

タイトル	手書き署名をフリー空間に埋め込む電子透かし法
著者	高井, 信勝
引用	北海学園大学工学部研究報告, 33: 97-111
発行日	2006-02-20

手書き署名をフーリエ空間に埋め込む電子透かし法

高井 信勝*

Digital Watermarking of Handwritten Images Embedded in the Fourier Space

Nobukatsu TAKAI*

Abstract

We present a watermarking technique by which a watermark image consisting of handwritten signature is hidden in the Fourier space. First, we investigate theoretically the conditions under which the original image is scarcely damaged and at the same time the watermark image can be recovered. According to the theoretical results, several experiments are conducted and the effects of the size of the watermark image and its embedding position in the Fourier space are made clear. Furthermore, the robustness of the presented watermarking method is also revealed with respect to removing the low-bit-planes and cutting out of images which contain the watermark.

1. はじめに

小切手・手形・証券では裏面に裏書きすることでその有効性が証明される。また、紙幣では、表と裏の図柄が一体となってその真正性が確認できる。このような有価証券に限らず、文書等の所有権を主張するために、それらの裏面に署名、印影、指紋などを入れることが、日常的に用いられ、社会に深く根ざしている。

ここでは、現実の社会で用いられている裏書きに似せた表現技法を、インターネット配信におけるデジタル画像というコンテンツに対して適用する手法を研究した。もちろんデジタルコンテンツに表と裏があるわけではないが、それらに対応するものとしてすぐに思いつくのは、フーリエ変換の実空間と周波数空間である。このフーリエ変換対の両者の関係は、「情報」という意味では等価であり、表と裏に異なる情報を持つものではない。しかし、画像自身

* 北海学園大学工学部電子情報工学科

* Department of Electronics and Information Engineering, Faculty of Engineering, Hokkai-Gakuen University

を表とし、それをフーリエ変換して得られるフーリエスペクトル分布を裏面として、裏面に表面の画像の何らかの属性を書き込むことによって裏書きに相当する機能を持たせることができる。この手法は、いわゆる周波数領域に透かし情報を埋め込む電子透かし技術¹⁻⁶⁾であり、近年、デジタルコンテンツの不正使用防止技術として広く注目されている。

ところが、透かし情報を周波数領域に埋め込むと、スペクトル分布自体が変化するので、その逆フーリエ変換として得られる画像は原画像とはどのようにしても厳密に一致しない。この不一致は、どのような電子透かし技術であっても避けられない問題であって、「透かしが埋め込まれたことによって、コンテンツ画像が変化しても、視覚的にはその変化が見分けられない」ことが電子透かし技術に要求されている。

本稿では、人の顔画像を原画像として、そのフーリエ空間に手書き文字の透かし画像を埋め込む電子透かし法を報告する。フーリエ空間に電子透かし画像を埋め込む方法として、フーリエスペクトル分布に透かし画像を加える「和の埋め込み」と、それに掛け合わせる「積の埋め込み」が考えられる。ここでは、まず、どちらの埋め込み方法が電子透かし技術として妥当であるかを考察し、結論として、後者の方法が適していることを示す。そのあとで、積の埋め込み方法のもとで、原画像に与える埋め込み画像の大きさの影響、埋め込み位置の影響、ビットプレーン除去の影響、および画像の切り取りの影響を報告する。

原画像と裏書きされた画像の差違は、両方の画像の対応する全画素にわたる画素値の差の標準偏差によって評価した。この標準偏差が、電子透かし技術でどこまで許されるかについては、明確な定義はない。ただ、汎用な画像データの各画素の値は8ビットデータであって、通常、下位2ビットの値が変化してもその変化は視覚的には感じられない。ここでは、原画像と透かしを含んだ画像との差、つまり原画像に対する誤差の標準偏差を評価し、最悪でも下位2ビットまで許容できるものとして議論を行った。

2. 透かし画像埋め込みの要件

画像データに限らず、2次元信号 $g(x,y)$ とそのフーリエスペクトル $G(\xi,\eta)$ のあいだには、つぎのフーリエ変換対が成り立つ。

$$G(\xi,\eta) = \iint g(x,y) \exp[-2\pi i(x\xi + y\eta)] dx dy \quad (1)$$

$$g(x,y) = \iint G(\xi,\eta) \exp[2\pi i(x\xi + y\eta)] d\xi d\eta \quad (2)$$

ここで、積分範囲 $[-\infty, \infty]$ の記述は省略してある（以下においても、同様に記述する）。

本研究における電子透かし技術では、図1に示すように、原画像を $g(x,y)$ とし、この周波数

領域に透かしの情報（画像）を埋め込む。つまり、透かしを埋め込むことによって、フーリエスペクトル $G(\xi, \eta)$ は、

$$G(\xi, \eta) \rightarrow G_e(\xi, \eta) \quad (3)$$

と置き換えられる。この結果、当然のことであるが、逆フーリエ変換から得られる透かし情報を含んだ出力画像は、 $g(x, y)$ そのものではなく、

$$g_e(x, y) = \iint G_e(\xi, \eta) \exp[2\pi i(x\xi + y\eta)] d\xi d\eta \quad (4)$$

である。

周波数領域に透かし情報を埋め込む電子透かし技術では、式(4)の出力画像 $g_e(x, y)$ に対してつぎの2つの要件が必要になる。

〈要件1〉画像データが一般のデータと異なる点は、非負の実数データであることである。つまり、入力画像 $g(x, y)$ と同様に、出力画像 $g_e(x, y)$ は

$$g_e(x, y) = |g_e(x, y)| \quad (5)$$

でなければならない。したがって、透かしの埋め込み、つまり式(3)の置き換えは、結果の $g_e(x, y)$ が非負の実数データになるように制限される。

〈要件2〉電子透かしに要求されるもう一つの要件は、入力画像 $g(x, y)$ と出力画像 $g_e(x, y)$ が視覚的には区別が付かない程度に、両者の差 $g(x, y) - g_e(x, y)$ を極力小さくすることである。以下では、この画像差を標準偏差

$$SD = \sqrt{\langle [g(x, y) - g_e(x, y)]^2 \rangle} \quad (6)$$

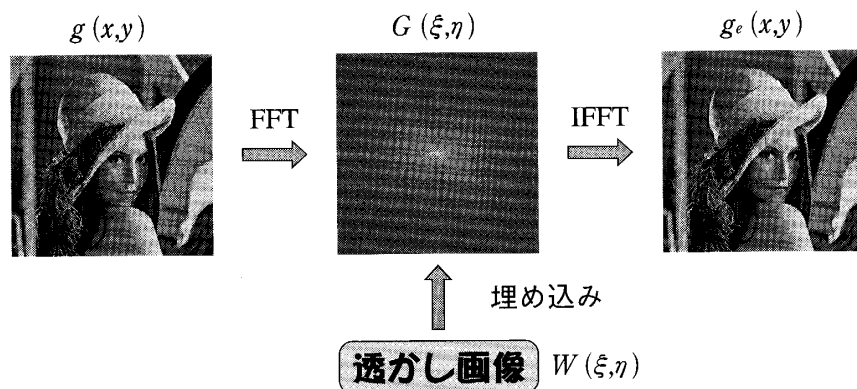


図1 原画像 $g(x, y)$ のフーリエスペクトル $G(\xi, \eta)$ に透かしデータ $W(\xi, \eta)$ を埋め込み、出力画像 $g_e(x, y)$ をえる。

によって定量的に評価する．ここで、 $\langle \dots \rangle$ は全画素にわたる平均（空間平均）を意味している．

なお、フーリエスペクトル $G(\xi, \eta)$ は、一般に複素数値である．したがって、これをそのまま画像として表示することはできない．また、上述したように $g(x, y)$ が非負の実数値であるので、ゼロ周波数に

$$G_0 = \int g(x, y) dx dy \quad (7)$$

の値をもつ大きなピークが現れ、これが周波数領域のスペクトル分布全体を明示する際に障害になる．そこで、以下ではスペクトル分布は、便宜的に、 $G(\xi, \eta)$ の絶対値 $|G(\xi, \eta)|$ の対数値で表示する．

3. 電子透かしの埋め込みと検出方法

本研究では、図2に見られるように、透かし画像の一例として手書き文字「麗奈」を用いた．しかし、これは、なにも手書き文字に限られるものではなく、指紋や印影のような2値画像であれば本手法は同様に適用できる．このような2値画像を周波数領域に埋め込む方法として、図2に示す和の埋め込みと積の埋め込みがある．

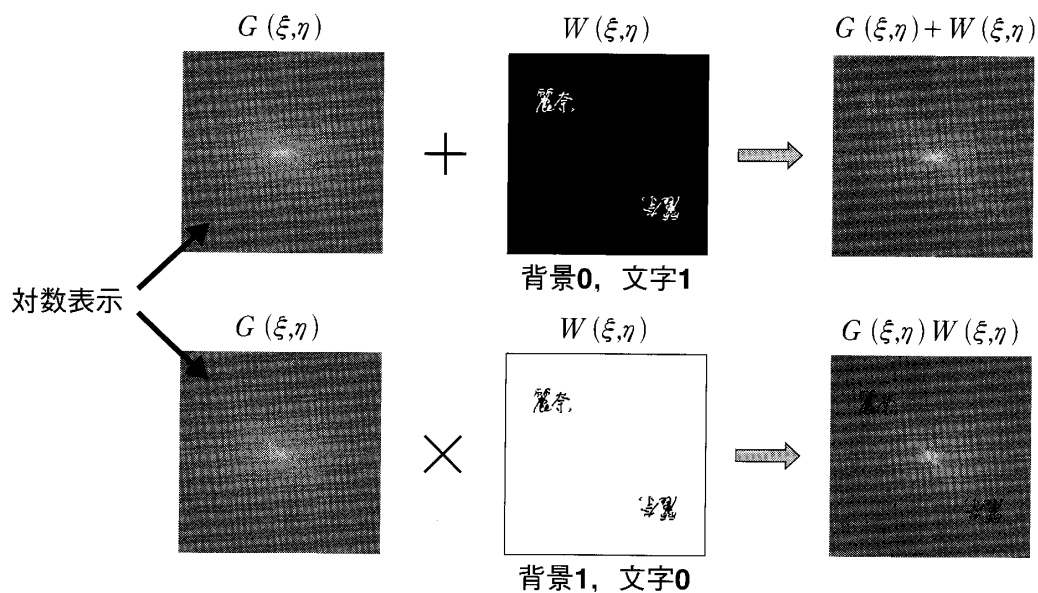


図2 和の埋め込み（上）と積の埋め込み（下）

3.1 和で埋め込む方法

この方法では、透かし画像を

$$W(\xi, \eta) = \begin{cases} 1 & (\text{文字の部分}) \\ 0 & (\text{上記以外}) \end{cases} \quad (8)$$

として、画像のスペクトル分布 $G(\xi, \eta)$ に加える。つまり、

$$G_e(\xi, \eta) = G(\xi, \eta) + W(\xi, \eta) \quad (9)$$

とすることで透かしを埋め込む。このようにすると、文字以外の部分のスペクトルは変化を受けずに透かしが埋め込まれる。この結果、式(4)の出力画像は

$$g_e(x, y) = g(x, y) + w(x, y) \quad (10)$$

となる。ここで、 $w(x, y)$ は透かし画像のフーリエ変換で

$$w(x, y) = \iint W(\xi, \eta) \exp[2\pi i(x\xi + y\eta)] d\xi d\eta \quad (11)$$

で与えられる。

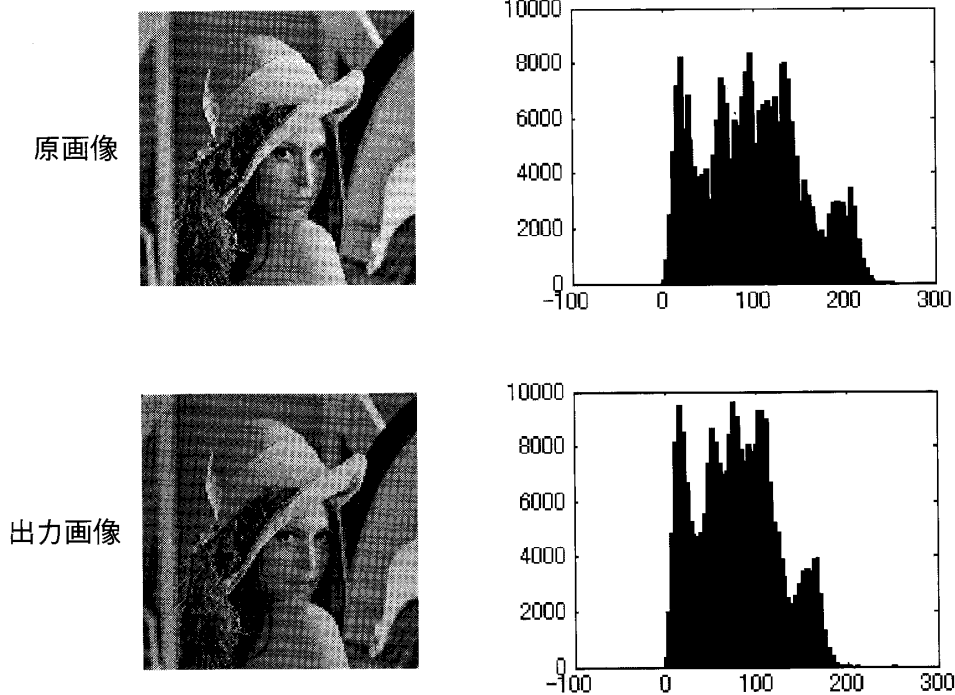


図3 和の埋め込みにおける入力画像と出力画像およびヒストグラムの比較

この場合、埋め込みの〈要件1〉が満たされるためには、式(9)が実数の非負の値でなければならない。このことは、式(10)の第2項の $w(x, y)$ が実数、すなわち $w^*(x, y) = w(x, y)$ (*は

複素共役) でなければならず, これを式(11)に用いると, 埋め込む透かし画像 $W(\xi, \eta)$ は,

$$W(\xi, \eta) = W(-\xi, -\eta) \quad (12)$$

を満足しなければならない. したがって, <要件1> が満たされるためには, 透かし画像は, 図2に示すような原点の周りで対称に配置したものでなければならないことになる.

和の埋め込みの実行例を図3に示す. ここで, 画像サイズは 512×512 で, 画像の強度値は, $[0, 255]$ の範囲に規格化されている. ここにみられるように, 肉眼で見る限りは, 原画像と出力画像 (透かしを含んだ画像) とは同一のように見えるが, 同時に示す画像の強度分布のヒストグラム分布は, 強度値がおよそ200を超える領域で大きく異なっている. この違いは, 透かし画像のフーリエ変換が和の形で加わったことによるものである. つまり, 透かし画像のフーリエ変換が原画像の強度分布に重畳することによって, それによる少数の分布が200を超えるヒストグラム領域に現れ, 同時に原画像のヒストグラム分布がおよそ $0 \sim 200$ の範囲に制限される結果である. そして, ヒストグラムのこのような相違は, 視覚的には, 原画像と比べて, 出力画像の全体の明るさが低下した, 暗い画像として観察される.

結果として, 和の形で透かし画像を埋め込む手法の出力画像は, 定量的な意味で原画像と大きく異なっており, 電子透かしの <要件2> を満足しない. なぜなら, その要件を満足するためには, 式(10)の第2項 $w(x, y)$ を極力小さくしなければならず, そうすることは透かし情報を喪失することにはほかならないからである.

3.2 積で埋め込む方法

透かし画像を積の形で埋め込むときには, 図2(下図)にみられるように, 式(8)と相補的な画像信号

$$W(\xi, \eta) = \begin{cases} 0 & (\text{文字の部分}) \\ 1 & (\text{上記以外}) \end{cases} \quad (13)$$

を用いる. つまり, 背景を1とし, 文字の部分を0としたもので, こうすることで原画像のスペクトル分布 $G(\xi, \eta)$ は, 文字以外の部分では透かし画像の影響を受けない. この場合, 式(4)の出力画像は

$$g_e(x, y) = \iint W(\xi, \eta) G(\xi, \eta) \exp[2\pi i(x\xi + y\eta)] d\xi d\eta \quad (14)$$

で与えられ, たたみ込み積分定理を用いると, 原画像 $g(x, y)$ と透かし画像のフーリエ変換 $w(x, y)$ のたたみ込み積分

$$g_e(x, y) = \iint g(s, t) w(s - x, t - y) ds dt \quad (15)$$

が得られる。

この結果を電子透かしの〈要件1〉で考えると、2.1節の「和の埋め込み方法」で述べたと同様に、 $w(x,y)$ が実数、したがって $W(\xi,\eta)=W(-\xi,-\eta)$ を満足するように透かし画像は原点の周りで対称でなくてはならない。一方〈要件2〉からは、すぐわかるように、

$$w(x,y) \approx \delta(x,y) \quad (16)$$

であることが要求される。つまり、 $w(x,y)$ が δ 関数に近いほど原画像と出力画像の差は小さいことになる。幸い、透かし文字を図2にあるように周波数領域の片隅（つまり、高周波数領域）に配置すると、 $W(\xi,\eta)$ の大部分は1の値であるので、そのフーリエ変換である $w(x,y)$ はよい近似で式(16)に従い、その結果、原画像に近い出力画像を得ることができる。

図4に、この場合の原画像と出力画像をそれらの強度値のヒストグラム分布とともに比較して示す。画像サイズは 512×512 で、強度値は $[0, 255]$ の範囲に規格化されてある。この結果の画像はよく類似しており、ヒストグラム分布も強度値の全域にわたってよく一致していることが認められる。言い換えると、周波数領域で透かし画像を積の形で埋め込む方法は、電子透かしの2つの要件をよく満足することがわかる。

なお、手書き文字の透かしにおける式(16)の妥当性は、後述するように、文字サイズを変えたときの影響の議論においてより詳細に示す。また、原画像と出力画像の差の定量的な評価は、引き続き具体的な実行例において与えられる。

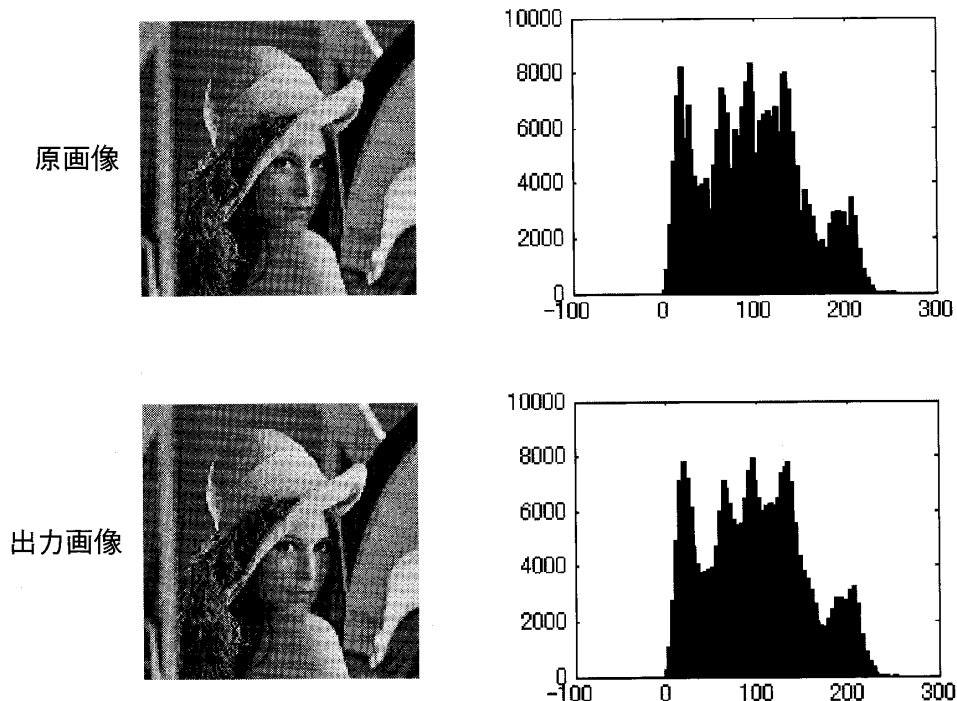


図4 積の埋め込みにおける入力画像と出力画像およびヒストグラムの比較

3.3 電子透かしの検出方法

ここまで周波数領域に透かし画像を埋め込む手法を検討し、原画像のスペクトル分布に透かし画像を積の形で埋め込む方法が適することを明らかにした。ここで、まず、この場合の手法の全体像を図5に示しておく。

この図において処理手順を説明すると、以下のようになる。まず、原画像 $g(x,y)$ のフーリエスペクトル $G(\xi,\eta)$ をFFT演算を用いてもとめる。 $G(\xi,\eta)$ は一般に複素量であるが、視覚的に表示するために図5ではその絶対値の対数値を示してある。そして、この全体に透かし画像 $W(\xi,\eta)$ を乗じる。このとき、 $W(\xi,\eta)$ は図5にあるように、透かし画像を中心対称の配置にしたものを用いる。つぎに、結果の $W(\xi,\eta)G(\xi,\eta)$ に逆フーリエ変換演算(IFFT)を施し、出力画像 $g_e(x,y)$ を得る。

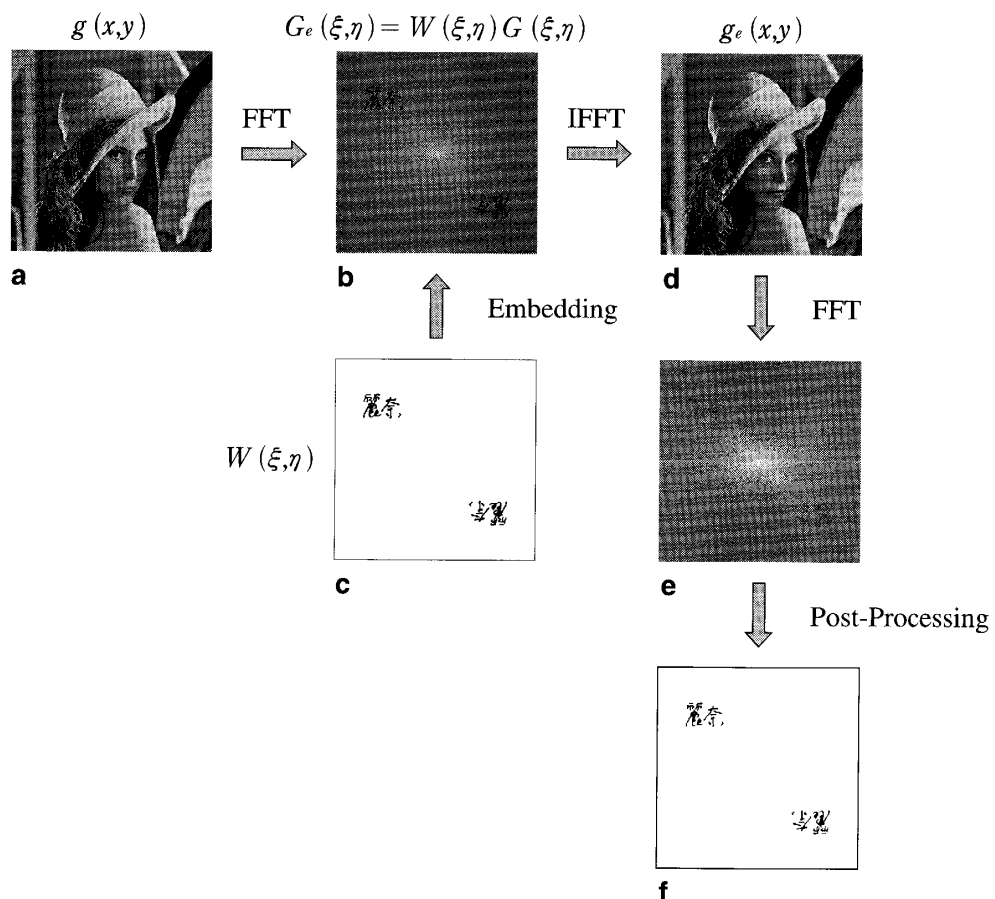


図5 積の埋め込みと透かし情報の検出

出力画像 $g_e(x,y)$ をもう一度フーリエ変換すると、スペクトル $G(\xi,\eta)$ に重なった透かし画像をみることができる(図6(e))。このように、本手法の電子透かしは逆フーリエ変換の演算で簡単にみることができる。したがって、この意味で本手法は「可視型の電子透かし法」であ

る。透かし画像データだけを抽出するには図6 (b)に示すようなマスクをかける。このマスクは、あらかじめ知られている透かしが存在する位置に合わせて作成する。しかし、このようなマスクングによって得られる透かし画像は原画像データのスペクトル成分と比べてパワーが格段に小さいために雑音を含んだ画像として得られるのが常である。この雑音を除去するためにメディアンフィルタリングを施すことによって良質の透かし画像を検出できる。



図6 透かし情報の検出過程

4. 定量的な検討

ここでは、「積の埋め込みによる電子透かし法」において、式(6)で与えられる原画像と出力画像の差の標準偏差を評価パラメータとするいくつかの実験を行い、本手法の特性を定量的に調べた。調査項目は、透かし画像の大きさの影響、透かし画像を埋め込む位置の影響、ビットプレーン除去に対する耐性、および画像の切り取りに関する耐性である。

4.1 透かし画像サイズの影響

図7に、文字サイズを変えたときの透かし画像 $W(\xi, \eta)$ とその逆フーリエ変換 $w(x, y)$ を視覚的に示す。ここで、文字サイズは、文字を方形領域で囲った面積とし、それを全領域 512×512 で規格化した値で評価した。すなわち、図7では、文字領域が全領域に対して (a) 1.09%, (b) 2.97%, (c) 5.79%である。これらに対する右列の $w(x, y)$ は、いずれも中心(原点)に δ 関数状の鋭いピークからなっていて、文字サイズが大きくなるにつれて中心ピークの周りに不規則な分布のスペクトルが現れる。このことは、文字サイズが小さいほど $w(x, y)$ は δ 関数に近く、つまり式(16)の近似がよく、出力画像と原画像の差が小さくなることを示している。

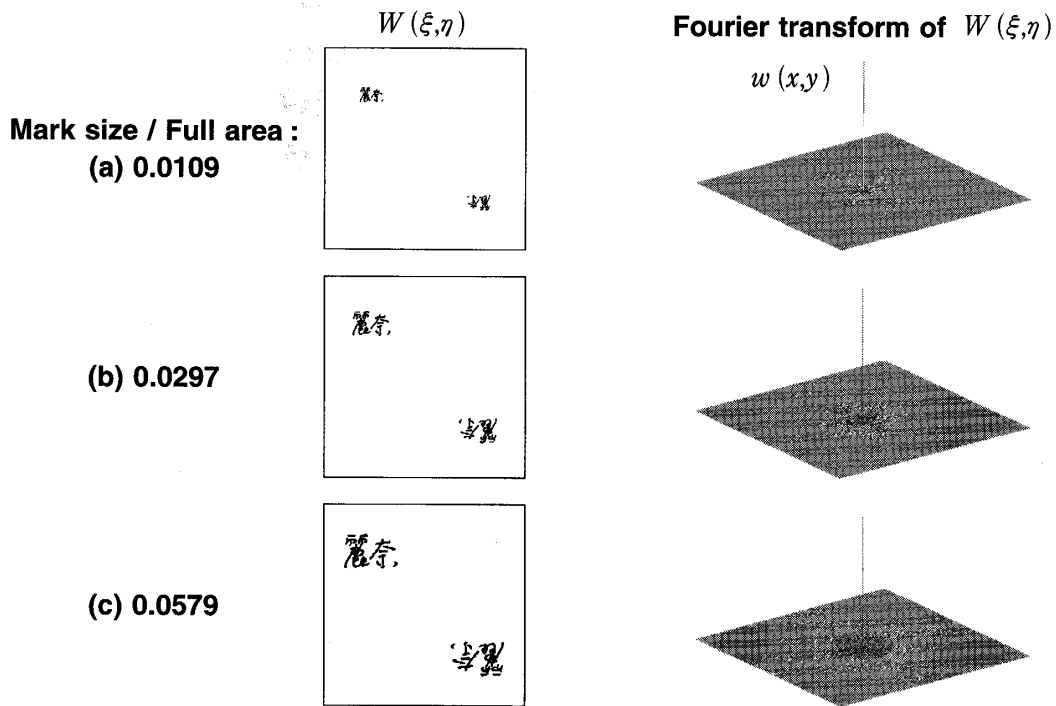


図7 透かし文字のサイズを変えたときの透かし画像(左)と各々のフーリエ変換 $w(x,y)$ (右).

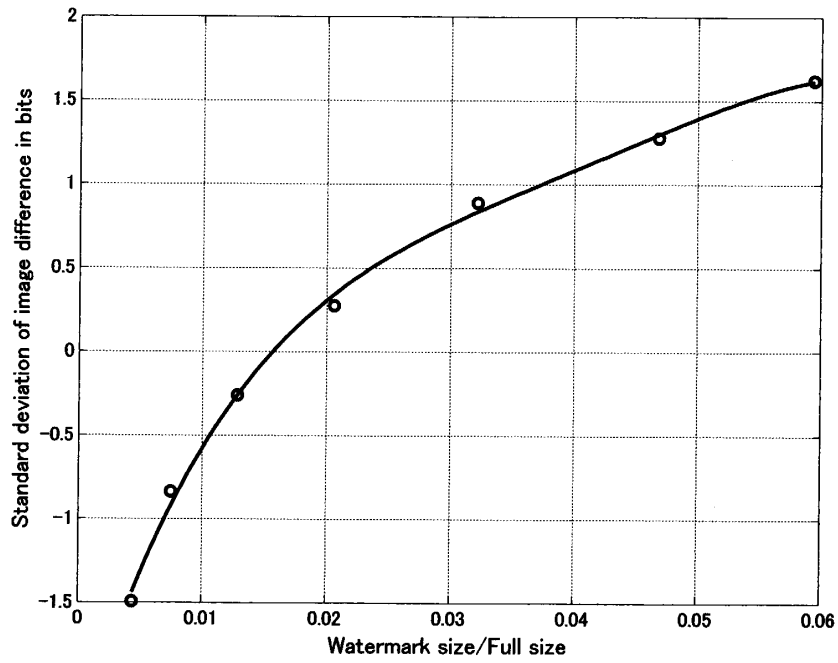


図8 透かし文字サイズ領域の関数として得られた出力画像と原画像の差の標準偏差値 (式(6)).

図8は、文字サイズ領域の大きさを変化させて、出力画像と原画像の差の標準偏差 (式(6))

の SD)を測定した結果である。図7における $w(x,y)$ の振る舞いに呼応して、標準偏差 SD は文字サイズ領域に対して単調に増大するが、文字サイズ領域が4%程度以下であれば、その差はおよそ1ビット以下、1.5%以下であれば0ビット以下である。つまり、両方の画像とも強度値は8ビットデータで、そのダイナミックレンジは0~255であるのに対して、両者の差は小さく、図8に示す範囲では、標準偏差はビット値で1.58以下、十進数でおよそ0~3程度である。

4.2 透かし画像の埋め込み位置の影響

透かし画像の文字の中心位置を周波数領域のその位置とすると、出力画像は、透かし画像を埋め込む位置の影響も受ける。周波数領域の各点は中心(原点)をゼロ周波数とする空間周波数に相当する。つまり、原点からの距離が空間周波数値であり、基本周波数を f_0 とすると、原点から n ピクセル離れた点は nf_0 の周波数にあたる。

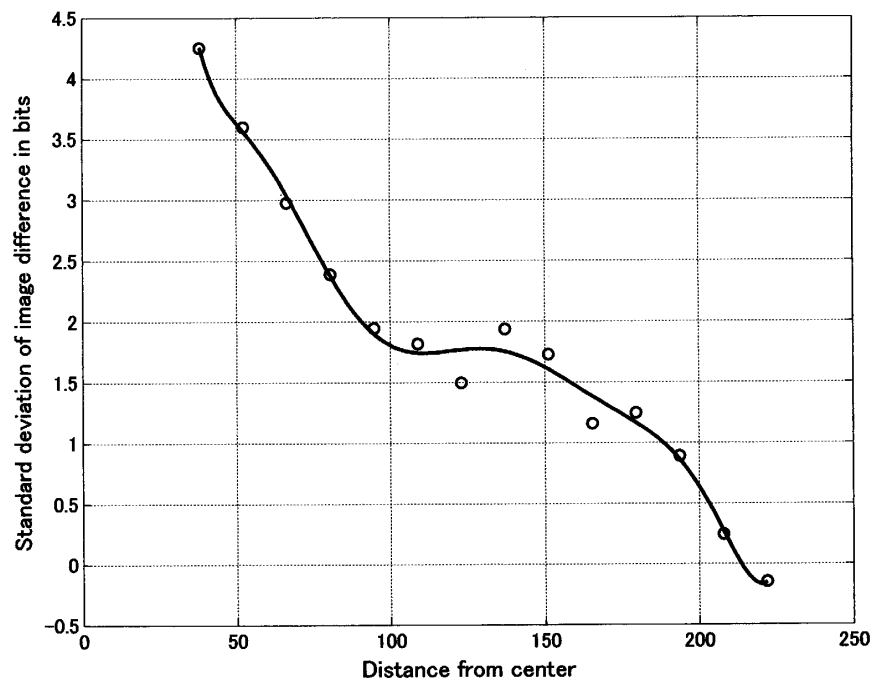


図9 原点から透かし文字の中心位置までの距離(横軸)の関数としての原画像と出力画像の差の標準偏差値(縦軸)。およそ180ピクセル以上離れた高周波数領域に透かし文字を配置すると、画像差の標準偏差は1ビット以下になる。

ここでは、図7(b)の透かし文字を原点からの距離を変えて配置し、出力画像を調べた。図9は、出力画像と原画像の差の標準偏差を、原点からの距離(ピクセル数)の関数として求めた結果である。この振る舞いは、透かし文字が原点から遠ざかるにつれて、差の標準偏差値が小さくなっている。すなわち、透かし文字を原点から離れた高周波数領域に配置するほど出力

画像は原画像に近いものとなる。この理由は、多くの画像では原画像のスペクトルが低周波数領域に支配的に存在するからで、そのため透かし画像を低周波数領域に配置すると、原画像のスペクトルが透かし画像によって強く影響を受けるからである。このことを反映にして、図9では、差の標準偏差は原点からの位置がおおよそ100ピクセルまでは急激に減少し、それ以上ではその減少はいったん緩やかになり、おおよそ180ピクセル以上になると、画像差の標準偏差値は1ビット以下の値まで小さくなることが読みとれる。

4.3 ビットプレーン除去に対する耐性

電子透かしを埋め込んだ画像に要求される耐性のひとつにロービットプレーン除去に対する耐性がある。汎用的な通常の画像の各ピクセルデータは8ビットデータで、その最下位ビットが除去されたり、書き換えられても視覚的にはその影響は知覚できないのがふつうである。言い換えると、最下位ビットプレーンの除去によって電子透かしが消えるような埋め込みでは、本来の電子透かしの意味をなさない。同様なことが、もっと高位のビットプレーンに対しても言うことができるが、高位ビットプレーンを除去したり、書き換えたりすると、もとの画像自体が大きな影響を受ける。このように、電子透かし技術では、下位ビットプレーンに対する攻撃に対して透かし情報が消去されない強さを持つことが要求されている。

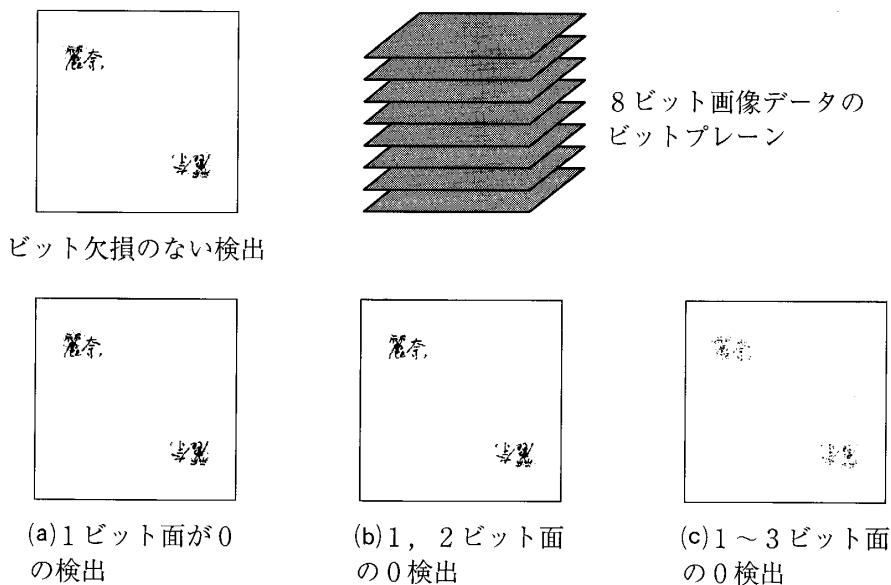


図10 ロービットプレーンを除去した出力画像から検出された透かし画像。

図10に、出力画像の下位ビットプレーンのデータをすべてゼロに置き換えた画像から検出された透かし画像を示す。図10(a) および(b) は、それぞれ、出力画像の1ビット面（最下位ビ

ット面)と1および2ビット面の両面の値をすべてゼロにした画像から検出された透かし画像で、これらからは明確に透かし文字が検出できる。図10(c)は、1～3ビット面のすべての値をゼロにした出力画像から検出された透かし画像で、この場合でも文字の存在は認められるが、検出された透かし文字のSN比はかなり劣化した結果になっている。

なお、この場合の原画像と出力画像の差の標準偏差 SD はいずれも小さく、ビット面除去がない場合の値 $SD = -0.070bits$ に対して、図10(a), (b), (c)の場合の標準偏差は、それぞれ、(a) $0.104bits$, (b) $0.55bits$, (c) $1.31bits$ であった。この結果は、ビットプレーン除去によって、原画像と出力画像の差が大きくなることを示しているが、視覚的に容易に認められるほどのものではない。

4.4 画像切り取りに対する耐性

電子透かし技術では、また、画像の部分使用に対して透かし情報が保持されることも要求される。ここでは、画像を切りとって使用した場合の電子透かしの耐性を調べた。

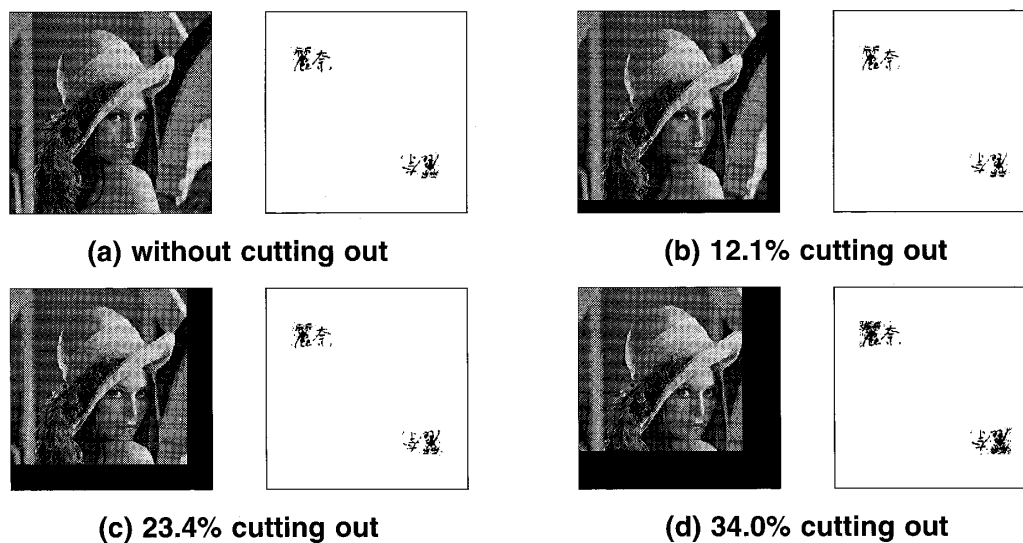


図11 切り取られた画像とその各からの検出透かし画像

図11がその結果である。この図で、画像の右側と下側の黒の帯状の部分が切り落とした部分で、(a)が切り取りがない場合、(b), (c), (d)が切り落とした部分の面積が、それぞれ、全体の12.1%, 23.4%, 34.0%の場合ある。これにみられるように、切り取り面積が増大するにつれて検出される電子透かしの画質は劣化する。しかし、ほぼ30%の切り取りの場合でも透かし文字を読み取ることは十分にできる。これは、透かし画像の情報が周波数領域に埋め込まれ、その結果の出力画像の全面にその情報が分散して存在するために、部分的な欠損に対して

ある程度の耐性を持つからである。

5. おわりに

本研究では、画像のフーリエ空間にその属性を示す手書き画像を埋め込む電子透かし手法を研究した。ここでは、まず画像データの特質と透かし画像を埋め込んだ結果の画像の損傷を考慮して、埋め込み条件を理論的に明らかにした。その手法の要件はつぎの三点である。

- 1) 透かし画像をフーリエ空間の原点に対称に配置する
- 2) 1) のように配置した透かし画像のフーリエ変換が良い近似で δ 関数的であること
- 3) 1), 2) を満たす透かし画像を、原画像のフーリエスペクトルに積の形で埋め込む

以上の要件を満たす手法によって実験を行い、透かしを埋め込んだ画像を種々の影響下で定量的に評価するとともに、それから検出される透かし画像を評価した。このとき、透かしを含んだ画像の評価は、それと原画像の差の標準偏差を用い、透かし画像をフーリエ空間の高周波数領域に埋め込むことによって、その差は統計的な意味において1ビット以下になることを示した。たとえば、透かしのサイズがフルサイズの約4%以下であれば、画像差は標準偏差値で1ビット以下であり、埋め込み距離が、基本周波数の200倍の位置（現実には、原点から200ピクセル離れた位置）であれば、やはり1ビット以下になる結果が得られた。

さらに、電子透かし技術の観点から、透かしを埋め込んだ画像のビットプレーン除去、あるいは書き換えに関する耐性を調べる実験を行い、下位ビットの1～2ビット面のデータ欠損の影響は極めて小さいことを示した。また、透かしを埋め込んだ画像の一部が利用する攻撃に対してもある程度の耐性があり、全領域の30%程度の切り取りであれば、透かしは検出できることを示した。なお、ここで行った電子透かし技術は、画像の中に直接みられるものではないが、透かしはフーリエ変換を施すと容易にみることができ。この意味で、いまの段階では、本手法は可視型の電子透かしといえる。したがって、暗号技術⁷⁻¹⁰⁾を組み込んで、透かしを暗号化して埋め込むことによって本格的な電子透かし技術になるが、これは今後の課題として残されている。

本研究は、北海学園大学ハイテクリサーチセンター事業の研究プロジェクト「視覚・画像・音声・言語情報処理の高度化と知的計測制御技術への応用」の一環として行った。

【参考文献】

- 1) 高井 信勝, 三船 雄都, 成田 貴文: デジタルホログラフィを用いる電子透かし法, 北海学園大学工学

- 部研究報告, 第28号, pp.261-275 (2001).
- 2) 高井 信勝:「MATLAB入門」, (工学社, 2000).
 - 3) N.Takai and Y.Mifune: Digital watermarking by a holographic technique, *Applied Optics*, Vol. 41, No. 5, 865-873 (2002).
 - 4) E. Ganic, D. Dexter Scott and M. Eskicioglu Ahmet: Embedding multiple watermarking in the DFT domain using low and high frequency bands, *Proc SPIE Int Soc Opt Eng*, Vol. 5681, pp. 175-184 (2005).
 - 5) C.H.Kung, W.S.Cheng and Y.H.Yan: *Proc Int Carnahan Conf ecur Technol*, Vol. 37, pp. 422-427 (2003).
 - 6) 江島 将高, 宮崎 明雄: 周波数領域利用形電子透かし方式の性能評価について, *電子情報通信学会論文誌A*, Vol.J84-A, No. 10, pp. 1272-1281 (2001).
 - 7) 高井 信勝: デジタルホログラフィとその暗号化技術への応用, *光技術コンタクト*, 第42巻, 第6号, 283-291 (2004).
 - 8) 高井 信勝: 拡散型デジタルホログラフィにおける再生像の誤差評価, *北海学園大学工学部研究報告*, 第31号, pp. 87-100 (2004).
 - 9) B. Schneier: *Applied Cryptography*, second edition (John Wiley & Sons, Inc. 2nd ed. 1996).
 - 10) 結城 浩著:「暗号技術入門」, (ソフトバンク・パブリッシング2003).