電子透かし検出問題のベイズ推定に基づく解法

宮崎 明雄　九州産業大学 情報科学部 情報科学科
Akio MIYAZAKI　Faculty of Information Science, Kyushu Sangyo University
miyazaki@is.kyusan-u.ac.jp, http://www.is.kyusan-u.ac.jp/~miyazaki/

1. は じ め に

本研究では，透かし入り画像に対する画像処理や攻撃に対応して，電子透かしシステムの検出部を補正することにより透かし情報の検出精度を上げるという立場で，ロバストな電子透かしシステムの設計についてベイズ推定手法を用いて検討を行った．

本研究の一部は，日本学術振興会科学研究費補助金:
【研究種目】基盤研究 (C)
【研究期間】2007〜2009 年度
【課題番号】19560401
【研究課題名】
ベイズ推定に基づくロバストな電子透かし検出システムの開発
Development of Robust Watermark Detection System Based on Bayesian Estimation
【研究代表者】宮崎明雄（九州産業大学）
の助成を受けて遂行された．本稿はその研究成果をまとめたものであり，これにより，電子透かしシステムが現状で耐性をもたないような画像処理や攻撃を受けた場合，及び，将来新たな画像処理や攻撃を受けた場合でも電子透かしが正確に検出できるようになると期待される．

2. 研究の背景及び目的

電子透かしは, マルチメディア情報の違法コピーなどの不正利用を抑止し，製作者や著作権者がマルチメディア情報を発信しやすくするための技術として関心が高まっている．特にディジタル画像については Web で公開したり，アプリケーションソフトウェアによって容易に編集加工が行えるため不正利用される機会が多い．このため画像の著作権保護やコピー制御を目的として数年前から電子透かしが盛んに研究されている [1].

ディジタル画像に対する電子透かしの基本方式は画素利用型と周波数領域利用型に大別される．画素利用型は画素値に処理を施して透かし情報を埋め込む方式である．これに対して，周波数領域利用型は画像データを周波数成分に変換し，特定の周波数成分に埋め込む方式である．後者の方式は前者の方式に比べて多くの透かし情報を埋め込むことはできないが，非可逆圧縮やフィルタリングなどの基本的な画像処理に対して耐性をもった（ロバストな）電子透かしを実現できる．通常，画像への電子透かしにはこのような耐性（ロバスト性）が要求されるので，フーリエ変換， 離散コサイン変換， ウェーブレット変換などの周波数変換を利用した電子透かしが数多く提案されている [1]〜[4]．また，最近ではこれらの方式を採用した電子透かし埋め込み／検出ソフトウェアが市場に現れている．しかしながら，あらゆる画像処理に対して耐性をもった電子透かしは今のところ現れていない．逆に，画像の中の電子透かしを壊してしまうような電子透かし攻撃ツールが出現している．このような状況の中で，現状考え得るすべての画像処理や攻撃に対して耐性をもった電子透かしを開発するのは非常に困難であると思われる．もし開発できたとしても，そのシステムは画像処理ツールや電子透かし攻撃ツールのバージョンアップに対してはロバストでなくなるであろう．

そこで筆者は，透かし入り画像に対する画像処理や攻撃に対応して，電子透かしシステムの検出部を補正することにより透かし情報の検出精度を上げるという立場で，ロバストな電子透かしシステムの設計について検討している．このような立場をとることにより， 電子透かしシステムが現状で耐性をもたないような画像処理や攻撃を受けた場合，及び，将来新たな画像処理や攻撃を受けた場合でも電子透かしが正確に検出できるようになると期待される．このために筆者は，周波数領域利用型の電子透かし埋め込み／検出システムの解析を行い，電子透かしシステムのモデルを透かし情報の入出力関係に注目してコンボリューションモデルとして記述した．そして，透かし入り画像に対する画像処理や攻撃によって「透かし情報がどのように歪むのか？」,「透かし情報の検出誤りがなぜ起きるのか？」を明確にし，透かし情報の歪みモデルを与えた [5][6]．本稿では，この歪みモデルを応用して, 電子透かしの検出問題をデコンボリューションの問題として定式化し分類整理する．そして, 電子透かし検出問題のベイズ推定に基づく解法について議論する．さらに, 本研究に関連して, 通信路等化や画像復元の分野でもブラインドデコンボリューションの問題は現れる．本稿で与えた解法がこれらの分野の諸問題に適用できるかどうかについても簡単に検討する．

3. 電子透かしシステムの解析

本章では, 周波数領域利用型電子透かし方式のモデルと画像処理による透かし情報の歪みモデルについて概説

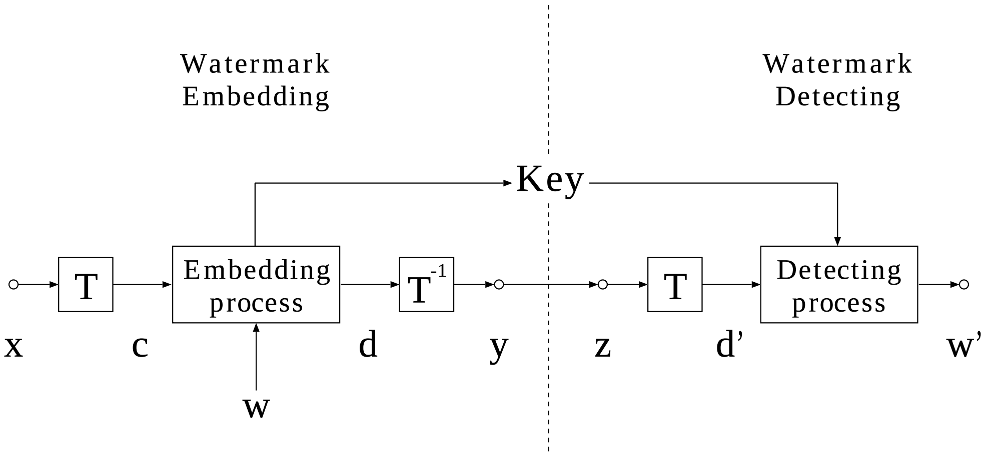

図 1　周波数領域利用型電子透かし方式のモデル

する [5][6].

3·1　電子透かしの埋め込み・検出モデル

周波数領域利用型電子透かし方式のモデルを図 1 に示す.

透かし情報を埋め込む画像（ホスト画像）を $\boldsymbol{x} = [x(m)]$ $(m = 1, 2, \cdots, M)$ (M 次元ベクトル*1）で表す．画像 $\boldsymbol{x}$ に離散ウェーブレット変換（DWT）などの周波数変換 $\boldsymbol{T}$ を施し，得られる変換係数を $\boldsymbol{c} = [c(m)]$ とする (M 次元ベクトル）．また, 透かし情報を $\boldsymbol{w} = [w(k)]$ $(w(k) = 1 \text{ or} -1,\ k = 1, 2, \cdots, K)$ で表す (K 次元ベクトル）.

電子透かしの埋め込み (Embedding process) では, $\boldsymbol{c}$ の中から透かし情報の埋め込み対象領域 $\Re$ が適当に設定され*2，その中から K 個の係数 $c(i_1), c(i_2), \cdots, c(i_K)$ が選ばれて, 透かし情報 $\boldsymbol{w} = [w(k)]$ $(w(k) = 1 \text{ or} -1)$ が量子化制御などの方法を用いて $\{c(i_k)\}$ に埋め込まれる. ここで，透かし入り係数を $\boldsymbol{d}$ で表すと，$\boldsymbol{d}$ に逆変換 $\boldsymbol{T}^{-1}$ を施すことで，透かし入り画像 $\boldsymbol{y}$ が得られる．透かし情報の埋め込み位置や埋め込みで用いられたパラメータのうちいくつかは，鍵データ Key として透かし情報の検出で用いられる.

一方，透かし情報の検出 (Detecting process) では，まず透かし入り画像 $\boldsymbol{z} = [z(m)]$ に周波数変換 $\boldsymbol{T}$ を施すことで変換係数 $\boldsymbol{d'} = [d'(m)]$ を得る．次に，Key を用いて $\boldsymbol{d'}$ の中から透かしが埋め込まれていた係数 $c'(i_1)$, $c'(i_2)$, $\cdots$, $c'(i_K)$ を抽出し，$\{c'(i_k)\}$ から透かし情報 $\boldsymbol{w'} = [w'(k)]$ を検出する.

3·2　画像処理による透かし情報の歪みモデル

本節では，透かし入り画像の保存（蓄積）や画像処理などによって生じる透かし情報の歪みについて簡単に説明する．透かし入り画像 $\boldsymbol{y}$ は通常量子化や圧縮された後に保存される．このとき生じる誤差ベクトルを加法性雑音 $\boldsymbol{n_1}$ で近似すると, 量子化・圧縮された透かし入り画像 $\boldsymbol{y'}$ は

$$\boldsymbol{y'} = \boldsymbol{y} + \boldsymbol{n_1} \tag{1}$$

と書くことができる．この $\boldsymbol{y'}$ が画像処理や攻撃などによって次式のようになったとしよう.

$$\boldsymbol{z} = \boldsymbol{f}(\boldsymbol{y'}) + \boldsymbol{n_2} \tag{2}$$

ここで, $\boldsymbol{f}$ は画像処理を表す作用素で

$$\boldsymbol{f}(\boldsymbol{y'}) = [f_1(\boldsymbol{y'})\ f_2(\boldsymbol{y'})\ \cdots\ f_M(\boldsymbol{y'})]^t \tag{3}$$

であり, $\boldsymbol{n_2}$ は加法性雑音である.

図 1 の電子透かしシステムにおいて, 透かし情報 $\boldsymbol{w}$ と $\boldsymbol{w'}$ の入出力関係に着目し, 透かし情報の埋め込みによる画質劣化は小さい ($||\boldsymbol{x}|| \gg ||\boldsymbol{y} - \boldsymbol{x}||$) ことと, 画像の品質を著しく劣化させるような画像処理や攻撃はなされない ($||\boldsymbol{y}|| \gg ||\boldsymbol{z} - \boldsymbol{y}||$) ことから, 式 (2) の歪みモデルは次のような線形変換の形に近似することができる.

$$\boldsymbol{w'} = \boldsymbol{A}\boldsymbol{w} + \boldsymbol{b} \tag{4}$$

ただし, $||\cdot||$ はベクトルのノルムを表し，$\boldsymbol{A}$ は $\boldsymbol{x}$ と $\boldsymbol{f}$ に依存する $K \times K$ 行列, $\boldsymbol{b}$ は $\boldsymbol{x}$ と $\boldsymbol{f}$, $\boldsymbol{n_1}$, $\boldsymbol{n_2}$ に依存する K 次元ベクトルである

ここで，$N = K + 1$ とおいて, $\boldsymbol{w} = [w(k)]$ を

$$\boldsymbol{w} = [w(1)\ w(2)\ \cdots\ w(K)\ 1] \tag{5}$$

（N 次元ベクトル）と改めて定義する．また, $\boldsymbol{w'} = [w'(k)]$ および $\boldsymbol{A}, \boldsymbol{b}$ からそれぞれ $\boldsymbol{u} = [w'(1)\ w'(2)\ \cdots\ w'(K)\ 0]$ （N 次元ベクトル）および

$$\boldsymbol{H} = \left[\begin{array}{c|c} \boldsymbol{A} & \boldsymbol{b} \\ \hline \boldsymbol{0} & 0 \end{array}\right] \quad (N \times N \text{ 行列}) \tag{6}$$

とおくと (ただし, $\boldsymbol{0}$ は K 次元の零ベクトル), 式 (4) の透かし情報の歪みモデルは

$$\boldsymbol{u} = \boldsymbol{H}\boldsymbol{w} \tag{7}$$

と書くことができる．従って，電子透かしの検出では，この歪みの影響で検出誤りが生じる可能性がある.

---

*1　本稿では特に断らない限り，ベクトルは列ベクトルであるとする.

*2　DWT の場合，MRA 成分（多重解像度近似成分，LL 成分）や，中低域の MRR 成分（多重解像度表現成分，LH・HL 成分）が $\Re$ として用いられる.

4.　ベイズ推定に基づく電子透かしの検出

3･2 節で, 電子透かし埋め込み・検出システムのモデル化とその解析を通して, 電子透かし $\boldsymbol{w}$ が画像処理や攻撃によってどのように歪むかを調べた．その結果, 画像処理や攻撃による画像の歪みが小さいと仮定すると, 画像処理や攻撃を受けた後の透かし情報 $\boldsymbol{u}$ は次のような線形変換の形に書けることを示した（コンボリューションモデル）．

$$\boldsymbol{u} = \boldsymbol{H}\boldsymbol{w} \tag{8}$$

ここで，$\boldsymbol{H} = [h_{ij}]$ はホスト画像と画像処理・攻撃に依存した行列であることに注意しておく．

このような歪みモデルで透かし情報の検出誤りを最小にするためには, $\boldsymbol{u} = \boldsymbol{r}$ を観測したときにそれが $\boldsymbol{w} = \boldsymbol{s}$ である確率 $p(\boldsymbol{s}|\boldsymbol{r})$ を計算し, $p(\boldsymbol{s}|\boldsymbol{r})$ を最大にする $\boldsymbol{s}$ を埋め込まれている透かし情報であるとすれば良い．これはベイズの公式

$$p(\boldsymbol{s}|\boldsymbol{r}) = \frac{p(\boldsymbol{r}|\boldsymbol{s})p(\boldsymbol{s})}{p(\boldsymbol{r})} \tag{9}$$

より $p(\boldsymbol{r}|\boldsymbol{s})p(\boldsymbol{s})$ を最大にすることと等価であり, $p(\boldsymbol{s})$ が一様分布に従うと仮定すると, 尤度関数 $p(\boldsymbol{r}|\boldsymbol{s})$ 又は対数尤度 $\log p(\boldsymbol{r}|\boldsymbol{s})$ を最大にするという最尤推定が使われることになる．ここでは, 電子透かしの検出問題を次の 3 つの場合に分けて, それぞれについて問題の定式化を行い, その解法について議論する．

(1) 歪みモデル $\boldsymbol{H} = [h_{ij}]$ が既知の場合
(2) 歪みモデル $\boldsymbol{H} = [h_{ij}]$ が未知ではあるが, その平均や共分散などの統計的性質が既知で, かつ透かし情報の集合 $S = \{\boldsymbol{s_i}, i = 1, 2, \cdots, L\}$ に関する情報を利用する場合
(3) 歪みモデル $\boldsymbol{H} = [h_{ij}]$ が未知ではあるが, その平均や共分散などの統計的性質が既知である場合

4･1　歪みモデル H が既知の場合

歪みモデル $\boldsymbol{H}$ が既知の場合, $\boldsymbol{r}$, $\boldsymbol{s}$ がガウス分布に従うと仮定すると,

$$\begin{aligned} p(\boldsymbol{r}|\boldsymbol{s}) &= p(\boldsymbol{r}|\boldsymbol{H}, \boldsymbol{s}) \\ &= \frac{1}{\sqrt{(\pi\sigma^2)^N}}\ e^{-\frac{1}{\sigma^2}(\boldsymbol{r}-\boldsymbol{H}\boldsymbol{s})^t(\boldsymbol{r}-\boldsymbol{H}\boldsymbol{s})} \end{aligned} \tag{10}$$

$$\log p(\boldsymbol{r}|\boldsymbol{s}) \doteq -\frac{1}{\sigma^2}(\boldsymbol{r}-\boldsymbol{H}\boldsymbol{s})^t(\boldsymbol{r}-\boldsymbol{H}\boldsymbol{s}) \tag{11}$$

と書けるので, 観測データ $\boldsymbol{r}$（透かし入り係数）から上式の最大化により $\boldsymbol{s}$ の推定を行えば良い．ここで, 上付き添字 t はベクトル・行列の転置を表し, 記号 $\doteq$ は最適化操作の意味で左辺と右辺が等価であることを表している．従って, 観測データ $\boldsymbol{r}$ から $\boldsymbol{H}\boldsymbol{s} = \boldsymbol{r}$ を満たす $\boldsymbol{s}$ を求めるデコンボリューションの問題になる．

もしホスト画像 $\boldsymbol{x}$ と画像処理 $\boldsymbol{f}$ が既知であれば，$\boldsymbol{z} = \boldsymbol{f}(\boldsymbol{y})$ より $\{y(k), z(k)\}$ のデータが得られる．これらのデータから，透かし情報 $\{w(k)\}$ と画像処理後の歪んだ透かし入り係数 $\{u(k)\}$ のデータが得られ，適当な学習アルゴリズムによって $\boldsymbol{x}$ と $\boldsymbol{f}$ に対する $\boldsymbol{H}$ とその逆行列（一般化逆行列）が推定できるので，上記の方法が適用できる [5][6]．一般には，$\boldsymbol{x}$ と $\boldsymbol{f}$ は未知であるため，上記のデコンボリューション問題はブラインドデコンボリューション問題になる．次節以降では，このブラインドデコンボリューション問題を取り扱うこととする．

4･2　歪みモデル H の統計的性質が既知で, かつ透かし情報の集合 S に関する情報を利用する場合

歪みモデル $\boldsymbol{H}$ が未知の場合, $p(\boldsymbol{s}|\boldsymbol{r})$ は

$$p(\boldsymbol{s}|\boldsymbol{r}) = E[p(\boldsymbol{s}, \boldsymbol{H}|\boldsymbol{r})] = \int_{\boldsymbol{H}} p(\boldsymbol{s}, \boldsymbol{H}|\boldsymbol{r})d\boldsymbol{H} \tag{12}$$

ただし,

$$p(\boldsymbol{s}, \boldsymbol{H}|\boldsymbol{r}) = \frac{p(\boldsymbol{r}, \boldsymbol{H}|\boldsymbol{s})p(\boldsymbol{s})}{p(\boldsymbol{r})} \tag{13}$$

となり, 観測データが $\boldsymbol{r}$ のみで不完全データであるため, $p(\boldsymbol{s}, \boldsymbol{H}|\boldsymbol{r})$ 又は $p(\boldsymbol{r}, \boldsymbol{H}|\boldsymbol{s})$ を最大にする $\boldsymbol{s}$ を直接に知ることはできない．そこで, 埋め込まれた透かし情報が $\boldsymbol{s}$ で, これが $\boldsymbol{r}$ として観測されたと仮定し, $p(\boldsymbol{r}, \boldsymbol{H}|\boldsymbol{s})$ 又は $\log p(\boldsymbol{r}, \boldsymbol{H}|\boldsymbol{s})$ の $\{\boldsymbol{r}, \boldsymbol{s}\}$ が与えられたもとでの $\boldsymbol{H}$ に関する条件付期待値

$$\begin{aligned} Q(\boldsymbol{s}) &= E[p(\boldsymbol{r}, \boldsymbol{H}|\boldsymbol{s})|\boldsymbol{r}, \boldsymbol{s}] \\ &= \int_{\boldsymbol{H}} p(\boldsymbol{r}, \boldsymbol{H}|\boldsymbol{s})p(\boldsymbol{H}|\boldsymbol{r}, \boldsymbol{s})d\boldsymbol{H} \end{aligned} \tag{14}$$

$$\begin{aligned} Q(\boldsymbol{s}) &= E[\log p(\boldsymbol{r}, \boldsymbol{H}|\boldsymbol{s})|\boldsymbol{r}, \boldsymbol{s}] \\ &= \int_{\boldsymbol{H}} [\log p(\boldsymbol{r}, \boldsymbol{H}|\boldsymbol{s})]p(\boldsymbol{H}|\boldsymbol{r}, \boldsymbol{s})d\boldsymbol{H} \end{aligned} \tag{15}$$

を計算する．観測データ $\boldsymbol{r}$ と透かし情報のすべての候補 $\boldsymbol{s}$ に対して $Q(\boldsymbol{s})$ を計算し, これを最大にする $\boldsymbol{s}^*$ を埋め込まれていた透かし情報と判定することにする．

$$\boldsymbol{s}^* = \arg\max_{\boldsymbol{s}} Q(\boldsymbol{s}) \tag{16}$$

ここで，$\boldsymbol{r} = [r_k]$，$\boldsymbol{s} = [s_k]$，$\boldsymbol{H} = [h_{ij}]$ がガウス分布に従い，$\boldsymbol{H}$ と $\boldsymbol{s}$ は統計的に独立であると仮定して，式 (15) の $Q(\boldsymbol{s})$ を計算すると式 (17)～式 (22) を得る．このとき，歪みモデル $\boldsymbol{H}$ の要素 h_{ij} の平均と共分散をそれぞれ $E[h_{ij}] = e_{ij}$, $E[(h_{ij} - e_{ij})(h_{kl} - e_{kl})] = \sigma_{ij}^2 (i = k$ かつ $j = l)$; $= 0$(それ以外) とし，$\boldsymbol{h_i} = [h_{ij}]$ (列ベクトル), $\boldsymbol{e_i} = [e_{ij}]$ (列ベクトル), $\boldsymbol{\Lambda_i} = E[(\boldsymbol{h_i} - \boldsymbol{e_i})(\boldsymbol{h_i} - \boldsymbol{e_i})^t]$ (対角行列) とおく．

$$\begin{aligned} Q(\boldsymbol{s}) = &-\frac{1}{\sigma^2}\sum_{k=1}^{N}\left\{(r_k - \boldsymbol{s}'\boldsymbol{d_k})^2 + \alpha_k(\boldsymbol{s})\right\} \\ &- \sum_{k=1}^{N}\left\{(\boldsymbol{d_k} - \boldsymbol{e_k})^t\boldsymbol{\Lambda_k}^{-1}(\boldsymbol{d_k} - \boldsymbol{e_k}) + \beta_k(\boldsymbol{s})\right\} \end{aligned} \tag{17}$$

$$\alpha_k(\boldsymbol{s}) = \frac{1}{2}\boldsymbol{s}^t \boldsymbol{\Delta_k} \boldsymbol{s} \quad (18)$$

$$\beta_k(\boldsymbol{s}) = \frac{1}{2}\mathrm{tr}({\boldsymbol{\Gamma_k}}^t {\boldsymbol{\Lambda_k}}^{-1} \boldsymbol{\Gamma_k}) \quad (19)$$

$$\boldsymbol{\Delta_k} = \boldsymbol{\Gamma_k}{\boldsymbol{\Gamma_k}}^t \quad (20)$$

$$\boldsymbol{d_l} = E[\boldsymbol{h_l}|\boldsymbol{r},\boldsymbol{s}] = \boldsymbol{\Delta_l}\left(\frac{r_l}{\sigma^2}\boldsymbol{s} + {\boldsymbol{\Lambda_l}}^{-1}\boldsymbol{e_l}\right) \quad (21)$$

$$\boldsymbol{\Delta_l} = \left(\frac{1}{\sigma^2}\boldsymbol{s}\boldsymbol{s}^t + {\boldsymbol{\Lambda_l}}^{-1}\right)^{-1} \quad (22)$$

式 (17) において, $\boldsymbol{d_k} = E[\boldsymbol{h_k}|\boldsymbol{r},\boldsymbol{s}]$ $(k = 1, 2, \cdots, N)$ は $\{\boldsymbol{r},\boldsymbol{s}\}$ から推定した歪みモデルを表しており, 右辺第一項は r_k と $\boldsymbol{s}^t\boldsymbol{d_k}$ との差の二乗和, 右辺第二項は $\boldsymbol{d_k}$ と $\boldsymbol{H}$ の先験情報 $\boldsymbol{e_k} = E[\boldsymbol{h_k}]$ との差の (重み付き) 二乗和を表している. 式 (17) の導出については文献 [7] を参照されたい.

以上より, 次のステップで $\boldsymbol{r}$ から $\boldsymbol{s}$ を推定する.

【アルゴリズム I】

(1) σ^2, $\boldsymbol{e_k}$, $\boldsymbol{\Lambda_k}$ の値を設定する. (σ^2, $\boldsymbol{\Lambda_k}$ は式 (17) の右辺の第一項と第二項の重み付けに関係する.) また, 透かし情報の集合を $S = \{\boldsymbol{s_i}, i = 1, 2, \cdots, L\}$ とする.

(2) 観測データと透かし情報の候補の組 $\{\boldsymbol{r},\boldsymbol{s_i}\}$ $(i = 1, 2, \cdots, L)$ に対して $Q(\boldsymbol{s_i})$ を計算する.

(3) $Q(\boldsymbol{s_i})$ を最大にする $\boldsymbol{s}^*$, すなわち,

$$\boldsymbol{s}^* = \arg\max_{\boldsymbol{s_i}} Q(\boldsymbol{s_i}) \quad (23)$$

を求め, $\boldsymbol{s}^*$ を埋め込まれていた透かし情報と判定する.

他方, 式 (15) の $\boldsymbol{Q(s)}$ の計算において, $\boldsymbol{r}$, $\boldsymbol{s}$, $\boldsymbol{H}$ に関する上記と同様の仮定のもとで, ある歪モデル $\boldsymbol{H}^*$ が存在し, これが $\boldsymbol{s}$ を $\boldsymbol{r}$ に歪ませている, すなわち, $\boldsymbol{r} = \boldsymbol{H}^*\boldsymbol{s}$ となっていると考えて, 条件付確率 $p(\boldsymbol{H}|\boldsymbol{r},\boldsymbol{s})$ を

$$p(\boldsymbol{H}|\boldsymbol{r},\boldsymbol{s}) = \delta(\boldsymbol{H} - \boldsymbol{H}^*) = \delta(\boldsymbol{H} - \boldsymbol{H}^*(\boldsymbol{r},\boldsymbol{s})) \quad (24)$$

ただし, $\delta(\cdot)$ はデルタ関数, とおいてみる. その結果, 次式が得られる.

$$\begin{aligned} Q(\boldsymbol{s}) &= \log p(\boldsymbol{r}|\boldsymbol{H}^*,\boldsymbol{s}) + \log p(\boldsymbol{H}^*) \\ &\doteq -\frac{1}{\sigma^2}(\boldsymbol{r} - \boldsymbol{H}^*\boldsymbol{s})^t(\boldsymbol{r} - \boldsymbol{H}^*\boldsymbol{s}) \\ &\quad - \sum_{k=1}^{N}(\boldsymbol{h_k^*} - \boldsymbol{e_k})^t {\boldsymbol{\Lambda_k}}^{-1}(\boldsymbol{h_k^*} - \boldsymbol{e_k}) \end{aligned} \quad (25)$$

以上より, $\boldsymbol{r}$ から $\boldsymbol{s}$ を推定するもう一つのアルゴリズムを得る [8][9].

【アルゴリズム II】

(1) σ^2, $\boldsymbol{e_k}$, $\boldsymbol{\Lambda_k}$ の値を設定する. (σ^2, $\boldsymbol{\Lambda_k}$ は式 (25) の右辺の第一項と第二項の重み付けに関係する.) また, 透かし情報の集合を $S = \{\boldsymbol{s_i}, i = 1, 2, \cdots, L\}$ とする.

(2) 観測データと透かし情報の候補の組 $\{\boldsymbol{r},\boldsymbol{s_i}\}$ $(i = 1, 2, \cdots, L)$ に対して, ノルム $\|\boldsymbol{r} - \boldsymbol{H}\boldsymbol{s_i}\|$ を最小にする $\boldsymbol{H}$ を反復アルゴリズムにより求める. ただし, 反復アルゴリズムの $\boldsymbol{H}$ の初期値は $\boldsymbol{E} = E[\boldsymbol{H}]$ $(\boldsymbol{e_k} = E[\boldsymbol{h_k}])$ とする. このとき得られた $\boldsymbol{H}$ を $\boldsymbol{H}_i^*$ とする.

$$\boldsymbol{H}_i^* = \arg\min_{\boldsymbol{H}} \|\boldsymbol{r} - \boldsymbol{H}\boldsymbol{s_i}\| \quad (26)$$

(3) $\boldsymbol{r}$, $\boldsymbol{H_i^*}$, $\boldsymbol{s_i}$ から $\boldsymbol{H^*} = \boldsymbol{H_i^*}$ とおいて $Q(\boldsymbol{s_i})$ を計算する. そして, $Q(\boldsymbol{s_i})$ を最大にする $\boldsymbol{s}^*$, すなわち, $\boldsymbol{s}^* = \arg\max_{\boldsymbol{s_i}} Q(\boldsymbol{s_i})$ を求め, $\boldsymbol{s}^*$ を埋め込まれていた透かし情報と判定する.

[注意] ステップ **(2)** で得られる $\boldsymbol{H_i^*}$ は $\|\boldsymbol{r} - \boldsymbol{H_i^*}\boldsymbol{s_i}\| \simeq 0$ となっているので, $Q(\boldsymbol{s_i})$ の大小は式 (25) の右辺第二項, すなわち, $\boldsymbol{H_i^*}$ と $\boldsymbol{E}$ ($\boldsymbol{H}$ の先験情報) との差で評価されることになる.

4·3 歪みモデル H の統計的性質が既知である場合

透かし情報の集合 S に関する情報を利用せずに, 透かし情報の歪みモデル $\boldsymbol{H} = [h_{ij}]$ に関する統計的性質 (先験情報) のみを使った電子透かし検出アルゴリズムは, **EM アルゴリズム (Expectation–Maximization algorithm)**[10][11] を用いて導出可能である. EM アルゴリズムは E–step (Expectation–step) と M–step (Maximization–step) と呼ばれる 2 つのステップから成り, これらのステップを反復することにより観測データ $\boldsymbol{r}$ から埋め込まれた透かし情報 $\boldsymbol{s}$ を推定しようというものである.

まず, 式 (13) の右辺の $p(\boldsymbol{r},\boldsymbol{H}|\boldsymbol{s})$ を

$$p(\boldsymbol{r},\boldsymbol{H}|\boldsymbol{s}) = p(\boldsymbol{H}|\boldsymbol{r},\boldsymbol{s})p(\boldsymbol{r}|\boldsymbol{s}) \quad (27)$$

のように変形し, 両辺の対数をとる.

$$\log p(\boldsymbol{r}|\boldsymbol{s}) = \log p(\boldsymbol{r},\boldsymbol{H}|\boldsymbol{s}) - \log p(\boldsymbol{H}|\boldsymbol{r},\boldsymbol{s}) \quad (28)$$

次に, 観測データ $\boldsymbol{u} = \boldsymbol{r}$ と透かし情報の推定値$\boldsymbol{w}=\hat{\boldsymbol{s}}$ から $\{\boldsymbol{r},\hat{\boldsymbol{s}}\}$ が与えられたもとでの $\boldsymbol{H}$ に関する条件付期待値をとる.

$$\begin{aligned} \log p(\boldsymbol{r}|\boldsymbol{s}) &= E[\log p(\boldsymbol{r},\boldsymbol{H}|\boldsymbol{s})|\boldsymbol{r},\hat{\boldsymbol{s}}] \\ &\quad - E[\log p(\boldsymbol{H}|\boldsymbol{r},\boldsymbol{s})|\boldsymbol{r},\hat{\boldsymbol{s}}] \end{aligned} \quad (29)$$

ここで, $L(\boldsymbol{s})$, $Q(\boldsymbol{s}|\hat{\boldsymbol{s}})$, および $R(\boldsymbol{s}|\hat{\boldsymbol{s}})$ をそれぞれ

$$L(\boldsymbol{s}) = \log p(\boldsymbol{r}|\boldsymbol{s}) \quad (30)$$

$$Q(\boldsymbol{s}|\hat{\boldsymbol{s}}) = E[\log p(\boldsymbol{r},\boldsymbol{H}|\boldsymbol{s})|\boldsymbol{r},\hat{\boldsymbol{s}}] \quad (31)$$

$$R(\boldsymbol{s}|\hat{\boldsymbol{s}}) = E[\log p(\boldsymbol{H}|\boldsymbol{r},\boldsymbol{s})|\boldsymbol{r},\hat{\boldsymbol{s}}] \quad (32)$$

で定義すると, 式 (29) は

$$L(\boldsymbol{s}) = Q(\boldsymbol{s}|\hat{\boldsymbol{s}}) - R(\boldsymbol{s}|\hat{\boldsymbol{s}}) \quad (33)$$

と書くことができる.

今, 我々が知りたいのは観測データ $\boldsymbol{r}$ に対する対数尤度 $L(\boldsymbol{s})$ を最大にする $\boldsymbol{s}$ であることに注意すると, Jensen

の不等式*3 より $R(\boldsymbol{s}|\hat{\boldsymbol{s}}) \leq R(\hat{\boldsymbol{s}}|\hat{\boldsymbol{s}})$ が成り立つので，$\boldsymbol{s}$ が $\{\boldsymbol{r}, \hat{\boldsymbol{s}}\}$ に対して $Q(\boldsymbol{s}|\hat{\boldsymbol{s}}) > Q(\hat{\boldsymbol{s}}|\hat{\boldsymbol{s}})$ を満たせば $L(\boldsymbol{s}) > L(\hat{\boldsymbol{s}})$ となり，$L(\boldsymbol{s})$ が増えることになる．この関係が EM アルゴリズムの基本であり，次の 2 つのステップからなるアルゴリズムが得られる．

(a) E–step

観測データ $\boldsymbol{u} = \boldsymbol{r}$ と現在の (時刻 k における) 透かし情報の推定値 $\boldsymbol{w} = \boldsymbol{s}^{(k)}$ から $\log p(\boldsymbol{r}, \boldsymbol{H}|\boldsymbol{s})$ の $\{\boldsymbol{r}, \boldsymbol{s}^{(k)}\}$ が与えられたもとでの $\boldsymbol{H}$ に関する条件付期待値

$$\begin{aligned} Q(\boldsymbol{s}|\boldsymbol{s}^{(k)}) &= E[\log p(\boldsymbol{r}, \boldsymbol{H}|\boldsymbol{s})|\boldsymbol{r}, \boldsymbol{s}^{(k)}] \\ &= \int_{\boldsymbol{H}} [\log p(\boldsymbol{r}, \boldsymbol{H}|\boldsymbol{s})] p(\boldsymbol{H}|\boldsymbol{r}, \boldsymbol{s}^{(k)}) d\boldsymbol{H} \quad (34) \end{aligned}$$

を計算する．

(b) M–step

E–step で得られた $Q(\boldsymbol{s}|\boldsymbol{s}^{(k)})$ を最大にする $\boldsymbol{s}$ を求め，これを $\boldsymbol{s}^{(k+1)}$ として $\boldsymbol{s}$ の値を更新する．

$$\boldsymbol{s}^{(k+1)} = \arg\max_{\boldsymbol{s}} Q(\boldsymbol{s}|\boldsymbol{s}^{(k)}) \quad (35)$$

これらの 2 つのステップを $\boldsymbol{s}$ が収束するまで繰り返す．

$\boldsymbol{s}$ を推定するためのアルゴリズムを具体的に与えるために，$\boldsymbol{r}$, $\boldsymbol{H}$, $\boldsymbol{s}$, $\boldsymbol{s}^{(\boldsymbol{k})}$ がガウス分布に従い，$\boldsymbol{H}$ と $\boldsymbol{s}$ は統計的に独立であると仮定して，式 (34) の計算をすると次式を得る．このとき，歪みモデル $\boldsymbol{H}$ の要素 h_{ij} の平均と共分散をそれぞれ $E[h_{ij}] = e_{ij}$, $E[(h_{ij} - e_{ij})(h_{kl} - e_{kl})] = \sigma_{ij}^2 (i = k$ かつ $j = l)$; $= 0$(それ以外) とし，$\boldsymbol{h_i} = [h_{ij}]$ (列ベクトル)，$\boldsymbol{e_i} = [e_{ij}]$ (列ベクトル)，$\boldsymbol{\Lambda_i} = E[(\boldsymbol{h_i} - \boldsymbol{e_i})(\boldsymbol{h_i} - \boldsymbol{e_i})^t]$ (対角行列) とおく．

$$\begin{aligned} Q(\boldsymbol{s}|\boldsymbol{s}^{(k)}) &\doteq -\sum_{l=1}^{N} r_l^2 + 2\boldsymbol{s}^t \left(\sum_{l=1}^{N} r_l \boldsymbol{d}_l^{(\boldsymbol{k})} \right) \\ &\quad - \boldsymbol{s}^t \left\{ \sum_{l=1}^{N} \left(\boldsymbol{d}_l^{(\boldsymbol{k})} \boldsymbol{d}_l^{(\boldsymbol{k})t} + \boldsymbol{\Delta_l}^{(k)} \right) \right\} \boldsymbol{s} \quad (36) \end{aligned}$$

ただし，

$$\boldsymbol{d_l}^{(k)} = E[\boldsymbol{h_l}|\boldsymbol{r}, \boldsymbol{s}^{(k)}] = \boldsymbol{\Delta_l}^{(k)} \left(\frac{r_l}{\sigma^2} \boldsymbol{s}^{(k)} + \boldsymbol{\Lambda_l}^{-1} \boldsymbol{e_l} \right) (37)$$

$$\boldsymbol{\Delta_l}^{(k)} = \left(\frac{1}{\sigma^2} \boldsymbol{s}^{(k)} \boldsymbol{s}^{(k)t} + \boldsymbol{\Lambda_l}^{-1} \right)^{-1} \quad (38)$$

式 (36) の導出については文献 [12][13] を参照されたい．

上記の $Q(\boldsymbol{s}|\boldsymbol{s}^{(k)})$ を最大にする $\boldsymbol{s}$ (これを $\boldsymbol{s}$ の更新値 $\boldsymbol{s}^{(k+1)}$ にする) は $\partial Q(\boldsymbol{s}|\boldsymbol{s}^{(k)}) / \partial \boldsymbol{s} = 0$ により求めることができる．従って，

$$\begin{aligned} \frac{\partial Q(\boldsymbol{s}|\boldsymbol{s}^{(k)})}{\partial \boldsymbol{s}} &= -2 \left\{ \sum_{l=1}^{N} \left(\boldsymbol{d}_l^{(\boldsymbol{k})} \boldsymbol{d}_l^{(\boldsymbol{k})t} + \boldsymbol{\Delta_l}^{(k)} \right) \right\} \boldsymbol{s} \\ &\quad + 2 \left(\sum_{l=1}^{N} r_l \boldsymbol{d}_l^{(\boldsymbol{k})} \right) \quad (39) \end{aligned}$$

*3 $\psi(x)$ を凸関数とする．$\psi(x)$ が可積分ならば $\psi(E[X]) \leq E[\psi(X)]$ が成り立つ．

より次の反復アルゴリズムを得る．

(1) σ^2, $\boldsymbol{e_l}$, $\boldsymbol{\Lambda_l}$ の値を設定する．$k = 0$ とし，$\boldsymbol{s} = \boldsymbol{s}^{(0)}$ と初期設定する．

(2) $\boldsymbol{\Delta_l}^{(k)}$, $\boldsymbol{d_l}^{(k)}$ を計算する．

$$\boldsymbol{\Delta_l}^{(k)} = \left(\frac{1}{\sigma^2} \boldsymbol{s}^{(k)} \boldsymbol{s}^{(k)t} + \boldsymbol{\Lambda_l}^{-1} \right)^{-1} \quad (40)$$

$$\begin{aligned} \boldsymbol{d_l}^{(k)} &= E[\boldsymbol{h_l}|\boldsymbol{r}, \boldsymbol{s}^{(k)}] \\ &= \boldsymbol{\Delta_l}^{(k)} \left(\frac{r_l}{\sigma^2} \boldsymbol{s}^{(k)} + \boldsymbol{\Lambda_l}^{-1} \boldsymbol{e_l} \right) \quad (41) \end{aligned}$$

(3) 次式により $\boldsymbol{s}$ の値を更新する．

$$\boldsymbol{D}^{(k)} = \sum_{l=1}^{N} \left(\boldsymbol{d}_l^{(\boldsymbol{k})} \boldsymbol{d}_l^{(\boldsymbol{k})t} + \boldsymbol{\Delta_l}^{(k)} \right) \quad (42)$$

$$\boldsymbol{s}^{(k+1)} = \left\{ \boldsymbol{D}^{(k)} \right\}^{-1} \left(\sum_{l=1}^{N} r_l \boldsymbol{d}_l^{(\boldsymbol{k})} \right) \quad (43)$$

(4) $k \to k+1$ として，$\boldsymbol{s}$ の値が収束するまでステップ (2), (3) を繰り返す．$\boldsymbol{s}$ の値が $\boldsymbol{s}^*$ に収束したら $g(\boldsymbol{s}^*)$ を埋め込まれていた透かし情報と判定する．ここで，$g(\cdot)$ はバイナリデータ ± 1 を判定するための適当なステップ関数である．

5. 電子透かし検出アルゴリズムの評価実験

電子透かしの耐性評価実験について簡単に記す．詳細については文献 [9][13] を参照されたい．

本研究では，離散ウェーブレット変換 (DWT) に基づく電子透かし方式を用いて画像処理に対する耐性評価実験を行い，提案手法の有効性を評価した．実験の諸元を以下に示す．

【テスト画像】LENNA（256 × 256 画素，8 bit ／画素）（図 2）

【ウェーブレット変換 (周波数変換) 】Daubechies 型（8 タップ）フィルタバンク，分解段数 3（サブバンド数 10）

【透かし埋め込み領域】サブバンド LH3，HL3（図 3）

【透かし埋め込み方法】量子化制御法：絶対値の小さなウェーブレット係数を N 個選び，透かし情報に応じて $\pm Q$ に量子化する．

【埋め込み強度】$Q = 10$

【透かし埋め込み情報量】$N = 25$ bit

【透かし入り画像の品質】$PSNR = 53.7$ dB

テスト画像 LENNA（図 2）を 3 階層にウェーブレット分解し，多重解像度表現成分 HL3 と LH3 のウェーブレット係数（図 3）に透かし情報を埋め込む．透かし情報は 4 ビットの情報ビットと 1 ビットの検査ビットからなる 5 ビットの系列とする．従って，この透かし系列は 16 パターン存在する．電子透かしの埋め込みでは，5 ビッ

表 1 評価実験の結果：透かし入り画像に対する画像処理と画像処理後の画質，透かし情報の検出率 (a) 検出補正なし（従来手法）(b) 検出補正あり（提案手法）

画像処理	PSNR (dB)	透かしの検出率 (%)	
		(a)	(b)
平滑化	29.8	100	–
雑音付加	28.1	75	100
JPEG 圧縮	31.2	50	100
幾何学変換	25.7	0	99

トの透かし系列を 5 倍冗長し，25 ビットの系列としてウェーブレット係数に埋め込む．ウェーブレット係数は HL3 と LH3 の帯域から絶対値の小さな係数を 25 個選び，透かし情報に応じて± 10 に量子化する．このとき，透かし入り画像の画質 (PSNR) は 53.7[dB] である．透かし情報の検出では，画像処理を施された透かし入り画像から 25 個の透かし入り係数を抽出し，次の方法で処理をする．

(1) 25 個の透かし入り係数の符号を調べてバイナリデータを検出する．次に，これらを 5 個づつ区切り，多数決判定により 5 ビットの透かし系列を得る．パリティチェックにより誤りが検出されなければ“ 検出誤りなし ”と判定し，4 ビットの情報ビットを埋め込まれていた透かし情報とする．パリティチェックにより誤りが検出された場合はステップ **(2)** の処理を行う．

(2) 25 個の透かし入り係数を 5 個づつ区切り，透かし入り係数の平均値を求め，情報ビットに対応する 4 ビットを観測データとする．この観測データを用いて提案手法により透かし情報の推定を行う（電子透かし検出システムの補正を行う）．

本実験では画像処理として，平滑化，雑音付加，JPEG 圧縮，幾何学変換を用いた．平滑化，雑音付加，JPEG 圧縮に対する評価実験では，16 パターンの透かし情報の埋め込みと検出を行う．幾何学変換に対する評価実験では，電子透かし攻撃ツール StirMark の中の Random Distortion を用いた画像処理に対する耐性を評価する．Random Distortion という処理は画像をランダムに僅かに歪ませる画像処理である．透かし情報と画像の歪み具合を変えながら透かし情報の埋め込みと検出を行い，従来手法で検出誤りが生じる観測データを 100 パターン用意する．そして，100 パターンの観測データそれぞれについて，提案方式を用いて埋め込まれていた透かし情報を推定する．表 1 に評価実験の結果を示す．表 1 から提案方式を用いることにより非常に高い確率で歪んだ透かし系列から埋め込まれていた透かし情報を推定できることが確かめられた．

図 2 テスト画像 LENNA

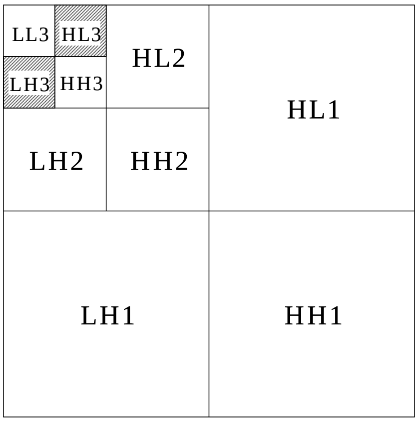

図 3 画像のウェーブレット分解 ($N = 3$) と帯域（サブバンド）成分

6. 通信・画像処理分野への適用について

本研究に関連して, 通信や画像処理の分野, 例えば, 伝送路の自動等化や画像復元の分野でもブラインドデコンボリューションの問題は現れる．

通信の分野では, 例えば, 歪んだ受信信号だけを用いて計算により送信信号を推定する問題などが挙げられる．送信信号を $w(n)$, 歪んだ受信信号を $u(n)$ とするとき, 歪みモデルがインパルス応答 $h(n)$ $(0 \leq n \leq L)$ をもった線形時不変システム, すなわち, $u(n)$ が $w(n)$ と $h(n)$ のたたみ込み演算

$$u(n) = \sum_{l=0}^{L} h(l)x(n-l) \quad (44)$$

によって表現あるいは近似できる場合, 上記のモデルは式 (8) のように行列で表すことができる．ここで, $\boldsymbol{H}$ は次式で与えられる．

$$\boldsymbol{H} = h(0)\boldsymbol{I} + h(1)\boldsymbol{D} + h(2)\boldsymbol{D}^2 + \cdots + h(L)\boldsymbol{D}^L \quad (45)$$

ただし, $\boldsymbol{I} = [\delta_{i,j}]$ (単位行列), $\boldsymbol{D} = [d_{i,j}] = [\delta_{i-1,j}]$, $\delta_{i,j} = 1$ $(i = j)$; $= 0$ $(i \neq j)$ (クロネッカーの記号)．これにより 4 章で述べたアルゴリズムが適用可能となる [14].

画像処理の分野では, 劣化した画像に含まれる情報のみから元の画像を復元する問題などが挙げられる．今, 元の画像を $w(m,n)$, 劣化した画像を $u(m,n)$ とするとき, 歪みモデルがインパルス応答 $h(m,n)$ $(-K \leq m \leq K,\ -L \leq n \leq L)$ をもった線形位置不変システム, すなわち, たたみ込み演算

$$u(m,n) = \sum_{k=-K}^{K} \sum_{l=-L}^{L} h(k,l)x(m-k,n-l) \quad (46)$$

によって表現あるいは近似できる場合も, 上記のモデルは式 (8) のような形に書くことができるので 4 章で述べたアルゴリズムが適用できる [14].

7. む　す　び

本稿では, 画像処理や攻撃を受けた透かし入り画像から透かし情報を検出する問題が一般にブラインドデコンボリューション問題になることを示し, 電子透かし検出問題を分類整理し, ベイズ推定に基づいた解法について議論した．そして, 透かし情報の歪みモデルが未知ではあるが, その平均などの統計的性質が既知である場合について, 電子透かし検出アルゴリズムを導いた．さらに, 数値実験によりこのアルゴリズムの有効性を検証した.

今後の課題としては，電子透かし歪みモデルの統計的性質の推定法ならびに EM アルゴリズムに基づく電子透かし検出手法におけるパラメータチューニングの問題などが挙げられる.

◇ 参　考　文　献 ◇

[1] 松井 甲子雄 "電子透かしの基礎–マルチメディアのニュープロテクト技術–, " 森北出版, p.235, 1998 年.

[2] G.C.Langelaar, I.Setyawan and R.L.Lagendijik "Watermarking Digital Image and Video Data," IEEE Signal Processing Magazine, Vol.17, No.5, pp.20–46, September 2000.

[3] I. J. Cox, M. L. Miller, and J. A. Bloom, DIGITAL WATERMARKING, p.542, Academic Press, 2002.

[4] M. Arnold, M. Schmucker, and S. D. Wolthusen, TECHNIQUES AND APPLICATIONS OF DIGITAL WATERMARKING AND CONTENT PROTECTION, p.274, Artech House, Inc., 2003.

[5] Akio MIYAZAKI, Akihiro OKAMOTO "Analysis of Watermarking Systems in the Frequency Domain and Its Application to Design of Robust Watermarking Systems," IEICE TRANS. FUNDAMENTALS, Vol.E85–A, No.1, pp.117–124, January 2002.

[6] Akio MIYAZAKI, "Digital Watermarking for Images – Its Analysis and Improvement Using Digital Signal Processing Technique–," IEICE TRANS. FUNDAMENTALS, Vol.E85–A, No.3, pp.582–590, March 2002.

[7] 宮崎明雄, "ベイズ推定に基づく電子透かしの検出," 電子情報通信学会技術研究報告 (スマートインフォメディアシステム), SIS2006-11, pp.61-66, 2006 年 6 月.

[8] 田中健一, 宮崎明雄, "ベイズの決定法に基づく電子透かしの検出," 電子情報通信学会技術研究報告 (ディジタル信号処理), DSP2003-161, pp.73-77, 2004 年 1 月.

[9] A. Miyazaki, "Improvement of Watermark Detection Process Based on Bayesian Estimation," Proc. of 2007 European Conference on Cuircuit Theory and Design (ECCTD2007), pp.408-411, Aug. 2007.

[10] G. J. McLachlan and T. Krishnan, THE EM ALGORITHM AND EXTENSIONS, p.274, John Wiley & Sons, Inc., 1997.

[11] 渡辺美智子, 山口和範 編著, EM アルゴリズムと不完全データの諸問題, p.259, 多賀出版, 2000 年.

[12] 宮崎明雄, "電子透かし検出問題のベイズ推定に基づく解法について," 電子情報通信学会技術研究報告 (信号処理), SIP2008-198, pp.191-196, 2009 年 3 月.

[13] Akio Miyazaki, "A Solution to the Watermark Detection Problem Based on Bayesian Estimation and EM Algorithm," Proc. of the 17th European Signal Processing Conference (EUSIPCO2009), VM5: Video Coding and Encryption (CD-ROM), pp.1789-1793, Aug. 2009.

[14] Akio Miyazaki, "A Sequence Estimation Method Based on EM Algorithm and Its Application to the Watermark Detection Problem," Proc. of 2009 Asia Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2009) (CD-ROM), pp.410-413, Oct. 2009.