社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

Wet Paper 符号に対する IST 法の導入とその問題点に関する検討

山本　隆博†　　川村　正樹†

† 山口大学大学院理工学研究科　〒 753–8512 山口県山口市吉田 1677–1
E-mail: ††m-kawamura@m.ieice.org

あらまし　Wet Paper 符号に対して IST 法を導入する．電子透かしでは，ステゴ画像への影響が小さいことを求められる．画像への影響を最小するために，原画像からステゴ画像への差分が小さいステゴ画像を求めることを必要とされる．スパースな差分を求める方法として，圧縮センシングで用いられる IST 法を用いる．Wet Paper 符号は演算をガロア体 GF(2) 上で行い，IST 法は演算を実数体 $\mathbb{R}$ 上で行う．Wet Paper 符号で求めた二値ベクトルを用いる IST 法と緩和した Wet Paper 符号で求めた実ベクトルを用いる IST 法を比較すると，後者の方がメッセージ情報を低い誤り率で推定できる．しかしながら，ステゴ画像のパリティベクトルが実数となるので，ステゴ画像が作成できない問題点がある．そこで，Wet Paper 符号の演算を実数体 $\mathbb{R}$ 上に拡張し，画素値に埋め込む手法を提案する．本手法を用いた結果，メッセージ情報を低い誤り率で推定でき，ステゴ画像を作成できた．
キーワード　電子透かし，Wet Paper 符号，スパース推定，IST 法，圧縮センシング

Consideration of introduction of IST method to wet paper code and its problem

Takahiro YAMAMOTO† and Masaki KAWAMURA†

† Graduate School of Science and Engineering, Yamaguchi University
1677–1 Yoshida, Yamaguchi-shi, Yamaguchi 753–8512 Japan
E-mail: ††m-kawamura@m.ieice.org

Abstract　We introduce the IST method to wet paper code (WPC). Smaller degradation for a stego image is preferred for digital watermarking. In order to minimize the degradation of the image, small difference between the cover image and the stego one is required. We apply the IST method, which is used in the compressive sensing, to WPC in order to get sparse solutions. While the caluculation in WPC is on the Galois Field GF(2), one in IST method is on real number field $\mathbb{R}$. Compared the IST method using binary vector generated from WPC to the IST method using real vector generated from relaxed WPC. The latter can achieve lower bit error rate (BER) of messages. However, no stego image can be constructed due to real parity vector for the stego image. We, therefore, propose the method that the calculation in WPC is on real number field $\mathbb{R}$ and watermarks are embeded into pixel values not parity bits in the image. As a result, our method can estimate messages with low BER and construct a stego image.
Key words　digital watermarking, wet paper code, sparse estimation, IST method, compressive sensing

1. ま え が き

電子透かしとは，画像や音楽などのデジタルコンテンツに著作者情報などを秘密裏に埋め込む技術である．電子透かしの手法として，メッセージ情報をスペクトル拡散し，係数に埋め込むスペクトル拡散型電子透かし [1]〜[5] や係数を量子化することにより，透かし情報を埋め込む Quantization Index Modulation (QIM) [6]〜[8] や，画像に影響を与えにくい箇所を選択し，その箇所に透かし情報を埋め込む Wet Paper 符号 [9] が提案されている．

透かし情報を埋め込むとき，埋め込み位置を決めなければならない．埋め込み位置を画素の値や画素の近傍から決定したり，予め決めておいた位置を使用したりすれば，復号者は埋め込み位置を簡単に特定することができる．しかしながら，この規則を攻撃者に知られると，透かし情報の解読や改ざん，破壊などの攻撃を行うことができる．したがって，攻撃者に埋め込み位

置を知られず，復号者が透かし情報を復号できる必要がある．この問題を解決する手法として Wet Paper 符号 [9] がある．

Wet Paper 符号とは，原画像から作成した二値のデータに透かしを埋め込む手法である．埋め込み時に，透かし情報の埋め込み位置を指定することができ，復号時に，埋め込み位置の情報を必要としない利点がある．透かしを埋め込んだステゴ画像は原画像からの変化が小さいことを必要とされる．Wet Paper 符号では，透かし情報の埋め込み位置を指定できるので，最適な埋め込みは，画像への影響が小さい箇所を選択することである．しかしながら，原画像とステゴ画像の差分が最小になるように，埋め込み位置の組み合わせを考えることは，膨大な組み合わせを考える必要があるので，最適な埋め込み位置を決めることは難しい．埋め込み位置の全ての組み合わせを求める方法は NP 困難である．ここで，変化が小さいとは，差分がスパースであるということである．スパースとは，非 0 の要素数がわずかであり，0 の要素数が多いことを表す．また，k-スパースとは，全要素中に非 0 の要素が k 個であることを表す．

スパースな解を求める手法として，圧縮センシングで用いられるスパース推定 [10]〜[16] が知られている．スパース推定とは，観測された低次元の信号から，高次元のスパースな原信号を推定することである．スパース推定の問題は最適化問題として定式化できる．スパース推定法として，Approximate Message Passing (AMP) 法 [13] や Iterative Shrinkage Thresholding (IST) 法 [14], [15] がある．AMP 法はメッセージ伝搬アルゴリズムと呼ばれる反復法に基づき，近似的に周辺分布を求め，解く手法である．IST 法は最適化問題をしきい値関数を用いて，反復的に解く手法である．

Wet Paper 符号はガロア体 GF(2) 上で演算を行い，IST 法は実数体 $\mathbb{R}$ 上で演算を行う．本稿では，実数体 $\mathbb{R}$ 上の演算と区別するために，ガロア体 GF(2) 上で演算を行う場合は，式に mod 2 と書く．

本研究では，Wet Paper 符号に対して IST 法の導入し，その問題点に関して検討する．本稿は次のように構成される．2. では，Fridrich ら [9] の Wet Paper 符号について説明する．3. では，スパース推定と IST 法について説明する．4. では，Wet Paper 符号に対して IST 法を導入し，問題点について述べる．5. では，IST 法を用いて，画素値に埋め込む手法を提案する．6. で，まとめを述べる．

2. Wet Paper 符号

Fridrich ら [9] の Wet Paper 符号を用いた電子透かしの手法では，画素値から求めたパリティビットにメッセージ情報を埋め込む．総画素数 n の原画像の埋め込み可能位置の集合 $C \subset \{1, 2, \cdots, n\}$ から k 個の埋め込み位置を選択する．集合 C を選ぶ方法を Selection Rule (SR) という．SR はランダムであったり，送信者が選択したり，原画像の情報を利用するなどの方法がある．

2.1 埋め込み

メッセージ長 q のメッセージ情報を $\boldsymbol{m} = (m_1, m_2, \cdots, m_q)^\top$, $m_j \in \{0, 1\}, j = 1, 2, \cdots, q$ とする．このメッセージ情報 $\boldsymbol{m}$ を原画像 $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)^\top$ に埋め込む．ここで，$q < n$ である．原画像の画素値 x_i を 8 ビットで表現し，8 ビット内の 1 の個数からパリティビット $r_i \in \{0, 1\}$ を作成する．作成したパリティビットのビット列をパリティベクトル $\boldsymbol{r} = (r_1, r_2, \cdots, r_n)^\top$ とする．

原画像 $\boldsymbol{x}$ から作成したパリティベクトル $\boldsymbol{r}$ を変更し，ステゴ画像のパリティベクトル $\boldsymbol{r}' = (r'_1, r'_2, \cdots, r'_n)^\top$ を作成する．このとき，ステゴ画像のパリティベクトル $\boldsymbol{r}'$ は，

$$\boldsymbol{A}\boldsymbol{r}' = \boldsymbol{m} \bmod 2, \tag{1}$$

を満たす必要がある．ここで，行列 $\boldsymbol{A}$ は擬似乱数により作成される $q \times n$ の 0 と 1 からなる二値行列であり，その乱数の種は秘密鍵として埋め込み者と復号者で共有する．

パリティベクトル $\boldsymbol{r}$ とステゴ画像のパリティベクトル $\boldsymbol{r}'$ の差分ベクトル $\boldsymbol{\omega}$ を，

$$\boldsymbol{\omega} = \boldsymbol{r}' - \boldsymbol{r} \bmod 2, \tag{2}$$

とする．差分ベクトル $\boldsymbol{\omega}$ は $\boldsymbol{r}$ に対して，変化した位置の値は 1 になり，変化しなかった位置は 0 となる．この差分ベクトル $\boldsymbol{\omega}$ を用いると，(1) は，

$$\boldsymbol{A}\boldsymbol{\omega} = \boldsymbol{m} - \boldsymbol{A}\boldsymbol{r} \bmod 2, \tag{3}$$

となる．埋め込み時，メッセージ情報 $\boldsymbol{m}$ と行列 $\boldsymbol{A}$ とパリティベクトル $\boldsymbol{r}$ は既知であるので，定数ベクトル $\boldsymbol{b}$ を，

$$\boldsymbol{b} = \boldsymbol{m} - \boldsymbol{A}\boldsymbol{r} \bmod 2, \tag{4}$$

とおくと，(3) は，

$$\boldsymbol{A}\boldsymbol{\omega} = \boldsymbol{b} \bmod 2, \tag{5}$$

と表せる．

ステゴ画像のパリティベクトル $\boldsymbol{r}'$ を求めるためには，方程式 (5) を解き，差分ベクトル $\boldsymbol{\omega}$ を求める必要がある．ここで，$q < n$ であるので，そのままでは，解くことができない．しかしながら，$\boldsymbol{\omega}$ の要素から k 個選択し，k が方程式の個数 q 以下であれば，解くことができる．埋め込み者は $\boldsymbol{\omega}$ の要素から集合 C に含まれる k 個の要素を任意に選択することができる．選択された k 個の要素のベクトルを $\boldsymbol{c}$ とする．また，$\boldsymbol{\omega}$ から選択された k 個の各要素に対応する行列 $\boldsymbol{A}$ の列から構成される行列を $\boldsymbol{H}$ とする．この k 次元ベクトル $\boldsymbol{c}$ と $q \times k$ 行列 $\boldsymbol{H}$ を用いて，(5) は，

$$\boldsymbol{H}\boldsymbol{c} = \boldsymbol{b} \bmod 2, \tag{6}$$

と表せる．$q \geqq k$ となるので，連立方程式 (6) を解くことにより，$\boldsymbol{c}$ を求める．$\boldsymbol{\omega}$ は選択された k 個の要素は対応する $\boldsymbol{c}$ の値とし，それ以外の要素は 0 となる．

差分ベクトル $\boldsymbol{\omega}$ を用いて，ステゴ画像のパリティベクトル $\boldsymbol{r}'$ は，

$$\boldsymbol{r}' = \boldsymbol{r} + \boldsymbol{\omega} \bmod 2, \tag{7}$$

となる．ステゴ画像のパリティベクトル $\boldsymbol{r}'$ に対応するように原画

像 $\boldsymbol{x}$ を変更することにより，ステゴ画像 $\boldsymbol{y} = (y_1, y_2, \cdots, y_n)^\top$ を作成する．

2.2 復　　号

ステゴ画像 $\boldsymbol{y}$ からステゴ画像のパリティベクトル $\boldsymbol{r}'$ を作成し，共有秘密鍵から $q \times n$ の二値行列 $\boldsymbol{A}$ を作成する．行列 $\boldsymbol{A}$ とステゴ画像のパリティベクトル $\boldsymbol{r}'$ を用いて，推定メッセージ情報 $\hat{\boldsymbol{m}} = (\hat{m}_1, \hat{m}_2, \cdots, \hat{m}_q)^\top$ は，

$$\hat{\boldsymbol{m}} = \boldsymbol{A}\boldsymbol{r}' \bmod 2, \tag{8}$$

と求められる．

3. スパース推定

未知の n 次元のベクトルを $\boldsymbol{\omega}$ とし，観測行列 $\boldsymbol{A}$ は $q \times n$ 行列とする．ただし，$q < n$ とする．未知ベクトル $\boldsymbol{\omega}$ と観測行列 $\boldsymbol{A}$ を用いて，観測ベクトル $\boldsymbol{b}$ を，

$$\boldsymbol{A}\boldsymbol{\omega} = \boldsymbol{b}, \tag{9}$$

とする．ここで，観測行列 $\boldsymbol{A}$ は任意の $q \times n$ の行列である．例えば，各要素を 0 と 1 の値を確率 1/2 でとる二値行列や，$\mathcal{N}(0, 1/q)$ に従うガウス行列などがある [11]．q 次元の観測ベクトル $\boldsymbol{b}$ から n 次元の未知ベクトル $\boldsymbol{\omega}$ を推定することを考える．$q < n$ であるので，他に条件がなければ，この解は一意に定まらない．しかしながら，未知ベクトル $\boldsymbol{\omega}$ がスパースなベクトルであるとき，$\boldsymbol{\omega}$ の非 0 の要素数 k が $k \leqq q$ であり，非 0 要素の位置が分かっているのならば，この解は一意に定めることができる．ただし，実際には，非 0 要素の位置が未知であるので，推定することは難しい [11] ．スパース推定を用いると観測ベクトル $\boldsymbol{b}$ からスパースな未知ベクトル $\boldsymbol{\omega}$ を推定することができる．

3.1 Iterative Shrinkage Thresholding (IST) 法

スパースなベクトルを推定する手法として Iterative Shrinkage Thresholding (IST) 法 [14], [15] がある．方程式 (9) の解を求めるために，目的関数 $f(\boldsymbol{A}\boldsymbol{\omega})$ を，

$$f(\boldsymbol{A}\boldsymbol{\omega}) = \frac{1}{2}\left\|\boldsymbol{A}\boldsymbol{\omega} - \boldsymbol{b}\right\|_2^2, \tag{10}$$

とし，スパースな未知ベクトル $\boldsymbol{\omega}$ を求めるために，制約条件として l_1-ノルム $\|\boldsymbol{\omega}\|_1$ 最小化を導入して，推定ベクトル $\hat{\boldsymbol{\omega}}$ を最適化問題，

$$\min_{\boldsymbol{\omega}} \frac{1}{2}\left\|\boldsymbol{A}\boldsymbol{\omega} - \boldsymbol{b}\right\|_2^2, \ \text{subject to } \|\boldsymbol{\omega}\|_1 \leqq s, \tag{11}$$

を解くことにより推定する．ここで，$s > 0$ は制御パラメータである．l_p-ノルムは，

$$\|\boldsymbol{\omega}\|_p = \begin{cases} \left(\sum_{i=1}^{N} |\omega_i|^p\right)^{\frac{1}{p}} & , p > 0 \\ \max\{|\omega_1|, |\omega_2|, \cdots, |\omega_N|\} & , p = \infty \end{cases}, \tag{12}$$

と定義される．最適化問題 (11) を罰則付き最適化問題にすると，

$$\min_{\boldsymbol{\omega} \in R^n} \left\{ \frac{1}{2}\left\|\boldsymbol{A}\boldsymbol{\omega} - \boldsymbol{b}\right\|_2^2 + \lambda\|\boldsymbol{\omega}\|_1 \right\}, \tag{13}$$

となる．$\lambda > 0$ はラグランジュ乗数である．λ が大きいほど推定ベクトル $\hat{\boldsymbol{\omega}}$ はスパースになりやすい．罰則項の l_1-ノルムは微分不可能であるので，最適化問題 (13) を解くことは難しい．

IST 法では，目的関数 $f(\boldsymbol{A}\boldsymbol{\omega})$ をステップ t における解 $\boldsymbol{\omega}^t$ の周りで展開し，近似した目的関数 $\tilde{f}(\boldsymbol{A}\boldsymbol{\omega})$ を用いて推定する．推定ベクトル $\hat{\boldsymbol{\omega}}$ は，

$$\hat{\boldsymbol{\omega}} = \arg\min_{\boldsymbol{\omega} \in R^n} \left\{ \frac{1}{2}\left\|\boldsymbol{\omega} - \boldsymbol{\theta}^t\right\|_2^2 + \eta\lambda\|\boldsymbol{\omega}\|_1 \right\}, \tag{14}$$

で推定できる (導出は付録 1. を参照)．ただし，ベクトル $\boldsymbol{\theta}^t$ は，

$$\boldsymbol{\theta}^t = \boldsymbol{\omega}^t + \eta\boldsymbol{A}^\top\left(\boldsymbol{b} - \boldsymbol{A}\boldsymbol{\omega}^t\right), \tag{15}$$

である．定数 η は，

$$\eta = \frac{1}{wc}, w \geqq 1, \tag{16}$$

であり，w は重み係数である．c は，$\boldsymbol{A}^\top\boldsymbol{A}$ の最大固有値である．

IST 法 [14], [15] は罰則付き最適化問題 (14) の解をソフトしきい値関数を用いて，

$$\hat{\omega}_i^{t+1} = \mathrm{ST}\left(\theta_i^t; \eta\lambda\right), \tag{17}$$

で求める．ここで，ソフトしきい関数 $\mathrm{ST}(x;\lambda)$ とは，

$$\mathrm{ST}(x;\lambda) = \begin{cases} x - \lambda & , \lambda < x \\ 0 & , -\lambda \leqq x \leqq \lambda \\ x + \lambda & , x < -\lambda \end{cases} \tag{18}$$

$$= \mathrm{sgn}(x)\max\left(|x| - \lambda; 0\right), \tag{19}$$

であり，関数 $\mathrm{sgn}(x)$ は，

$$\mathrm{sgn}(x) = \begin{cases} 1 & , x \geqq 0 \\ -1 & , x < 0 \end{cases}, \tag{20}$$

で与えられる．また，関数 $\max(x;y)$ は，

$$\max(x;y) = \begin{cases} x & , x \geqq y \\ y & , x < y \end{cases}, \tag{21}$$

と定義する．

ここまで，ラグランジュ乗数 λ を定数として扱っていた．しかしながら，λ を反復ごとに調節する方法 [16] がある．t 回目の反復時のラグランジュ乗数 λ^t は，

$$\lambda^t = \max\left(\zeta\|\boldsymbol{A}^\top\left(\boldsymbol{b} - \boldsymbol{A}\boldsymbol{\omega}^t\right)\|_\infty; \lambda^{t-1}\right), \tag{22}$$

で与えられる．ここで，ζ は重み係数であり，$0 < \zeta < 1$ とする．ラグランジュ乗数 λ^t を用いると，(17) は，

$$\hat{\omega}_i^{t+1} = \mathrm{ST}\left(\theta_i^t; \eta\lambda^t\right), \tag{23}$$

となる．

4. Wet Paper 符号に対する IST 法の導入

Wet Paper 符号では，連立方程式 (5) を解き，スパースな差分ベクトル $\boldsymbol{\omega}$ を求めることが必要である．そこで，スパース推定を適用することができる．本研究では，Wet Paper 符号にお

ける連立方程式 (5) の解法として IST 法を適用することを考える．Wet Paper 符号はガロア体 GF(2) 上で演算を行い，IST 法は実数体 $\mathbb{R}$ 上で演算を行う．そこで，Wet Paper 符号に対して IST 法を導入し，Wet Paper 符号で求めた二値ベクトル $\boldsymbol{b}$ を用いる IST 法と緩和した Wet Paper 符号で求めた実ベクトル $\boldsymbol{b}$ を用いる IST 法を比較する．

4.1 Wet Paper 符号で求めた二値ベクトルを用いる IST 法

原画像から作成したパリティベクトル $\boldsymbol{r}$ と行列 $\boldsymbol{A}$ を用いて，ベクトル $\boldsymbol{b}$ を，

$$\boldsymbol{b} = \boldsymbol{m} - \boldsymbol{A}\boldsymbol{r} \bmod 2, \tag{24}$$

と求める．求めた二値ベクトル $\boldsymbol{b}$ を用いて，IST 法で連立方程式，

$$\boldsymbol{A}\boldsymbol{\omega} = \boldsymbol{b}, \tag{25}$$

を実数体 $\mathbb{R}$ 上で解くことにより実差分ベクトル $\boldsymbol{\omega}$ を求める．すなわち，実差分ベクトル $\boldsymbol{\omega}$ を反復式 (23) に基づき求める．IST 法を用いて求めた解は実数となるので，二値化する必要がある．すなわち，二値差分ベクトルの要素 ω_i' は，

$$\omega_i' = \begin{cases} 1 & , |\omega_i| > 0 \\ 0 & , |\omega_i| \leqq 0 \end{cases}, \tag{26}$$

で求める．二値差分ベクトル $\boldsymbol{\omega}'$ を用いて，ステゴ画像のパリティベクトル $\boldsymbol{r}'$ を，

$$\boldsymbol{r}' = \boldsymbol{r} + \boldsymbol{\omega}' \bmod 2, \tag{27}$$

と求める．推定メッセージ情報 $\hat{\boldsymbol{m}}$ は，

$$\hat{\boldsymbol{m}} = \boldsymbol{A}\boldsymbol{r}' \bmod 2, \tag{28}$$

と求められる．

4.2 緩和した Wet Paper 符号で求めた実ベクトルを用いる IST 法

Wet Paper 符号の演算を実数体 $\mathbb{R}$ 上で行うため，パリティベクトル $\boldsymbol{r}'$ を実数に緩和する．原画像から作成したパリティベクトル $\boldsymbol{r}$ と行列 $\boldsymbol{A}$ を用いて，実数ベクトル $\boldsymbol{b}$ を，

$$\boldsymbol{b} = \boldsymbol{m} - \boldsymbol{A}\boldsymbol{r}, \tag{29}$$

と実数体上で求める．(24) とは異なり，実数値になることに注意する．求めた実数ベクトル $\boldsymbol{b}$ を用いて，IST 法で連立方程式，

$$\boldsymbol{A}\boldsymbol{\omega} = \boldsymbol{b}, \tag{30}$$

を解くことにより実差分ベクトル $\boldsymbol{\omega}$ を求める．これを二値化すると，誤りを生じてしまう．したがって，二値化せずに実差分ベクトル $\boldsymbol{\omega}$ のままメッセージ情報を推定する．実差分ベクトル $\boldsymbol{\omega}$ を用いて，ステゴ画像の実数ベクトル $\boldsymbol{r}'$ を，

$$\boldsymbol{r}' = \boldsymbol{r} + \boldsymbol{\omega}, \tag{31}$$

と求める．実推定メッセージ情報 $\tilde{\boldsymbol{m}}$ を，

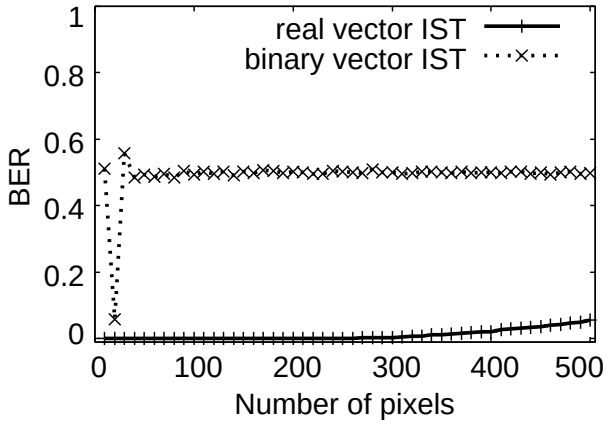


図 1　Wet Paper 符号で求めた二値ベクトルを用いる IST 法と緩和した Wet Paper 符号で求めた実ベクトルを用いる IST 法のビット誤り率 BER

Fig. 1　BER for the IST method using binary vector generated from WPC and the IST method using real vector generated from relaxed WPC

$$\tilde{\boldsymbol{m}} = \boldsymbol{A}\boldsymbol{r}', \tag{32}$$

と求める．実数ベクトル $\boldsymbol{r}'$ を用いるので，実推定メッセージ情報 $\tilde{\boldsymbol{m}}$ に，実数の値が生じる．したがって，推定メッセージ情報を二値化する．二値推定メッセージ情報 $\hat{m}_j$ を

$$\hat{m}_j = \begin{cases} 1 & , |\tilde{m}_j| > 0 \\ 0 & , |\tilde{m}_j| \leqq 0 \end{cases}, j = 1, 2, \cdots, q, \tag{33}$$

と求める．

4.3 計算機シミュレーション

IST 法を用いて Wet Paper 符号における連立方程式 (5) を解き，差分ベクトル $\boldsymbol{\omega}$ を求め，差分ベクトル $\boldsymbol{\omega}$ からメッセージ情報を推定する．メッセージ情報 $\boldsymbol{m}$ とパリティベクトル $\boldsymbol{r}$ の各要素は 0 と 1 の値を確率 1/2 でとる．行列 $\boldsymbol{A}$ は 0 と 1 の二値行列とし，擬似乱数を用いて作成した．メッセージ情報 $\boldsymbol{m}$ と推定メッセージ情報 $\hat{\boldsymbol{m}}$ のビット誤り率 BER を評価する．ビット誤り率 BER は，

$$\mathrm{BER} = \frac{1}{q}\sum_{j=1}^{q} |m_j - \hat{m}_j|, \tag{34}$$

と定義される．メッセージ情報 $\boldsymbol{m}$ と推定メッセージ情報 $\hat{\boldsymbol{m}}$ の要素が全て一致しているとき，ビット誤り率 BER は 0 となる．反転しているとき，ビット誤り率 BER は 1 となる．

画素数を $n = 10, 20, \cdots, 500$ とし，メッセージ長を $q = 0.5n$ とする．(22) の重み係数を $\varsigma = 0.001$ とし，ラグランジュ乗数の初期値を $\lambda^0 = 0.001$ とする．(16) の重み係数は $w = 1$ とする．各画素数のとき，100 回試行を行い，ビット誤り率 BER の平均を求めた．Wet Paper 符号で求めた二値ベクトル $\boldsymbol{b}$ を用いる IST 法と緩和した Wet Paper 符号で求めた実ベクトル $\boldsymbol{b}$ を用いる IST 法のビット誤り率 BER を図 1 に示す．横軸はベクトル $\boldsymbol{\omega}$ の要素数 n であり，縦軸はビット誤り率 BER である．Wet Paper 符号で求めた二値ベクトル $\boldsymbol{b}$ を用いる IST 法は，$n = 20$ を除くどの画素数 n のときもビット誤り率 BER

が高くなり，メッセージ $\boldsymbol{m}$ を推定できていないことがわかる．実数体 $\mathbb{R}$ 上に緩和した Wet Paper 符号で求めた実ベクトル $\boldsymbol{b}$ を用いる IST 法の方がビット誤り率 BER が低い．しかしながら，パリティベクトル $\boldsymbol{r}'$ が実数であり，二値にならない問題点がある．すなわち，そのままでは，ステゴ画像を作成できない問題点がある．

5. 画素値を用いる手法の提案

前節で述べた問題点を解決するために，Wet Paper 符号の演算を実数体 $\mathbb{R}$ 上に緩和し，ベクトル $\boldsymbol{r}$ として画素値を用いる手法を提案する．

5.1 提 案 手 法

画素ベクトルを $\boldsymbol{r} = (r_1, r_2, \cdots, r_n)^\top, r_i \in \{0, 1, 2, \cdots, 255\}, i = 1, 2, \cdots, n$ とする．メッセージ情報 $\boldsymbol{m}, m_j \in \{1, -1\}, j = 1, 2, \cdots, q$ の各要素は ± 1 の値を確率 $1/2$ でとる．行列 $\boldsymbol{A}$ の各要素は $\mathcal{N}(0, 1/q)$ に従って定められるガウス行列とする．画素ベクトル $\boldsymbol{r}$ の値の範囲は 0 から 255 の範囲であるので，画素ベクトル $\boldsymbol{r}$ から 128 を引く．すなわち，減算後の画素ベクトルの要素 r_i^{sub} は，

$$r_i^{sub} = r_i - 128, i = 1, 2, \cdots, n, \tag{35}$$

となる．画素ベクトル $\boldsymbol{r}^{sub}$ と行列 $\boldsymbol{A}$ を用いて，実数ベクトル $\boldsymbol{b}$ を，

$$\boldsymbol{b} = \frac{\boldsymbol{m}}{\|\boldsymbol{m}\|} - \frac{\boldsymbol{A}\boldsymbol{r}^{sub}}{\|\boldsymbol{r}^{sub}\|}, \tag{36}$$

と実数体 $\mathbb{R}$ 上で求める．求めた実数ベクトル $\boldsymbol{b}$ を用いて，IST 法で連立方程式，

$$\boldsymbol{A}\boldsymbol{\omega} = \boldsymbol{b}, \tag{37}$$

を解くことにより実差分ベクトル $\boldsymbol{\omega}$ を求める．実差分ベクトル $\boldsymbol{\omega}$ を用いて，ステゴ画像の実画素ベクトル $\tilde{\boldsymbol{r}}$ を，

$$\tilde{\boldsymbol{r}} = \boldsymbol{r} + \left\|\boldsymbol{r}^{sub}\right\| \boldsymbol{\omega}, \tag{38}$$

と求め，この $\tilde{\boldsymbol{r}}$ の各要素を整数に丸め，ステゴ画像の画素ベクトルの要素 r_i' を，

$$r_i' = \begin{cases} 255 & , \tilde{r}_i > 255 \\ \tilde{r}_i & , 0 \leqq \tilde{r}_i \leqq 255 \\ 0 & , \tilde{r}_i < 0 \end{cases}, \tag{39}$$

と求める．

メッセージ情報の推定には，減算後のステゴ画像の画素ベクトル $\boldsymbol{r}'^{sub}$ を用いる．この要素 $r_i'^{sub}$ は，

$$r_i'^{sub} = r_i' - 128, \tag{40}$$

とする．行列 $\boldsymbol{A}$ の要素を a_{ji} と表すと，推定メッセージの要素 $\hat{m}_j$ は，

$$\hat{m}_j = \mathrm{sgn}\left(\sum_{i=1}^{n} \frac{a_{ji} r_i'^{sub}}{\|\boldsymbol{r}'^{sub}\|}\right), j = 1, 2, \cdots, q, \tag{41}$$

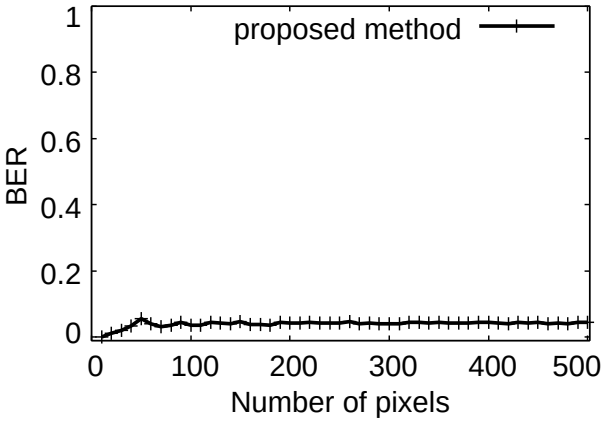


図 2 本手法のビット誤り率 BER
Fig. 2 BER for proposed method

で求められる．

メッセージ情報の要素 m_j は ± 1 の値であるので，ビット誤り率 BER は，

$$\mathrm{BER} = \frac{1 - M}{2}, \tag{42}$$

となる．ここで，M は，

$$M = \frac{1}{q} \sum_{j=1}^{q} m_j \hat{m}_j, \tag{43}$$

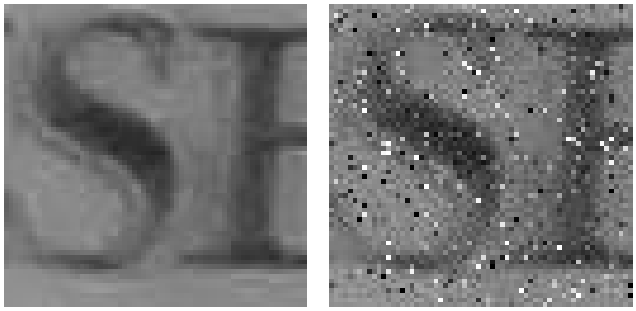
と定義する．メッセージ情報 $\boldsymbol{m}$ と推定メッセージ情報 $\hat{\boldsymbol{m}}$ の要素が全て一致しているとき，ビット誤り率 BER は 0 となる．反転しているとき，ビット誤り率 BER は 1 となる．

画素数を $n = 10, 20, \cdots, 500$ とし，メッセージ長を $q = 0.5n$ とする．(22) の重み係数を $\varsigma = 0.05$ とする．各画素数に対して，100 回試行を行い，ビット誤り率 BER の平均を求めた．本手法のビット誤り率 BER を図 2 に示す．本手法では，ビット誤り率 BER が 0 に近く，メッセージを推定できていることが分かる．さらに，ステゴ画像の画素ベクトル $\boldsymbol{r}'$ は 0 から 255 の値となるようにしているので，ステゴ画像を作成できる．情報ハイディング及びその評価基準 (IHC) 委員会 [17] の IHC 評価画像 2 (Street View) に対して透かしを埋め込む．透かしを埋め込む領域は IHC 評価画像 2 の点 (491,1530) を頂点とした 64×64 の矩形領域とする．画素数を $n = 4096$ とし，メッセージ長を $q = 512$ とする．(22) の重み係数を $\varsigma = 0.05$ としたときの埋め込み前と埋め込み後の IHC 評価画像 2 を図 3 に示す．図 3(b) からステゴ画像を作成できていることを確認できる．

6. ま と め

Wet Paper 符号では，透かし情報の埋め込み位置を任意に指定できる．このとき，画像への影響を最小にするために，スパースな差分 $\boldsymbol{\omega}$ を求める必要がある．スパースな差分 $\boldsymbol{\omega}$ を求める方法としてスパース推定を適用できる．スパース推定として圧縮センシングの解法である IST 法を用いた．

Wet Paper 符号で求めた二値ベクトル $\boldsymbol{b}$ を用いる IST 法と実数体 $\mathbb{R}$ 上に緩和した Wet Paper 符号で求めた実ベクトル $\boldsymbol{b}$ を用いる IST 法を比較すると，後者の方がメッセージ情報を推



(a) 埋め込み前　　(b) 埋め込み後

図 3　IHC 評価画像 2
Fig. 3　IHC evaluation image no.2

定できていた．しかしながら，パリティベクトル $\boldsymbol{r}'$ が二値にならず，ステゴ画像を作成できない問題点があった．そこで，Wet Paper 符号の演算を実数体 $\mathbb{R}$ 上に拡張し，画素値を利用して埋め込む手法を提案した．本手法を用いた結果，ビット誤り率 BER は小さくでき，ステゴ画像が作成できた．

謝　　辞

本研究の一部は文部科学省科学研究費補助金 (若手研究 (B) No. 21700255 及び，基盤研究 (C) No.25330028) の補助を受けて行われた．本研究では，山口大学計算機クラスターシステムを利用した．

文　　献

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for images, audio and video,” IEEE Int. Conf. Image Processing, vol.3, pp.243–246, 1996.
[2] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Processing, vol.6, no.12, pp.1673–1687, 1997.
[3] I. J. Cox, M. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, “Digital watermarking and steganography,” 2nd Ed., Morgan Kaufmann, 2007.
[4] M. Kuribayashi, and M. Morii, “Iterative detection method for CDMA-based fingerprinting scheme,” LNCS, vol.5284, pp.357–371, 2008.
[5] K. Senda, and M. Kawamura, “Statistical-mechanical approach for multiple watermarks using spectrum spreading,” LNCS, vol.5973, pp.231–247, 2010.
[6] M. H. M. Costa, “Writing on dirty paper,” IEEE Trans. Inform. Theory, vol.29, pp.439–441, 1983.
[7] J. J. Eggers, R. Bäuml, R. Tzscchoppe, and B. Girod, “Scalar costa scheme for information embedding,” IEEE Trans. Signal Processing, vol.51, No.4, 2003
[8] 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
[9] J. Fridrich, M. Goljan, P. Lisoněk, and David Soukal, “Writing on wet paper,” IEEE Trans. Signal Processing, vol.53, No.10, pp.3923–3935, 2005
[10] 田中利幸, “圧縮センシングの数理,” IEICE Fundamentals Review, vol.4, No.1, pp.39–47, 2010
[11] 三村和史, “圧縮センシング－疎情報の再構成とそのアルゴリズム－,” 数理解析研究所講究録, vol.1803, pp.26–56, 2012
[12] 樺島祥介, “圧縮センシングへの統計力学的アプローチ,” 日本神経回路学会誌, vol.17, No.2, pp.70–78, 2010
[13] D. L. Donoho, A. Maleki, and A. Montanari, “Message-passing algorithms for compressed sensing,” Proc. Natl. Acad. Sci. USA, vol.106, No.45, pp.18914–18919, 2009
[14] M. A. T. Figueiredo, J. M. Bioucas-Dias, and R. D. Nowak, “Majorization-minimization algorithms for wavelet-based image restoration,” IEEE Trans. Image Processing, vol.16, No.12, pp.2980–2991, 2007
[15] 富岡 亮太, 鈴木 大慈, 杉山 将, “スパース正則化およびマルチカーネル学習のための最適化アルゴリズムと CV・PR への応用,” 信学技報, PRMU, vol.109, No.182, pp.43–48, 2009
[16] S. J. Wright, R. D. Nowak, and M. A. T. Figueiredo, “Sparse reconstruction by separable approximation,” IEEE Trans. Signal Processing, vol.57, No.7, pp.2479–2493, 2009
[17] 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/

付　　録

1. 罰則付き最適化問題 (14) の導出

目的関数 $f(\boldsymbol{A\omega})$ をステップ t における解 $\boldsymbol{\omega}^t$ の周りで展開し近似するために，テイラー展開する．ステップ t における解 $\boldsymbol{\omega}^t$ の周りで第 2 次の項までテイラー展開すると，$\tilde{f}(\boldsymbol{A\omega})$ は，

$$\tilde{f}(\boldsymbol{A\omega}) \simeq f(\boldsymbol{A\omega}^t) + (\nabla_\omega f(\boldsymbol{A\omega})|_{\omega=\omega^t})^\top(\boldsymbol{\omega}-\boldsymbol{\omega}^t) + \frac{1}{2!}(\boldsymbol{\omega}-\boldsymbol{\omega}^t)^\top\nabla^2_\omega f(\boldsymbol{A\omega})|_{\omega=\omega^t}(\boldsymbol{\omega}-\boldsymbol{\omega}^t), \quad \text{(A·1)}$$

となる．(A·1) の右辺第 2 項を

$$\frac{1}{2!}(\boldsymbol{\omega}-\boldsymbol{\omega}^t)^\top\nabla^2_\omega f(\boldsymbol{A\omega})|_{\omega=\omega^t}(\boldsymbol{\omega}-\boldsymbol{\omega}^t) \simeq \frac{1}{2\eta}\left\|\boldsymbol{\omega}-\boldsymbol{\omega}^t\right\|_2^2, \quad \text{(A·2)}$$

と近似する．これより，推定ベクトル $\hat{\boldsymbol{\omega}}$ は，

$$\hat{\boldsymbol{\omega}} = \arg\min_{\omega\in R^n}\left\{f(\boldsymbol{A\omega}^t) + (\nabla_\omega f(\boldsymbol{A\omega})|_{\omega=\omega^t})^\top(\boldsymbol{\omega}-\boldsymbol{\omega}^t) + \frac{1}{2\eta}\left\|\boldsymbol{\omega}-\boldsymbol{\omega}^t\right\|_2^2 + \lambda\|\boldsymbol{\omega}\|_1\right\}, \quad \text{(A·3)}$$

で推定できる．最適化問題を解くとき，定数は無視できるので，定数 $f(\boldsymbol{A\omega}^t)$ を消去し，(A·3) を η 倍すると，

$$\hat{\boldsymbol{\omega}} = \arg\min_{\omega\in R^n}\left\{\eta(\nabla_\omega f(\boldsymbol{A\omega})|_{\omega=\omega^t})^\top(\boldsymbol{\omega}-\boldsymbol{\omega}^t) + \frac{1}{2}\left\|\boldsymbol{\omega}-\boldsymbol{\omega}^t\right\|_2^2 + \eta\lambda\|\boldsymbol{\omega}\|_1\right\}, \quad \text{(A·4)}$$

となり，定数 $1/2\,\|\eta(\nabla_\omega f(\boldsymbol{A\omega})|_{\omega=\omega^t})\|_2^2$ を加えると，

$$\begin{aligned}\hat{\boldsymbol{\omega}} &= \arg\min_{\omega\in R^n}\left\{\eta(\nabla_\omega f(\boldsymbol{A\omega})|_{\omega=\omega^t})^\top(\boldsymbol{\omega}-\boldsymbol{\omega}^t) + \frac{1}{2}\left\|\boldsymbol{\omega}-\boldsymbol{\omega}^t\right\|_2^2 + \eta\lambda\|\boldsymbol{\omega}\|_1 + \frac{1}{2}\|\eta(\nabla_\omega f(\boldsymbol{A\omega})|_{\omega=\omega^t})\|_2^2\right\}\\ &= \arg\min_{\omega\in R^n}\left\{\frac{1}{2}\left\|(\boldsymbol{\omega}-\boldsymbol{\omega}^t) + \eta\nabla_\omega f(\boldsymbol{A\omega})|_{\omega=\omega^t}\right\|_2^2 + \eta\lambda\|\boldsymbol{\omega}\|_1\right\}, \quad \text{(A·5)}\end{aligned}$$

となる．これより，推定ベクトル $\hat{\boldsymbol{\omega}}$ は，

$$\begin{aligned}\hat{\boldsymbol{\omega}} &= \arg\min_{\omega\in R^n}\left\{\frac{1}{2}\left\|\boldsymbol{\omega}-(\boldsymbol{\omega}^t-\eta\nabla_\omega f(\boldsymbol{A\omega})|_{\omega=\omega^t})\right\|_2^2 + \eta\lambda\|\boldsymbol{\omega}\|_1\right\} \quad \text{(A·6)}\\ &= \arg\min_{\omega\in R^n}\left\{\frac{1}{2}\left\|\boldsymbol{\omega}-\boldsymbol{\theta}^t\right\|_2^2 + \eta\lambda\|\boldsymbol{\omega}\|_1\right\}, \quad \text{(A·7)}\end{aligned}$$

となり，(14) を導出できた．