統計的手法を用いた電子透かし情報の信頼性評価について*

3D−8

小川 宏　中村 高雄　富岡 淳樹　高嶋 洋一†
NTTヒューマンインタフェース研究所‡

1 はじめに

マルチメディア著作物の著作権保護に有効な手段として注目されている技術に電子透かしがある．この技術は，画像や音声などの冗長性を利用し，人間に知覚されないように情報コンテンツ (主情報) に別の情報 (透かし情報) を重畳するものである．著作権者や送信先の識別子を透かし情報とすることで，著作権情報の提示や証明，海賊版流出元の特定や不正複製の抑止といった効果が期待されている．一方，情報コンテンツの劣化に伴い埋め込んだ透かし信号も劣化するため，抽出された透かし情報の正当性の評価が重要である．本稿では，統計手法に基づく透かし情報の復元法を提案し，透かし情報の定量的評価について考察する．

2 透かし情報再構成法

電子透かし処理は，透かし埋め込み・透かし読みとりの対から成る．透かし埋め込み処理では，秘密鍵情報などを用いて，情報コンテンツ内の透かし対象領域 A から透かし埋め込み領域 $B(\subseteq A)$ を選定し，固有の規則でデータを変更する．透かし読みとりでは，透かし埋め込み領域 B のデータを解釈し，透かし情報を再構成する．本稿では，電子透かしアルゴリズムとして，透かしとして1ビットの情報 $b \in \{0,1\}$ を n 回繰り返し埋め込む (埋め込む系列を $b_0 b_1 \cdots b_{n-1}$ とする) ものについて議論する．また，繰り返し回数 n は統計的特徴を得るのに十分な数であるとする．

2.1 多数決による情報再構成法

透かし領域 B から読みとったビット情報 $\tilde{b}_0 \tilde{b}_1 \cdots \tilde{b}_{n-1}$ から透かし情報 $\tilde{b}$ を決定するのに多数決判定法を用いる．

$$\tilde{b} = \begin{cases} 0 & \sum_{k=0}^{n-1} \tilde{b}_k < \frac{n}{2} \text{ のとき} \\ 1 & \sum_{k=0}^{n-1} \tilde{b}_k > \frac{n}{2} \text{ のとき} \\ \text{不明} & \sum_{k=0}^{n-1} \tilde{b}_k = \frac{n}{2} \text{ のとき} \end{cases}$$

情報コンテンツの透かし対象領域における読みとりビットの0と1の出現確率に偏りがないと仮定すると，透かしが入っている情報コンテンツからの抽出においては，透かし情報が壊れていても，多数決によって正しい情報が再構成される可能性は高い．しかしながら単純な多数決手法では，仮定した条件の充足可能性が情報コンテンツに依存しているため，透かし情報の信頼性とその有無の判定に関して厳密な定量評価ができない．

2.2 統計モデルを用いた情報再構成法

電子透かしアルゴリズムを用いて，ある情報コンテンツの透かし対象領域 A から無作為に1ビット情報を読みとったときの $\{0,1\}$ の出現確率をそれぞれ $1-q$，q とする．透かし対象領域 A から任意の n ビット抽出を行なったとき，この系列にビット1が k 個現れる確率 $P(x=k)$ は，二項分布の密度関数

$$P(x=k) = \left(\begin{array}{c} n \\ k \end{array} \right) q^k \cdot (1-q)^{n-k}$$

で表され，その分布関数 $F(x)$ は，

$$F(x) = \sum_{k=0}^{x} \left(\begin{array}{c} n \\ k \end{array} \right) q^k \cdot (1-q)^{n-k} \quad (0 \le x \le n)$$

である．では，この情報コンテンツに透かしが入っていた場合を考える．多数決法と同様に，透かし埋め込み領域 B から読みとった系列 $\tilde{b}_0 \tilde{b}_1 \cdots \tilde{b}_{n-1}$ に含まれる1の個数 x を用いて透かし情報を再構成する．埋め込んだ透かしは n 個の0もしくは1の系列であるため，q が極端に0もしくは1に偏っていない限り，読みとった透かし系列は分布 $P(x)$ において確率的に稀な系列である．また，透かし情報が部分的に壊れていても，例えば図1の分布 $P1$ において $x = n_0$ は透かしが入っていると推測される．しかしながら，分布 $P2$ においては，統計的に透かしが入っていない確率が高い．これらを考慮して，信頼度の閾値 α $(\frac{1}{2} < \alpha \le 1)$ を設け，透かし情報を

$$\tilde{b} = \begin{cases} 0 & 0 \le F(x) \le 1-\alpha \text{ のとき} \\ 1 & \alpha \le F(x) \le 1 \text{ のとき} \\ \text{不明もしくは無し} & 1-\alpha < F(x) < \alpha \text{ のとき} \end{cases}$$

と分類する．すなわち，$0 \le F(x=x_0) \le 1-\alpha$ を満たす最小の x_0 と，$\alpha \le F(x=x_1) \le 1$ を満たす最大の x_1 を閾値として，図2のように透かし情報を判定する．α は，抽出した情報の正当率の下限を示す指標である．透かしが入っていない情報コンテンツを透かし有りと判定したり，透かしが入っている情報コンテンツから正しくない透かしを抽出する確率を $2(1-\alpha)$ で抑えることができる．

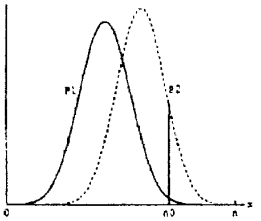

図1: 透かし密度関数

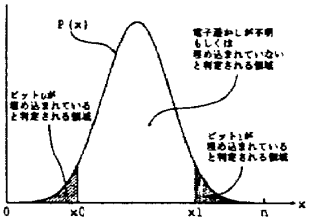

図2: 透かし情報分類

前記方式では，分布に偏りがない，すなわち，$q \simeq \frac{1}{2}$ となることを前提としている．しかしながら，q の値は電子透かしアルゴリズムと情報コンテンツに依存しているため，分布が偏る

*Reliability Evaluation of Digital Watermark Data using a Statistical Method

†Hiroshi Ogawa, Takao Nakamura, Atsuki Tomioka, Y-ouichi Takashima
‡NTT Human Interface Laboratories

可能性は十分ある．この問題を解消するために，疑似乱数系列を用いて埋め込み系列 $b_0b_1\cdots b_{n-1}$ を予め変調し，読みとり透かし系列を復調する処理を追加する．例えば，疑似乱数系列を $r_0r_1\cdots r_{n-1}$, $r_i \in \{0,1\}$ とおくと，排他的論理和を用いて埋め込み系列を $m_0m_1\cdots m_{n-1}$, $m_i = b_i \oplus r_i$ に変調する．復調は変調と同じ疑似乱数系列を用いて $\tilde{b}_i = m_i \oplus r_i$ により行なわれる．電子透かし情報読みとりには，正しい電子透かしの秘密鍵情報と疑似乱数系列の組が必要となる．疑似乱数系列として M 系列などを用いることで $q \simeq \frac{1}{2}$ となり，電子透かしアルゴリズムと情報コンテンツに依存することなく提案手法を適用可能である．読みとり透かし系列のビット 1 の出現確率は，変調の有無に関わらず二項分布に近似できると考えられるため，密度関数の分散に影響はない．また，秘密鍵情報と疑似乱数系列なしに q の偏りから透かしの有無並びにその値を検知することも困難になる．実装においては，$q = \frac{1}{2}$ と仮定することで，透かし情報再構成処理は多数決処理と同程度の計算量となり，高速化が図れる．

3　実験

参考文献[1]の電子透かしアルゴリズムに本提案手法を適用し，透かし情報抽出実験を行なった．実験対象画像として 128×128 画素の“lena”画像を用い，信頼度の閾値 α を 0.999999 として実験を行なった．

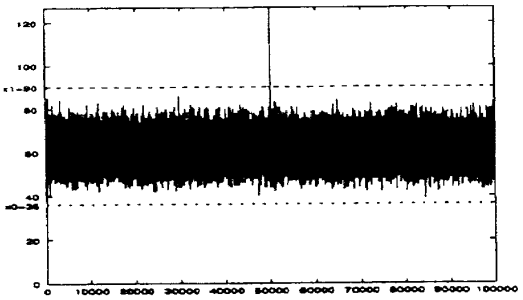

図 3: 透かし系列読みとり結果 (変調無し)

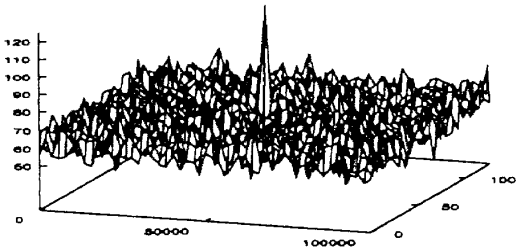

図 4: 透かし系列読みとり結果 (変調有り)

実験 1

1 ビットの透かし情報“1”を秘密鍵情報“50,000”を用いて 127 回繰り返し埋め込み，任意の秘密鍵情報を用いて透かし系列の読みとりを行なった．図 3 は，秘密鍵情報に対する読みとり透かし系列のビット 1 の個数を示したものである．縦軸は読みとった透かし系列におけるビット 1 の個数，横軸は秘密鍵情報の値を表している．ただし，透かし対象領域 A のビット 1 の出現頻度は $q = 0.492247$ であった．正しい秘密鍵 (50,000) を用いた場合，ビット 1 の個数が透かし有無の判定閾値 x_1 より大きいことから，正当率 99.9999%で透かし情報は 1 であると判定し，正しくない秘密鍵を用いた場合はすべて，透かし無しもしくは不明と判定した．

実験 2

7 段のシフトレジスタを用いた M 系列 (シフトレジスタの初期状態は 1000000) を用いて変調した透かし系列を埋め込み，任意の秘密鍵情報と初期状態が任意の M 系列を用いて実験 1 と同様の実験を行なった (図 4)．変調を行なうことにより，実験 1 のデータと比較して q の値は 0.500000 に，分散は 31.008265 から 31.718777 とほとんど変化しなかった．透かしが抽出できたのは，正しい秘密鍵情報と疑似乱数系列の組を用いたときのみであった．また，透かし対象領域 A の半分のデータに透かし系列を埋め込んだ場合，変調なしでは $q = 0.741547$ であったのに対し，変調を行なうことで $q = 0.499768$ という結果が得られた．

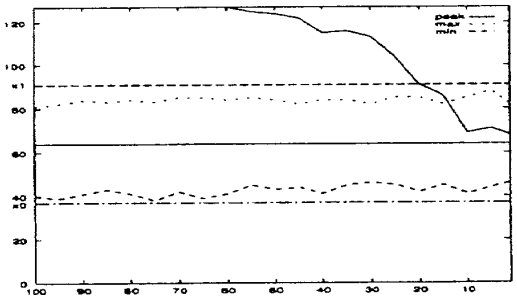

図 5: JPEG 圧縮と透かし系列の劣化の関係

実験 3

図 5 は，実験 2 の透かし入り画像 (SNR=50.211947) を様々な圧縮率で JPEG 符号化し，透かし系列を読みとったときのビット 1 の個数を示したグラフである．縦軸は透かし系列のビット 1 の個数，横軸は透かし画像の JPEG 圧縮率を表している．図中の peak は正しい秘密鍵情報と M 系列を用いたものであり，それ以外の場合については，最大値を max，最小値を min で示してある．参考文献[1]では，節 2.1 の多数決法を用いているため，圧縮率 1%の JPEG 符号化画像からも透かし読みとりが成功したと判定するが，正当率を 99.9999%とした場合は，圧縮率 20%までしか透かし情報の正当性を保証できない．正しくない秘密鍵情報もしくは正しくない M 系列を用いたとき，JPEG 圧縮の影響による透かし情報誤抽出はなかった．

4　おわりに

透かし情報を統計的に定量評価可能な方法を提案した．透かしの誤抽出を許した電子透かし性能の向上と透かし情報の正当率の精度のどちらを優先するかはアプリケーションに依存している．これより，電子透かしシステムは，従来のように透かし正当率を利用者に提示するより，その閾値を内部で定数として管理するのが理想である．本稿では透かし情報を 1 ビットとして論じたが，同様の議論で複数ビットに拡張が可能である．この場合，バースト誤りにより透かし情報の特定ビットのみを誤る可能性も考えられるが，誤り訂正符号と併用することでこれを防ぐことができると考える．

参考文献

[1] 中村，小川，高嶋，“画像の周波数領域処理による電子透かし”，1997 年電子情報通信学会総合大会，D-11-47