codes

平田 展裕 † 川村 正樹 ‡
Nobuhiro Hirata Masaki Kawamura

1. はじめに

電子透かしとは，画像や音楽，動画などのデジタルコンテンツに秘密情報を埋め込む技術である．秘密情報が埋め込まれた画像は，JPEG 圧縮で情報を削減されたり，切り取られたりされる可能性がある．秘密情報を直接埋め込む場合，これらの攻撃に対する耐性が弱く，正しく情報を取り出すことができなくなる可能性がある．そこで，秘密情報を直接埋め込まずに，誤り訂正符号を用いて符号化し，冗長化した情報を埋め込むことを考える．

提案手法では，誤り訂正符号にソーラス符号 [**?**, **?**] を用いる．ソーラス符号は，誤り訂正符号の一種であり，秘密情報のビット列をそのまま用いるのではなく，ビット間の積をパリティとして用いるものである．あるビットに対して他のすべてのビットとの積を求めるため，冗長度の高い誤り訂正符号になる．

電子透かしに対して切り取り攻撃を考える場合，ソーラス符号のように冗長度が高い符号を用いていれば，切り取られた画像からだけでも正しくメッセージを読み取ることができる．本研究では，取り出したパリティから正しく秘密情報を得ることができるかを検証する．また，画質も評価する．計算機シミュレーションでは，情報ハイディング及びその評価基準 (IHC) 委員会 [**?**] の電子透かしコンテストにおける評価基準に従う．

本研究では，ソーラス符号を用いた電子透かしを提案する．2. では，ソーラス符号について説明する．3. では，提案手法の埋め込みと復号のアルゴリズムについて述べる．4. では，計算機シミュレーションの結果を示す．5. で，まとめを述べる．

2. ソーラス符号

ソーラス符号 [**?**, **?**] は，誤り訂正符号の一種である．ソーラス符号では，メッセージ $\boldsymbol{\xi} = (\xi_1, \xi_2, \cdots, \xi_N)^\top, \xi_i \in \{+1, -1\}, i = 1, 2, \cdots, N$ に対して，K ビットの積であるパリティ，

$$J_{i_1 i_2 \cdots i_K} = \xi_{i_1} \xi_{i_2} \cdots \xi_{i_K}, \tag{1}$$

を作る．これは，N ビットから K ビットを選ぶ組み合わせのすべてについて考えるので，元のメッセージ $\boldsymbol{\xi}$ よりも冗長性をもっている．また，$N \to \infty$ の極限のとき，$K \to \infty$ とすると，ソーラス符号は，シャノンの限界を漸近的に満たすことが知られている [**?**, **?**]．本研究では $K = 2$ を考える．すなわち，2 つのビットの積の組み合わせをすべて考える．N ビットのメッセージ $\boldsymbol{\xi}$ に対して，パリティ $\boldsymbol{J}$ の総数は ${}_N C_2$ ビットである．2 体のソーラス符号において，i 番目と j 番目のメッセージビットのパリティ J_{ij} は，

$$J_{ij} = \xi_i \xi_j \quad (i < j), \tag{2}$$

で求めることができる．電子透かしとして用いる場合，パリティ $\boldsymbol{J}$ をメッセージ $\boldsymbol{\xi}$ の代わりに画像へ埋め込む．

取り出したパリティ $\boldsymbol{J'}$ から元のメッセージ $\boldsymbol{\xi}$ を求めるには，次の式を反復すればよい．t ステップ目の推定メッセージ $\boldsymbol{\sigma}^t = (\sigma_1^t, \sigma_2^t, \cdots, \sigma_N^t)^\top, \sigma_i^t \in \{+1, -1\}$ とすると，

$$\sigma_i^{t+1} = \mathrm{sgn}\left(\sum_j J'_{ij} \sigma_j^t \right), \tag{3}$$

で求めることができる．ここで，関数 $\mathrm{sgn}(x)$ は，

$$\mathrm{sgn}(x) = \begin{cases} +1 & (x \geq 0) \\ -1 & (x < 0) \end{cases}, \tag{4}$$

である．σ^0 は，初期値であり，任意に発生させた乱数で決める．

3. 提案手法

3.1. 埋め込みアルゴリズム

メッセージ $\boldsymbol{\xi}$ からパリティ $\boldsymbol{J}$ を作成する．このパリティ $\boldsymbol{J}$ を，YUV 画像の Y 成分に埋め込む．Y 成分を 8×8 画素でブロック分割し，ブロックごとに DCT を行う．DCT 係数に Quantization Index Modulation(QIM)[**?**, **?**] を用いてパリティ $\boldsymbol{J}$ の 1 つを埋め込む．埋め込む座標は，全ブロック $(0, 4)$ とする．埋め込み後，ブロックごとに IDCT を行い，原画像の U,V 成分と合わせて，画像を構成する．パリティが埋め込まれた画像をステゴ画像と呼ぶ．

3.2. 復号アルゴリズム

ステゴ画像の Y 成分をブロック分割して，ブロックごとに DCT を行い，DCT 係数から QIM を用いて埋め込んだパリティ $\boldsymbol{J}$ を取り出す．取り出したパリティ $\boldsymbol{J'}$ から，(**??**) より，元のメッセージ $\boldsymbol{\xi}$ を推定する．

4. 計算機シミュレーション

IHC 評価画像 [**?**] を用いて，第二回電子透かしコンテストの評価基準を元に計算機シミュレーションで評価する．評価画像は，4608×3456 の YUV 画像 6 種類である．メッセージ $\boldsymbol{\xi}$ は，8 次の M 系列乱数を用いて 10 種類の初期値から 10 種類のメッセージ 200 ビットを作成する．作成したメッセージ $\boldsymbol{\xi}$ からソーラス符号を用いて，埋め込むパリティ $\boldsymbol{J}$ を 19,900 ビット作成する．YUV 画像の Y 成分 $\boldsymbol{f}^{org} = (f_1^{org}, f_2^{org}, \cdots, f_P^{org})^\top$ を 8×8 のブロックに分割し，各ブロックの座標 $(0, 4)$ に 1 ビットずつ QIM を用いて埋め込んでいく．ここで，P は総画素数 $P = 4608 \times 3456$ である．また，ブロックの総数は，248,832

†山口大学理学部
‡山口大学大学院理工学研究科

評価画像	BER	PSNR[dB]
1	0.00	39.6
2	0.00	41.5
3	0.00	41.8
4	0.00	44.1
5	0.00	41.7
6	0.00	38.8
平均	0.00	41.3

表 1: 提案手法における BER と PSNR

個であり，そのうちの約 8% にあたる 19,900 個のブロックを用いる．IHC 評価基準に従い，埋め込み処理を行ったステゴ画像 $\boldsymbol{f}^{stego} = (f_1^{stego}, f_2^{stego}, \cdots, f_P^{stego})^\top$ を，1/15 以下になるように JPEG 圧縮する．JPEG 圧縮された画像を，さらに 1/2 圧縮し，2 回圧縮したステゴ画像 $\tilde{\boldsymbol{f}}^{stego} = (\tilde{f}_1^{stego}, \tilde{f}_2^{stego}, \cdots, \tilde{f}_P^{stego})^\top$ を作成する．圧縮後は，埋め込んだパリティ $\boldsymbol{J}$ を QIM を用いて取り出し，取り出したパリティ $\boldsymbol{J}'$ から，(**??**) より，推定メッセージ $\boldsymbol{\sigma}$ を求める．

性能はビット誤り率 BER で評価する．メッセージ $\boldsymbol{\xi}$ と推定メッセージ $\boldsymbol{\sigma}$ のビット誤り率 BER は，

$$\mathrm{BER} = \frac{1-M}{2}, \tag{5}$$

で定義される．ここで，M は，

$$M = \frac{1}{N}\sum_{i=1}^{N} \xi_i \sigma_i, \tag{6}$$

である．2 回圧縮したステゴ画像 $\tilde{\boldsymbol{f}}^{stego}$ の画質を PSNR で評価する．

IHC 評価画像が 6 種類，メッセージが 10 種類ある．表**??**に各画像ごとにメッセージ 10 種類を各 1 回ずつ埋め込んだ時の BER と PSNR の平均を示す．IHC 委員会の評価基準では，高画質の条件として，BER が各画像に対して 1.0% 以下でなければならないとされている．提案手法の結果では，すべて BER が 1.0% 以下なので，この基準は満たしている．また，画質 PSNR は，最低基準が 30dB 以上とされている．提案手法の結果では，PSNR はすべて 38dB 以上と基準よりも高い画質をもっている．

次に，圧縮率を 1.0%(1/100) から 3.3%(1/30) の間で変えた場合の，各画像における BER を図**??**に示し，PSNR を図**??**に示す．IHC 委員会の評価基準では，高耐性の条件として，BER が各画像に対して 0% でなければならないとされている．図**??**より，2.5%(1/40) 圧縮までなら，全ての画像において圧縮耐性を持つ．また，その時の画質 PSNR は，すべて 30dB 以上となった．

5. まとめ

ソーラス符号を用いた電子透かしを検証した．IHC 評価基準に従い，計算機シミュレーションを行った．高画質の基準に基づくと，BER は平均で 0 であり，画質 PSNR の平均は 41dB となった．高耐性の基準に基づくと，2.5% 圧縮まで耐性をもつという結果となった．これらの結果より，ソーラス符号を用いた電子透かしの実用性が期待できる．

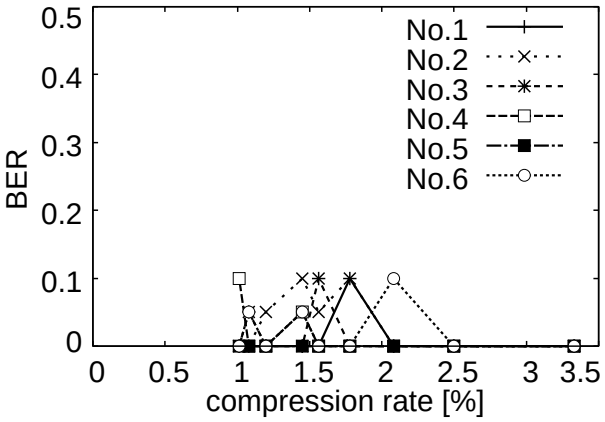

図 1: 圧縮率による各画像の BER

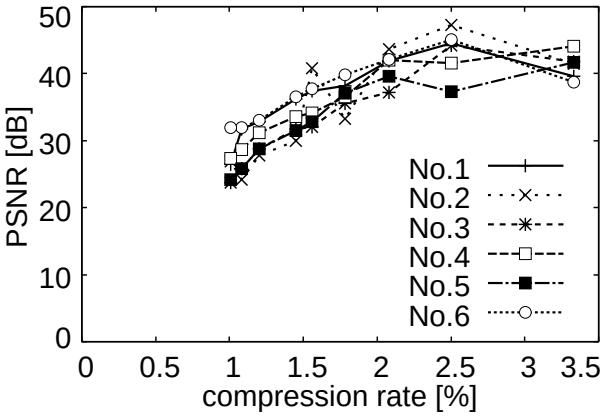

図 2: 圧縮率による各画像の PSNR

参考文献

[1] N. Sourlas, “Spin-glass models as error-correcting codes,” Nature, vol.339, pp.693-695, 1989

[2] 西森秀稔, “スピングラス理論と情報統計力学,” 岩波書店, 1999

[3] B. Chen and G. W.Wornell, “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” IEEE Trans. Inform. Theory, vol.47, No.4, pp.1423-1443, 2001

[4] I. J. Cox, M. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, “Digital watermarking and steganography,” 2nd Ed., Morgan Kaufmann, 2007.

[5] 情報ハイディング及びその評価基準委員会, http://www.ieice.org/iss/emm/ihc/