

秘密鍵を用いた画像圧縮耐性を有する電子透かし埋め込み法の開発

(知能情報システム学) 井上 大輔

1. 緒言

ブロードバンド環境の爆発的普及やデジタル放送の開始で、CD や DVD といったデジタルデータに触れる機会は増える一方である。デジタルデータは扱いやすい反面、手軽に複製・編集することが可能である。これに伴い、不正コピーを防止し、著作権者の権利を守る必要性がますます大きくなってきており、この状況を打破するひとつの解決策として電子透かし技術の研究が進められている。

そこで本研究では、静止画像というデジタルデータに焦点をあて、「ウェーブレット係数の可変閾値判定に基づく電子透かし法」[1]を用いて、ウェーブレット変換係数の配列において、最も大きな JPEG (Joint Photographic Experts Group) 圧縮耐性を有する電子透かしの埋め込み位置を決定する最適化問題を作成し、遺伝的アルゴリズム(Genetic Algorithm,GA)を用いて近似最適解を求めることを目的とした。JPEG 圧縮は静止画像が最も施され易い加工処理の 1 つである。更に、透かし情報の埋め込み・検出に秘密鍵を用いることで、秘匿性の向上も図った。

2. ウェーブレット変換

2次元信号のウェーブレット展開係数を求める方法では、まず、画像信号の横軸(u)方向に一次元直交ウェーブレット変換を行い、展開係数を求める。次にその展開係数に対して縦軸(v)方向のウェーブレット展開係数を求める。原画像 $F(u,v)$ をレベル 0 の展開係数 $s_{u,v}^{(0)}$ とみなし(1a-d)式によりレベル $j+1$ の 4 種類の展開係数を求める。

$$s_{u,v}^{(j+1)} = \sum_l \sum_k \overline{p_{k-2u}} \overline{p_{l-2v}} s_{k,l}^{(j)} \quad (1a)$$

$$w_{u,v}^{(j+1,h)} = \sum_l \sum_k \overline{p_{k-2u}} \overline{q_{l-2v}} s_{k,l}^{(j)} \quad (1b)$$

$$w_{u,v}^{(j+1,v)} = \sum_l \sum_k \overline{q_{k-2u}} \overline{p_{l-2v}} s_{k,l}^{(j)} \quad (1c)$$

$$w_{u,v}^{(j+1,d)} = \sum_l \sum_k \overline{q_{k-2u}} \overline{q_{l-2v}} s_{k,l}^{(j)} \quad (1d)$$

ここで、 p_k はスケーリング関数の数列、 q_k はウェーブレットの数列を表す。 $w_{u,v}^{(j+1,h)}$ は横軸方向にスケーリング関数、縦軸方向にウェーブレットを作用させた展開係数を示す。 $w_{u,v}^{(j+1,v)}$ は横軸方向にウェーブレット、縦軸方向にスケーリング関数を作用させた展開係数を示し、 $w_{u,v}^{(j+1,d)}$ は縦方向、横方向にウェーブレットを作用させた展開係数を示す。(1a-d)式を繰り返し用いて $j=0$ から最高レベル $j=J-1$ までの展開係数を求める。ウェーブレット変換によって画像は図 1 のように分解される(L:低周波成分、H:高周波成分)。順次、 jLL の部分のウェーブレット展開係数がウェーブレット変換される。

3. 対象とする問題の定式化

JPEG 画像(JPEG 圧縮後に復号した画像)における電子透かし検出率 $d(x, y)$ に制約を課し、JPEG 圧縮および電子透かし埋め込みで生じる誤差 $e(x, y)$ と検出率 $d(x, y)$ を目的関数とした多目的最適化問題(P)を下記のように定式化した。

$$P \text{ Minimize } e(x, y) \quad (2)$$

$$\text{Maximize } d(x, y) \quad (3)$$

$$\text{Subject to } d(x, y) \geq a \quad (4)$$

$$e(x, y) = e_R(x, y) + e_G(x, y) + e_B(x, y) \quad (5)$$

$$e_l = \frac{\sum_{k=1}^m \sum_{i=0}^7 \sum_{j=0}^7 \{f_{l,k}(i, j) - f_{l,k}^*(x, y, i, j)\}^2}{64m} \quad (6)$$

$$l = R, G, B$$

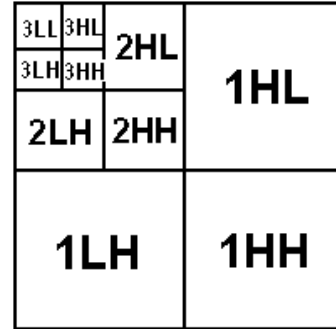


図1 Mallat 分割

ここで、原画像の RGB 成分を $YCbCr$ 成分に変換し、Y 成分の画像に対してウェーブレット変換を施し、その展開係数を図 1 のように配置された配列要素とした場合の 2 次元の要素番号を x, y (整数)とした(図 1 の左上の隅が $x=0, y=0$ で、右方向、下方向が各々 x, y の増加する方向)。そして、指定された展開係数から同一の展開係数群の範囲(例えば、3LH)内で秘密鍵で決まる電子透かし埋め込み位置(後述)に対して、埋め込み開始位置が (x, y) になるよう、全部の埋め込み位置をラスタースキャンの方向にずらして順次電子透かしを導入した後、 $CbCr$ 成分の画像とウェーブレット逆変換して得られる Y 成分の画像を RGB 成分画像に変換した。しかる後画像圧縮を施した。画像圧縮の手法としては JPEG を用いる。 $f_{l,k}, f_{l,k}^*$ は各々 k 番目のブロックの l ($l=R, G, B$)成分の原画における部分画像および JPEG 画像における部分画像である。 m はブロック数で、 a は定数である。電子透かしの検出は、JPEG 圧縮後、復号して行った。

4. GA におけるコード化

GA における遺伝子を 0,1 で表現し、上位 2 ビットでそのレベルでの展開係数の配列領域番号 n を表し、下位ビットの前半と後半でその領域内での透かし埋め込み開始位置の 2 次元配列の要素番号 x_n, y_n (整数)(左上の隅が $x_n = 0, y_n = 0$ で、右方向、下方向が各々 x_n, y_n の増加する方向)を各々 2 進数で表した。最も低い周波数成分である $(J-1)LL$ 部分に透かし情報を埋め込むと画像に埋め込みの形跡が出やすいと考えられるので、その領域を埋め込み対象から除外した。このため、各レベルでの展開係数の配列領域の種類は 3 となる(図 1)。この理由で、1/4 の割合で埋め込み対象としない領域を個体が表現する場合は起こる。その場合は、致死遺伝子として取り扱う。

5. 実験

実験環境として、Dell Dimension8400(CPU:PentiumIV 3.4GHz,メモリ:2GB)、OSにWindowsXP、開発言語としてVisual C++6.0を使用した。武蔵工業大学電気電子工学科信号処理研究室[2]よりダウンロードした「標準用画像データベース(SIDBA)」の一部から画像(mandrill,lenna,aerial,earth,couple)計5枚を取得し、256×256(画素)の24ビットカラーBMP形式に変換した。埋め込む透かし情報としてはランダムに発生させた100個のビット列を用いた。この実験では、ドベシィのウェーブレット変換を透かしの耐性と画質を考慮してレベル3まで施し、このうちの最も低い周波数成分となる3HL、3LH、3HHの3領域に対して近似最適解の探索を行った。下位ビット長は画像サイズで決まるため、遺伝子長は12ビットとなる。自然画像にウェーブレット変換を施し、その多重解像度表現(MRR)部のウェーブレット展開係数のヒストグラムをとると0を中心とする分布になる[1]。本研究ではその現象を利用した電子透かし法 [1]を用いた。

また秘密鍵には画像ごとに、レベル3の領域の大きさに相当する0~1024の範囲内で100個の乱数を発生させたものを各1個用意し、GAの個体表現で決まる位置のずらしを行った後、その数字に対応する位置で乱数の発生順序に従って透かしの埋め込み・検出を行うこととした。

GAの条件として、世代数20、個体数30、ルーレット戦略、2点交叉(交叉率0.6)、1点突然変異(突然変異率0.1)、を用いた。また、JPEG圧縮におけるクオリティを90とした(JPEG圧縮にはIndependent JPEG Group's softwareのオープンソース[3]を用いた)。制約条件は透かし検出率が90%以上($a = 90$)、適応度には $(d(x, y) - a + 1) / e(x, y)$ を用いた。

画像lenna(図2aを用いた場合の実験結果例を示す(実験で得られた埋め込み開始位置は、3LH領域, $x_1 = 31, y_1 = 30$, 検出率95.0%)。ランダムに埋め込み開始位置を決めた場合(◆)と本法によって求められた近似最適解(□)での埋め込みを行い比較した結果、本法により、検出率と画質が両立する良好な結果が得られることがわかった(図3)。また、本法と最適化を試みない場合[1]として3HL領域の左上隅を埋め込み開始位置とした場合での埋め込みと比較し最適化の効果を確認した(図4)。またJPEG2000による圧縮も行い良好な結果が出ることを確認した(図4)。



図2 電子透かし埋め込み例

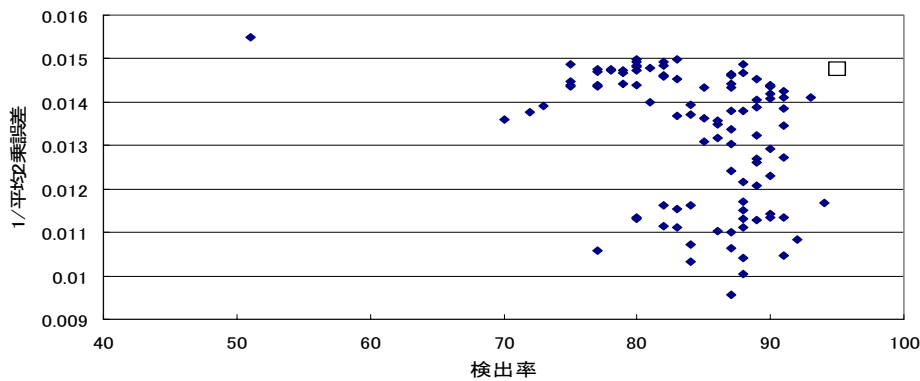


図3.画像lennaでのランダムに埋め込み位置を決定した場合との比較

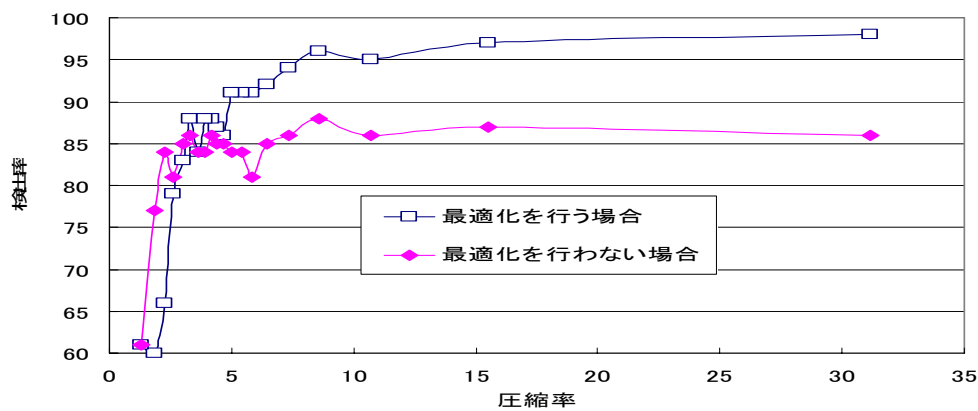


図4.画像lennaでの最適化を行う場合と行わない場合の比較

画像 lenna 以外の 4 枚の画像についても、検出率と誤差の関係で本法により良好な特性が得られた。4 枚の平均検出率は 99.25%であった。また 5 枚の画像の近似最適解探索にかかる平均処理時間は 23.56 秒/枚であった。なお、ランダムに秘密鍵を多数発生させ、埋め込み開始位置をずらさない方法より本法のほうが高検出率と低い 2 乗誤差の両立の点で優れていることも確認した。

6. 結言

画像のウェーブレット展開係数の配列において透かし情報埋め込み開始位置を決定するという多目的最適化問題を作成し、GA を用いて近似最適解を求めた。本法により、画像ごとに最適に近い埋め込み位置を決定することができる。また、近似最適解として求められた埋め込み位置情報だけでなく、画像特有の秘密鍵を所有していなければ埋め込み・検出を行うことができず、セキュリティの点でも性能向上することができた。

参考文献

- [1] 篠政義, 崔潤基, 相澤清晴, “ウェーブレット係数の可変閾値判定に基づく電子透かし法”, 信学技報 DSP2000-86, Vol.100, No.327, pp.29-34, 2000, Sept
- [2] 武蔵工業大学電気電子工学科信号処理研究室 ; <http://www.sp.ee.musashi-tech.ac.jp/app.html>
- [3] Independent JPEG Group's software ; <ftp://ftp.uu.net/graphics/jpeg/>