情報処理学会論文誌 Vol. 51 No. 3 1078–1082 (Mar. 2010)

テクニカルノート

Wet Paper 符号を用いた画質劣化の少ない改ざん検出用 JPEG 画像の生成

山脇和美[†1] 野田秀樹[†1] 新見道治[†1]

本論文では，JPEG 画像を対象とした改ざん場所の特定可能なフラジャイル電子透かしにおいて，Wet Paper 符号を用いた高性能な埋め込み法を提案する．提案法は，量子化前の実数 DCT 係数の情報を積極的に利用して，画質劣化が少ない埋め込みを行う点が特徴である．提案法は，LSB 置換やマトリックス埋め込みと比べて画質劣化が少ない方法であることを確認した．

Less Degraded Watermarked Images Using Wet Paper Code for Content Authentication of JPEG Images

Kazumi Yamawaki,[†1] Hideki Noda[†1]
and Michiharu Niimi[†1]

This paper presents a block-wise content authentication method for JPEG images, which produces less degraded watermarked images. The proposed method utilizes the wet paper codes which can suppress distortions of DCT coefficients caused by embedding and quantization. It is confirmed that quality of watermarked images by the proposed method is better than those by LSB and matrix embedding.

1. はじめに

デジタル画像は複製・編集が容易であるため，その真正性を認証するための技術が求められている．その 1 つとして，認証に必要な情報を透かしデータとして画像に埋め込む電子透かし技術[1)] があるが，その対象となる画像は BMP 形式を想定する場合が多い．しかし，実際に流通している画像は圧縮画像が大多数を占め，その中でも JPEG 形式が用いられることが多い．これまでに，JPEG 画像を対象とした電子透かしとして，量子化された離散コサイン変換（DCT）係数の最下位ビット（LSB）を透かしデータで置換する手法が提案されている[1)]．しかし，透かしデータの埋め込みにより，画質劣化が生じるという問題があった．電子透かしでは，透かし情報が埋め込まれていることを隠す必要はないため，多少の画質劣化は問題にならないことが多い．しかし，医用画像や犯罪証拠写真等なんらかの判断に用いられるような画像の場合は，画質劣化が判断に影響を与える可能性があるため，できるだけ劣化を抑えることが望ましい．埋め込まれた透かしデータを抽出した後，完全に原画像を復元できる可逆（ロスレス）電子透かし[2)] も提案されているが，余分な復元処理が必要で，復元された原画像自体は無防備になるという問題点がある．また，ロスレス電子透かしは一般に，埋め込み量が少なく，画質劣化も大きい．

本論文では，ロスレスでない通常の改ざん検出電子透かし（フラジャイル電子透かし）を対象とする．できるだけ劣化の少ない透かし入り JPEG 画像の生成を目的とし，Wet Paper 符号（WP 符号）[3)] を用いたフラジャイル電子透かしを提案する．LSB 置換をはじめとして通常は，量子化後の DCT 係数を変化させて埋め込みを行うが，提案法では，量子化前の実数 DCT 係数の情報を積極的に利用して，変化（画質劣化）が少ない埋め込みを行う点が特徴である．そのために，WP 符号を用いる．WP 符号を用いると，量子化誤差の小さい DCT 係数のみを埋め込みに使用することができ，画質劣化を抑えることができる．受信者は鍵を用いて，埋め込まれた場所を知ることなしに情報を抽出できる．ステガノグラフィの方法として提案されている WP 符号のフラジャイル電子透かしへの適用は，ほとんど直接的に行うことができる．しかし，二値画像の場合以外にその適用例の報告はまだないようである．

2. 透かし入り JPEG 画像の生成と改ざん検出

改ざんが行われた場合に，改ざん場所を特定できる機能は有用であるため，改ざん場所の特定可能なフラジャイル電子透かしを考える．改ざん場所の特定は，一定の大きさのブロックごとに行われる．ブロックごとの認証情報として，ブロック内の量子化 DCT 係数（最下位ビットを除く上位ビット）全体のハッシュ値を用い，それをブロック内の量子化 DCT 係数の LSB に埋め込む．フラジャイル電子透かしに対する各種の攻撃に耐性を持たせるには，

†1 九州工業大学
Kyushu Institute of Technology

128 ビット程度のハッシュ値を用い，同じ 128 ビットで画像識別番号や画像中のブロック番号等を表現し，両者の排他的論理和を取ったものを埋め込み情報とする方法が推奨されている[4]．実用場面ではそのような情報を埋め込む必要があるが，本論文では透かし入り JPEG 画像の画質評価を主眼にしているため，1 ブロックあたり 128 ビットのハッシュ値のみを埋め込んでいる．

JPEG 画像は，前処理，DCT 変換，量子化，エントロピー符号化の手順で生成される．本手法では，DCT 係数の量子化時に透かしデータを埋め込み，透かし入り JPEG 画像を生成する．まず，通常の JPEG 符号化を量子化工程まで行い，得られた量子化 DCT 係数画像をブロックに分割する．次に，ブロック内のすべての量子化 DCT 係数について，LSB を切り捨てた量子化 DCT 係数すべてを用いてハッシュ値を算出する．その後，量子化工程に戻り，求めたハッシュ値を透かしデータとして各ブロックに埋め込む．その際，埋め込みによって量子化 DCT 係数の上位ビットの値が変わらないような実数 DCT 係数のみを用いる必要がある．具体的には，実数 DCT 係数 x が，$2i < x < 2i+1,\ i \in Z$ の範囲にある係数のみを用いる．埋め込み後の量子化 DCT 係数をエントロピー符号化して，透かし入り JPEG 画像を得る．

改ざん検出は以下のように行う．まず，透かし入り JPEG 画像をエントロピー復号化し，量子化 DCT 係数を得る．復号した量子化 DCT 係数を符号化時と同様にブロック分割後，LSB を切り捨て，各ブロックのハッシュ値を算出する（ハッシュ値 1）．また，復号した量子化 DCT 係数の LSB から透かしデータ（ハッシュ値 2）をブロックごとに抽出し，先に求めたハッシュ値 1 との比較を行う．ハッシュ値 1 とハッシュ値 2 が等しければ改ざんなし，異なっていれば改ざんありとして，改ざんの有無を判定できる．量子化 DCT 係数の LSB を除く上位ビットの改ざん検出は，ハッシュの衝突がない限り確実に行えることを実験的に確認している．

3. WP 符号による埋め込みと抽出

WP 符号による埋め込みでは，埋め込み側が埋め込み場所（どの DCT 係数に埋め込むか）を指定することができる．この埋め込み場所のことを selection channel と呼ぶ．selection channel を隣接する量子化代表値の中間付近に設定することで，埋め込みと量子化による DCT 係数の変化を小さくすることができる．具体的には，実数 DCT 係数 x が，$2i + 0.5 - \delta < x < 2i + 0.5 + \delta,\ i \in Z$ の範囲にある係数のみを用いる．ただし，δ は，$0 < \delta < 0.5$ であり，埋め込み範囲を設定するパラメータである．また，データ抽出においては，抽出側が埋め込み場所を知らなくてもデータ抽出ができるという特徴がある．

n 画素からなる原画像を $\boldsymbol{x} = \{x_i, i = 1, \ldots, n\}$，埋め込み後の画像を $\boldsymbol{y} = \{y_i, i = 1, \ldots, n\}$ とする．埋め込み側は，n 画素の中から selection channel を k 画素選択し，それを x_j，$j \in J \subset \{1, \ldots, n\}$，$|J| = k$ とする．x_i の LSB を $b(x_i)$，y_i の LSB を $b(y_i)$ とすると，原画像の LSB ベクトル $\boldsymbol{b_x} = (b(x_1), b(x_2), \ldots, b(x_n))^t$ は $\boldsymbol{b_y} = (b(y_1), b(y_2), \ldots, b(y_n))^t$ へ変更される．$\boldsymbol{x^t}$ は $\boldsymbol{x}$ の転置を表す．

m ビットのメッセージ $\boldsymbol{m}$ を埋め込むため，selection channel x_j，$j \in J$ を次式を満足するように変更する．

$$\boldsymbol{D b_y} = \boldsymbol{m} \tag{1}$$

$\boldsymbol{D}$ は $m \times n$ の 2 値行列であり，埋め込み側と抽出側で共有される鍵となる．$\boldsymbol{v} = \boldsymbol{b_y} - \boldsymbol{b_x}$ となる変数 $\boldsymbol{v}$ を考え，式 (1) を書き換えると，

$$\boldsymbol{D v} = \boldsymbol{m} - \boldsymbol{D b_x} \tag{2}$$

となる．$\boldsymbol{v}$ の中で k 個の v_j，$j \in J$ は，埋め込みによって LSB 値が変化する可能性のある場所を表し，未知数である．残りの $n-k$ 個の v_i，$i \notin J$ は $v_i = 0$ である．そこで，$\boldsymbol{D}$ から $n-k$ 個の列ベクトル $\boldsymbol{d_i}$，$i \notin J$ を除いて，$m \times k$ 行列 $\boldsymbol{D'}$ を得る．同様に $\boldsymbol{v}$ から $n-k$ 個の要素 v_i，$i \notin J$ を消去したものを，同じ記号を用いて $\boldsymbol{v}$ とすると式 (2) は，

$$\boldsymbol{D'v} = \boldsymbol{s} \tag{3}$$

となる．$\boldsymbol{s} = \boldsymbol{m} - \boldsymbol{D b_x}$ は $m \times 1$ ベクトルであり，埋め込みでは m 次線形方程式を解く必要がある．また，抽出時は $\boldsymbol{b_y}$ が既知となるため，式 (1) によりメッセージを抽出できる．

4. 実　　験

提案法の性能を評価するために，画質比較実験を行った．実験には，512×512 画素の 4 枚の標準画像（lena，mandrill，milkdrop，peppers）を用いた．それぞれ，1 画素あたり 8 ビット（8 bpp）で表現されたモノクロ濃淡画像と，24 bpp のカラー画像を用いた．

比較のため，以下の 5 種類の手法により生成した JPEG 画像を用いた．ただし，ロスレス埋め込みはモノクロ画像に対してのみ行った．

(a)　埋め込みなしの JPEG 圧縮（品質係数 80）
(b)　WP 埋め込み（提案法）
(c)　LSB 置換埋め込み
(d)　マトリックス埋め込み
(e)　ロスレス埋め込み

表 1　モノクロ濃淡画像に対する埋め込み実験結果（数字は PSNR (dB) 値）
Table 1　Experimental results in PSNR (dB) for monochrome images.

image	埋め込みなし	WP	LSB 置換	マトリックス	ロスレス
lena	38.54	38.48	38.09	38.28	33.96
mandrill	32.30	32.29	32.19	32.24	26.71
milkdrop	40.63	40.54	39.93	40.22	36.01
peppers	37.00	36.96	36.69	36.81	33.70

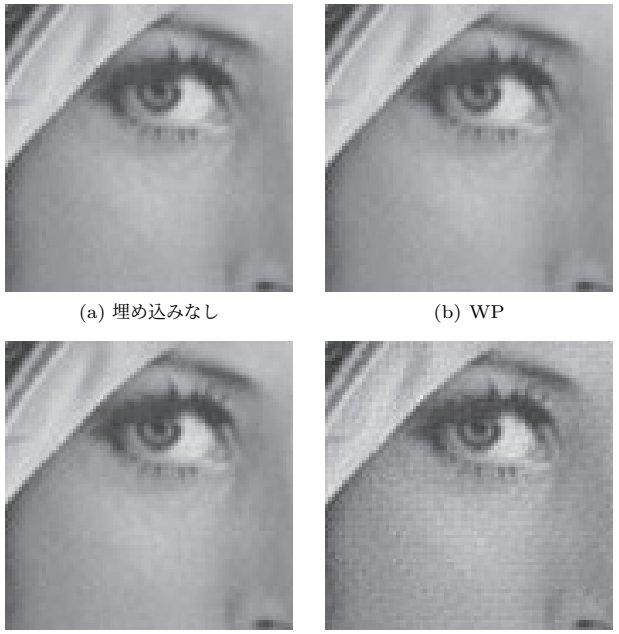
表 2　カラー画像に対する埋め込み実験結果（数字は PSNR (dB) 値）
Table 2　Experimental results in PSNR (dB) for color images.

image	埋め込みなし	WP	LSB 置換	マトリックス
lena	33.57	33.45	32.16	32.47
mandrill	26.65	26.62	26.39	26.41
milkdrop	33.47	33.28	32.04	32.42
peppers	35.46	35.25	33.49	33.95

128 ビットのハッシュ値を埋め込むためのブロックサイズは 64×64 画素とした．これは，JPEG 圧縮の処理単位である，DCT 変換を行う 8×8 画素のブロック（DCT 変換ブロックと呼ぶ）の 64 個分に相当する．提案法では，128 ビットのハッシュ値を 16 ビットごとに分けて，16 ビットを 8 個の DCT 変換ブロックに埋め込んだ．各 DCT 変換ブロック内では，64 個の周波数成分のうち，低周波（直流成分含む）の 21 個の周波数成分に埋め込みを行い，selection channel を定める δ は，$\delta = 0.3$ とした[⋆1]．マトリックス埋め込みは，LSB 置換と同様に，量子化 DCT 係数の LSB を変化させて埋め込みを行うが，埋め込み効率の良い方法として知られている．ここでは，符号長 7 のハミング符号を用いたマトリックス埋め込み[1] を行った．LSB 置換やマトリックス埋め込みでは，64 個の DCT 変換ブロックの低周波 21 個の周波数成分にランダムに埋め込みを行った．ロスレス埋め込みは，文献 2) 中の方法 1 で行った．

表 1 にモノクロ濃淡画像に対する埋め込み実験結果を，**表 2** にカラー画像に対する埋め込み実験結果を示す．画質評価尺度としては PSNR 値を用いている．**図 1** にモノクロの lena 画像に対する実験結果を，**図 2** にカラーの lena 画像に対する実験結果を示す．表 1 より，ロスレス埋め込みの PSNR 値が極端に低く，WP 符号を用いた提案法が最も高い PSNR 値を得ていることが分かる．ただし，ロスレス以外の 3 つの方法では，埋め込みなしの画像と比較して，埋め込み後の PSNR 値の低下は少ない．これと符合して，図 1 の WP や LSB 置換による埋め込み画像は，埋め込みなしの画像と比較して，差違は知覚できない．一方，ロスレス埋め込み画像では，明らかな画質劣化が知覚できる．図 1 では，性能面で WP と LSB 置換の間に位置するマトリックス埋め込みの図示は省略している．

表 2 より，カラー画像の場合も，WP 符号を用いた方法が最も高い PSNR 値を得ていることが分かる．ただし，カラー画像の場合は，WP 以外の方法ではやや大きな PSNR 値の低下が見られる．図 2 から，WP による埋め込み画像は，埋め込みなしの画像と比較して，



(a) 埋め込みなし　(b) WP

(c) LSB　(e) ロスレス

図 1　モノクロ濃淡画像 lena に対する実験結果
Fig. 1　Experimental results for monochrome lena image.

⋆1 周波数成分の数や δ の値は実験的に設定した．他の画像でも同様の傾向であったが，lena 画像において，周波数成分数 21 で $\delta = 0.2$，0.3，0.4 の場合，PSNR 値はそれぞれ，38.49，38.48，38.46 dB であった．周波数成分数 31 で $\delta = 0.2$，0.3，0.4 の場合，PSNR 値はそれぞれ，38.47，38.43，38.36 dB であった．δ については 0.2 の場合が最も PSNR 値が高いが，selection channel 内の埋め込み可能画素数を考慮して $\delta = 0.3$ とした．selection channel 内の画素数が埋め込みメッセージ長の 2 倍未満になると，式 (3) の解が得られない場合が起こるようになる．周波数成分数 21 で $\delta = 0.2$ の場合でも，selection channel 内の画素数は埋め込みメッセージ長 16 の 2 倍以上はあるが，余裕をみて 3 倍程度ある $\delta = 0.3$ とした．

(a) 埋め込みなし　(b) WP

(c) LSB　(d) マトリックス

図 2　カラー画像 lena に対する実験結果
Fig. 2　Experimental results for color lena image.

差違はほとんど知覚できないが，LSB 置換やマトリックス埋め込み画像では，差違が知覚できる．

WP 符号を用いた方法では，式 (3) の解を求めるために多くの計算時間を要するという欠点がある．本実験では，文献 3) 中の meet-in-the-middle アルゴリズムを用いて式 (3) の解を求めた．モノクロの透かし入り JPEG 画像 1 枚の作成に要した時間は，Intel(R) Pentium(R) 4 CPU 3.00 GHz 使用で，WP，マトリックス埋め込み，LSB 置換の場合でそれぞれ，220，33，2 秒程度であった．改ざん検出（認証）に要した時間は，WP で 3 秒程度，マトリックス埋め込みと LSB 置換では 2 秒程度であった．

5. おわりに

本論文では，JPEG 画像を対象とした改ざん場所の特定可能なフラジャイル電子透かしにおいて，WP 符号を用いた高性能な埋め込み法を提案した．提案法は，量子化前の実数 DCT 係数の情報を積極的に利用して，画質劣化が少ない埋め込みを行う点が特徴である．提案法は，LSB 置換やマトリックス埋め込みと比べて画質劣化が少ない方法であることを確認した．ただし，提案法は他の方法と比べて，透かし入り JPEG 画像の作成時に多くの処理時間を要するという欠点がある．

参 考 文 献

1) Cox, I.J., et al.: *Digital Watermarking and Steganography, 2nd Edition*, Elsevier (2008).
2) Fridrich, J., Goljan, M. and Du, R.: Lossless data embedding-new paradigm in digital watermarking, *EURASIP Journal on Applied Signal Processing*, Vol.2002, No.2, pp.185–96 (2002).
3) Fridrich, J., Goljan, M. and Soukal, D.: Wet paper codes with improved embedding efficiency, *IEEE Trans. Information Secrity and Forensics*, Vol.1, No.1, pp.102–110 (2006).
4) Fridrich, J.: Security of fragile authentication watermarks with localization, *Proc. SPIE*, Vol.4675, pp.691–700 (2002).

(平成 21 年 7 月 31 日受付)
(平成 21 年 12 月 17 日採録)

山脇　和美

平成 8 年九州工業大学工学部電気工学科卒業．平成 10 年同大学大学院修士課程修了．同年（株）アドバンスト・ディスプレイ入社．現在，九州工業大学研究補助員．画像処理，情報ハイディング等の研究に従事．電子情報通信学会会員．

野田　秀樹

昭和 48 年九州大学工学部電子工学科卒業．昭和 50 年同大学大学院修士課程修了．同年第二精工舎（現，セイコーインスツル），その後，警察庁科学警察研究所，郵政省通信総合研究所（現，情報通信研究機構）を経て，平成 7 年九州工業大学助教授，現在，同教授．博士（工学）．画像処理，情報ハイディング等の研究に従事．電子情報通信学会，日本音響学会各会員．

新見　道治（正会員）

平成 4 年九州工業大学工学部電気・計算機工学コース卒業．平成 6 年同大学大学院博士前期課程修了．同年長崎総合科学大学助手．平成 8 年九州工業大学工学部助手，平成 15 年同大学工学部助教授，平成 15 年同大学情報工学部助教授，平成 18 年同准教授，現在に至る．画像を中心とした情報ハイディングおよび自然言語処理の研究に従事．博士（工学）．電子情報通信学会，IEEE，映像情報メディア学会，人工知能学会各会員．