J_054

# JPEG圧縮に耐性のあるデジタル画像の改ざん検出・修復可能な電子透かし

# Semi-Fragile Digital Watermarking Method for Detection and Restoration of Manipulation

安田 拓矢† 汐崎 陽† 岩田 基† 荻原 昭夫†
Takuya Yasuda Akira Shiozaki Motoi Iwata Akio Ogihara

## 1. まえがき

近年，デジタル技術やインターネットの普及に伴い，デジタルコンテンツを扱う機会が増加している．デジタルコンテンツには痕跡を残さずに変更を加えることができるため，改ざんの有無を確認することは困難である．そこで，デジタルコンテンツにおける改ざん検出・修復手法の一つとして電子透かしという技術が注目されている [1]．電子透かしとは，デジタルコンテンツ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のことである．このとき埋め込む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・修復する手法の一つに誤り訂正符号を用いる方法がある [2]。まず，デジタル画像のLSB以外の情報を情報記号としてReed-Solomon符号化 [3](以下，RS符号化) を施し，得られた検査記号を透かし情報としてLSBに埋め込む．改ざんされた場合，改ざんされたデジタル画像のLSB以外の情報を情報記号とし，LSBから抽出した透かし情報を検査記号として誤り訂正することにより改ざんを検出・修復する．この方法ではJPEG圧縮画像を対象にできないが，デジタルカメラで撮影された画像は，一般的にJPEG圧縮画像である．また，改ざんの後にJPEG圧縮を再度施されることを想定し，JPEGによる再圧縮に耐性を持つことが望ましい．そこで，本発表ではRS符号を用いた，JPEG圧縮画像に対する改ざん検出・修復用電子透かしを提案する．なお，提案法では3進数値を埋め込むことで画質の劣化を抑える手法 [4] を用いる．

## 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符号化を用いる．その1単位に含まれるシンボルは同じ符号語内のシンボルとなる．そのため，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．RS復号時には，選択されたシンボルの位置関係が必要となる．

### 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表色系に変換する．8×8画素のブロックごとにDCTを施し，$Q(i,j)$ を用いて量子化する．$Q(i,j)(0 \le i < 8, 0 \le j < 8)$ はDCT係数のブロック内での位置 $(i,j)$ に対応する量子化テーブルの値である．$Q(i,j)$ として，出力結果のJPEG圧縮の量子化テーブルの値を用いる．次に，$Q(i,j)$ による量子化後のDCT係数を $2^{\beta_p}$ でさらに量子化する．そして，$-2^{\alpha_p-1}$ 以下の値は $-2^{\alpha_p-1}$ に，$2^{\alpha_p-1}-1$ 以上の値は $2^{\alpha_p-1}-1$ とすることで，$[-2^{\alpha_p-1}, 2^{\alpha_p-1}-1]$ の範囲に値を制限する．ここで，$p$ はジグザグスキャンによるブロック内での順番を表わす．これにより，DCT係数の情報量は $\alpha_p$ ビットに削減される．この操作を画像全体に施し，ビット削減されたY成分を得る．得られたY成分にRS符号化を施して検査記号を生成し，3ビットごとに2桁の3進数で表現したものを透かし情報とする．

### 2.3 改ざん修復用画像の復元法

透かし情報を取り出し，2進数で表現する．また，透かし情報を埋め込んだ画像のY成分を2.2節の方法でビット削減する．このY成分と透かし情報をシンボル化し，RS復号を施す．8×8画素のブロックごとにRS復号後のビット削減されたY成分の情報を求め，$[-2^{\alpha_p-1}, 2^{\alpha_p-1}-1]$ の範囲の整数値とし，$2^{\beta_p}$ による逆量子化を施す．得られた $Q(i,j)$ による量子化後のDCT係数に再び逆量子化を施し，DCT係数を得る．そして，各ブロックにIDCTを施し改ざん修復用画像を得る．

## 3. 透かし情報の埋め込み法と抽出法

### 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であると考えられる．そのため，RS符号語内のシンボル同士が埋め込まれる位置が近いと，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縦方向，横方向ともに間隔をあけて埋め込む．抽出時には埋め込み時のブロック位置の対応関係が必要となる．

### 3.2 RGB表色系の切捨て処理

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，誤差の生じる原因となる．そのため，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，Y成分の8×8画素のブロックごとにDCTを施す．得られたDCT係数を $D_{kl}(i,j)(0 \le i < 8, 0 \le j < 8, 0 \le k < M/8, 0 \le l < N/8)$ とする．ここで，$k,l$ は画像内での8×8画素のブロックとしての位置を表し，$i,j$ は8×8画素のブロック内での画素としての位置を表す．式(2)のように $D_{kl}(i,j)$ を $D'_{kl}(i,j)$ に変更し，透かし情報 $r_{kl}$ を埋め込む．

$$D'_{kl}(i,j) = [I - \{(I - r_{kl}) \bmod 3\}] \times Q(i,j) \qquad (1)$$

† 大阪府立大学大学院工学研究科

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | 5 | 5 | 2 | − | − | − | − |
| 5 | 5 | 2 | − | − | − | − | − |
| 5 | 2 | − | − | − | − | − | − |
| 2 | − | − | − | − | − | − | − |
| − | − | − | − | − | − | − | − |
| − | − | − | − | − | − | − | − |
| − | − | − | − | − | − | − | − |
| − | − | − | − | − | − | − | − |

(a) $\alpha_p$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 2 | 3 | − | − | − | − |
| 2 | 2 | 3 | − | − | − | − | − |
| 2 | 3 | − | − | − | − | − | − |
| 3 | − | − | − | − | − | − | − |
| − | − | − | − | − | − | − | − |
| − | − | − | − | − | − | − | − |
| − | − | − | − | − | − | − | − |
| − | − | − | − | − | − | − | − |

(b) $\beta_p$

図1 透かし情報の生成におけるパラメータ

(a) 改ざん画像

(b) 改ざん修復後の画像

図2 改ざん検出・修復実験の結果

ここで，$I$ は $D_{kl}(i,j)$ を量子化テーブルの値 $Q(i,j)(0 \leq i < 8, 0 \leq j < 8)$ で量子化した値である．また，画質の劣化を抑えるために $(I - r_{kl}) \bmod 3 \in \{-1, 0, 1\}$ とする．これを埋め込み位置が重複しないように $n$ 回繰り返し，3進数値を $n$ 個埋め込む．これにより，ブロックごとに $1.5n$ ビットの透かし情報が埋め込まれる．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量子化DCT係数 $I'$ を得る．$r'_{kl} = I' \bmod 3$ より透かし情報 $r'_{kl}$ 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

改ざん画像から抽出した透かし情報を検査記号，改ざん画像のY成分をビット削減したものを情報記号として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．そして，改ざん修復用画像をCb,Cr成分は零値としてRGB表色系に変換し，改ざん箇所に上書きする．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，256×256画素，RGB各256階調の画像lennaを用いた．JPEG圧縮はconvertで行い，3.3節で埋め込みに用いた量子化テーブル $Q(i,j)$ に対応する品質である75[%]で圧縮した．画像の客観評価にはPSNRを用いた．透かし情報の生成におけるパラメータは図1に示す $\alpha_p$，$\beta_p$ を用いた．図1に示される値の位置は，DCT係数ブロック内の係数の位置に対応する．なお，値が表記されていない位置のDCT係数は0とし，ビット削除のときには情報を保持しない．RS符号を施すときは削減されたY成分の10ビットを1シンボルとして扱い，256シンボルごとに $GF(2^{10})$ の上の，誤り訂正能力16のRS符号化を施した．画質の劣化を考慮し，対応する量子化テーブルの値が8から10の中間周波数領域付近のDCT係数4箇所を埋め込み位置とした．JPEG圧縮に対する耐性を考慮し，切捨て値は $K = 10$ とした．透かし情報の作成時には縦横1ブロックおきに1シンボルずつ選んで情報記号を生成し，RS符号化した．透かし情報の埋め込み時には，隣り合う2つのブロックに1シンボルを埋め込む．このとき，1つの検査記号内の32シンボルを，横に6ブロック，縦に3ブロックの間隔をあけて埋め込んだ．一箇所に集中して改ざんされる場合，復元可能面積は6.25%であった．本実験では透かし入り画像にさらに同品質のJPEG圧縮を施すことをJPEG再圧縮と呼ぶ．

原画像をJPEG圧縮した画像に対する透かし入り画像のPSNRは40.2[dB]となり，主観的には画像の全体に薄いもやのようなノイズが生じていた．これは埋め込み位置が低周波数領域に近いためだと考えられる．次に，透かし入り画像に改ざんを施し，JPEG再圧縮した後に改ざん検出・修復を行った．図3に実験の結果を示す．なお，改ざん画像では改ざん箇所を白枠で囲んだ．実験の結果，JPEG再圧縮を施されても改ざんは全て正しく修復された．

## 6. むすび

本発表では，埋め込みに用いる量子化テーブルに対応した品質のJPEG再圧縮に耐性のある改ざん検出・修復用電子透かしを提案した．実験により，本手法が出力結果と同じ品質のJPEG再圧縮に耐性を持ち，改ざん修復が可能であることを示した．しかし，本手法のアルゴリズムが公開されると，透かし情報の上書きが可能になり安全性を保証できない．よって，アルゴリズムを公開したときの安全性を高めることが今後の課題となる．

**謝辞** 本研究の一部は，(財) 柏森情報科学振興財団の研究助成を受けて行われた．

## 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] 今井秀樹，“符号理論，” 電子情報通信学会，1990.
[4] T. Koga, A. Shiozaki, M.Iwata, and A.Ogihara, “Information hiding using operation of modulo 3 in JPEG coded domain，” Electron. Lett，vol.41，no.17，pp.957–958，2005.