I-075

JPEG 画像を対象とした改ざん箇所の復元可能な電子透かし法

Digital Watermarking Method Restoring Manipulated JPEG Images

堀 友樹† 汐崎 陽† 岩田 基† 荻原 昭夫†
Tomoki Hori Akira Shiozaki Motoi Iwata Akio Ogihara

1. まえがき

デジタル技術やインターネットの普及に伴い, デジタル情報を扱う機会が増加している. デジタル情報は痕跡を残さずに変更を加えることが可能であるため, 改ざんの有無を確認することは困難である. そこで, デジタル情報に対する改ざんを検出・修復する手法の 1 つとして電子透かしが注目されている. 電子透かしとは, デジタル情報に対して人間が知覚できないように何らかの情報を埋め込む技術である [1]. このとき, 埋め込まれる情報を透かし情報と呼ぶ.

この技術を用いてデジタル画像の改ざんを検出・修復する手法に誤り訂正符号を用いる方法がある [2][3]. 文献 [2][3] の手法とも誤り訂正に Reed-Solomon 符号（以下, RS 符号）を用いているものの, 文献 [2] の手法は BMP 画像を対象としているのに対し, 文献 [3]（以下, 従来法）では, JPEG 圧縮画像を対象としている. 従来法では, YCbCr 成分の量子化後の DCT 係数から情報記号を生成し, それを RS 符号化して得られる検査記号を, 情報記号が変化しないように量子化後の DCT 係数に埋め込む. この画像が改ざんされた場合, 改ざんされた透かし入り画像から同じ手法で情報記号を生成し, 透かし入り画像から抽出した透かし情報を検査記号として誤り訂正を行い, 改ざんを検出・修復する.

従来法では高周波数領域の改ざんを検出するために, 高周波数領域から 1 つの係数を選択し, 情報記号に加えている. しかし, 1 つの係数のみを用いているため, 高周波数領域の改ざんを検出できない場合が多く, 安全性に問題があった. そこで, 本論文では高周波数領域全体からビット列を作成し, 情報記号に加える手法を提案する. 提案法は高周波数領域全ての値を用いるため, 従来法よりも安全性が高い. また, 提案法では, 従来法より改ざん修復後の画像の画質を向上させる.

2. 透かし情報と改ざん修復用画像

2.1 情報記号を構成するシンボルの選択法

本手法では, m ビットを 1 シンボルとし, 複数のシンボルを 1 単位として $GF(2^m)$ の上の RS 符号を使う. 1 つのシンボルが画像内の離れた位置の情報から構成されると, 改ざんにより複数のシンボルが壊される可能性が高くなる. よって, 1 つのシンボルは画像内の近い位置の情報から構成する. また, 1 単位に含まれるシンボルは同じ符号語に含まれるため, 画像内の近い位置から得たシンボルが同一単位内にあると, 改ざんによる誤りシンボル数が誤り訂正能力を超える可能性が高くなる. よって, 同一単位内には画像内の離れた位置の情報から生成されるシンボルが含まれるようにシンボルを選択する.

† 大阪府立大学大学院工学研究科

2.2 透かし情報の生成法

$M \times N$ 画素の原画像を RGB 表色系から YCbCr 表色系に変換し, 8×8 画素のブロックごとに DCT を施し, $Q(p)$ を用いて量子化する. $Q(p)(0 \leq p < 64)$ は DCT 係数のブロック内でのジグザグスキャンによる位置 p に対応する量子化テーブルの値である. 次に, 低周波数領域の量子化後の DCT 係数を 2^{β_p} で量子化し, $[-2^{\alpha_p-1}, 2^{\alpha_p-1}-1]$ の範囲のビット系列を得る. これは, -2^{α_p-1} 以下の値は -2^{α_p-1} に, $2^{\alpha_p-1}-1$ 以上の値は $2^{\alpha_p-1}-1$ にすることによって実現する. 量子化後の DCT 係数のうち, ビット系列作成に用いなかった DCT 係数全体の値を関数 g に入力し, 得られた出力を 6 ビット長の 2 進数として得る. この 6 ビットと, 低周波数領域から得られたビット系列を合わせたものを, 秘密鍵 key をシードとする乱数を用いてブロックごとに並び替え, 情報記号を生成する. 以上の操作を Y,Cb,Cr 成分それぞれで行い, 得られた情報記号に RS 符号化を施し, 検査記号を生成する. これを 3 ビットごとに 2 桁の 3 進数で表現し, 透かし情報 $R = \{r_{kl}(p) | r_{kl}(p) \in \{0,1,2\},\ 0 \leq k < M/8,\ 0 \leq l < N/8,\ 0 \leq p < n\}$ を得る. ここで, n は 1 ブロックに埋め込む透かし情報の要素数を表し, k, l は画像内での 8×8 画素のブロックとしての位置を表す.

3. 透かし情報の埋め込みと抽出法

3.1 透かし情報の埋め込み位置

意味のある改ざんは近接する複数のブロックの改変を伴うと考えられる. そのため, 一つの RS 符号語内のシンボル同士を近接するブロックに埋め込むと, 改ざんによって誤り訂正能力以上のシンボルが壊される可能性が高くなる. よって, 同じ RS 符号語内のシンボルは間隔をあけて埋め込む.

3.2 RGB 表色系の切捨て処理

DCT 係数に透かし情報を埋め込むと, YCbCr 表色系から RGB 表色系への変換において R, G, B の値が 0 以下や 255 以上になることがある. このとき, 端数が切捨てられること自体を, 改ざんであると誤って検出する可能性がある. そこで, 透かし情報を埋め込む前に原画像の R, G, B の値で 0 から K までの値を K に, $255-K$ から 255 までの値を $255-K$ に変更する. 以降は K を切捨て値と呼ぶ.

3.3 埋め込み法

原画像を YCbCr 表色系に変換し, DCT を施し, 得られた DCT 係数 $D_{kl}(p)(0 \leq p < 64,\ 0 \leq k < M/8,\ 0 \leq l < N/8)$ を, 式 (1) に従い $D'_{kl}(p)$ に変更し, 透かし情報 $r_{kl}(p)$ を埋め込む.

$$D'_{kl}(p) = [I_{kl}(p) - \{(I_{kl}(p) - r_{kl}(p)) \bmod 3\}] \times Q(p) \quad (1)$$

$I_{kl}(p)$ は $D_{kl}(p)$ を $Q(p)$ で量子化した値である．また，$(I_{kl}(p)-r_{kl}(p))\bmod 3 \in \{-1,0,1\}$ とする．これを $p=0$ から $p=n-1$ まで行い，ブロックごとに n 個の 3 進数値の透かし情報を埋め込む．以上の処理を画像全体に施し，透かし情報を全て埋め込む．各ブロックに対し IDCT を施した後，YCbCr 表色系から RGB 表色系に変換し，JPEG 圧縮して透かし入り画像を得る．

3.4 抽出法

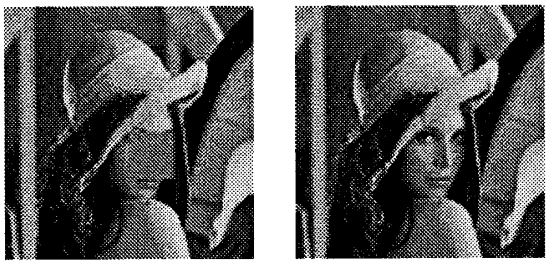
透かし入り画像の Y,Cb,Cr 成分の 8×8 画素のブロックごとに量子化 DCT 係数を求め，埋め込みを行った位置の $I'_{kl}(p)$ を得る．$r'_{kl}(p)=I'_{kl}(p) \bmod 3$ より透かし情報 $r'_{kl}(p)$ を得る．以上の処理を全てのブロックに施し，透かし情報を全て抽出する．

4. 改ざんの修復法

改ざん画像から 2.2 節と同様に情報記号を求め，改ざん画像から抽出した透かし情報を検査記号として，RS 復号を行う．検出された誤り位置から改ざん箇所を，誤り訂正の結果から改ざん修復用画像を得る．改ざん画像の YCbCr 表色系における改ざん箇所に改ざん修復用画像を上書きすることにより改ざんを修復する．ただし，誤り訂正能力を超えた誤りが生じ，誤り位置を検出できないときは改ざんの有無のみを出力する．

5. 実験と考察

実験には，標準品質である 75[%] で JPEG 圧縮し，BMP 形式に復号した 256 × 256 画素，RGB 各 256 階調の画像 lenna を用いた．透かし入り画像を得るときの JPEG 圧縮も標準品質とした．画像の客観評価には PSNR を用いた．秘密鍵 key は 100, 200, ··· ,900 の 9 種類を用い，関数 g の出力として入力の総和の絶対値を用いた．情報記号の生成におけるパラメータは，各ブロックについてジグザグスキャン順に，Y 成分の α_p は {7, 5, 5, 4, 5, 4, 4, 3, 3, 4}，Y 成分の β_p は {1, 2, 2, 3, 2, 3, 2, 2, 2, 2}，CbCr 成分の α_p は {5, 4, 4, 4, 3, 4}，CbCr 成分の β_p は {3, 2, 2, 1, 2, 1} とした．また，各ブロックについてジグザグスキャン順に，Y 成分は 11〜16 番目の 6 つの係数，CbCr 成分は 7〜10 番目までの 4 つの係数に，透かし情報を埋め込んだ．提案法では改ざん修復用画像の画質を向上させるために，α_p の値を従来法よりも大きく設定した．α_p の値を大きくしたことによって，低周波数領域から得るビット数が増え，埋め込む検査記号の数が増えるため，埋め込み位置を従来法より増やした．JPEG 圧縮に対する耐性を考慮し，切捨て値は $K=15$ とした．RS 符号化では，ビット削減された情報の 10 ビットを 1 シンボルとして扱い，256 シンボルを 1 単位として $f(x)=1+x^3+x^{10}$ を原始多項式とする $GF(2^{10})$ の上の，誤り訂正能力 21 の短縮化 RS 符号を用いた．情報記号の構成時には，縦横 1 ブロックおきに 1 シンボルを選択した．透かし情報の埋め込み時には，Y 成分では同じ検査記号内の 42 シンボルを縦 2× 横 2 の 4 つのブロックを 1 単位として横に 6 ブロック，縦に 6 ブロックの間隔をあけて埋め込んだ．また，CbCr 成分では同じ検査記号内の 42 シンボルを縦 2× 横 4 の 8 つのブロックを 1 単位として横に 4 ブロック，縦に 6 ブロックの間隔をあけて埋め込んだ．



(a) 改ざん画像　(b) 改ざん修復後の画像

図 1　改ざん検出・修復実験の結果

提案法では，従来法より低周波数領域から得るビットを増やしたため，改ざん修復用画像の PSNR は，従来法に比べて 1.59[dB] 高くなった．しかし，透かし入り画像の PSNR は，従来法に比べて 3.78[dB] 低かった．これは，低周波数領域から得るビットを増やしたことにより，埋め込む情報量が増えたためである．次に，提案法について，透かし入り画像に対して改ざんを施し，JPEG 圧縮を施した後に改ざん検出・修復実験を行い，正しく検出・修復されるか確認した．図 1 の (a) の改ざん画像は，従来法において，画像のどの位置であっても改ざんを修復できる最大の面積を改ざんした，提案法の透かし入り画像である．図 1 の (b) に改ざん修復後の画像を示す．実験の結果，改ざんは正しく検出・修復することができ，改ざん修復能力が下がっていないことが確認できた．

6. 安全性に関する考察

従来法では，高周波数領域から 1 係数をランダムに選択し，情報記号に加えることで，高周波数領域を改ざんされた場合や，アルゴリズムを公開した場合でも，改ざんの検出を可能にしていた．しかし，1 ブロックの高周波数領域の係数の数は約 50 個程度であるため，総当たりで探すことにより，選択された 1 係数を特定することは容易であり，また，画像によっては高周波数領域の値はほとんどが 0 であることから安全性が高いとはいえなかった．提案法では，透かし情報の生成において，高周波数領域全ての値を情報記号生成に用いている上，情報記号を生成する際に用いる関数 g に任意性があるため，関数 g を秘密鍵とすれば，関数を特定することは困難であり，安全性が高い．

7. むすび

本論文では，高周波数成分全体を情報記号に含めることにより，高周波数領域の改ざん検出能力を高め，安全性を向上させた．今後の課題として，透かし入り画像の画質を維持した上で，改ざん修復用画像の画質を向上させる方法の考案が挙げられる．

参考文献

[1] 松井甲子雄，“電子透かしの基礎，” 森北出版，1998.

[2] 南憲明，笠原正雄，“誤り訂正符号と暗号手法に基づく電子透かしの復号法，” 信学論 (A)，vol.J87-A, no.7, pp.967–975，2000.

[3] 安田拓矢，“安全性を考慮した電子透かしによる JPEG 画像の改ざん検出・修復法，” SCIS2007 予稿集，2B1-2, 2007.