電子透かしを保存する凸射影法を用いたJPEG復号方法

伊藤　浩　　馬養　浩一　　藤井　亮介　　鈴木　光義
三菱電機（株）情報技術総合研究所

1．はじめに

電子透かしを画像の真正性の証明に応用した手法が提案されている[2,5]。このような手法を用いれば、監視画像に証拠性を与えたり、電子商取引で商品(画像)の原本性を証明したりすることができる。電子透かしは画像そのものに情報が埋め込まれるので、デジタル署名を用いた手法[6]に比べて、1)真正性を照合するためのコード(MAC)を画像と別個に取り扱う不便さがない、2)フォーマットの変換や編集などを行っても画像自体に変更がない限り真正性を証明することができるなどの特長がある。

多くの場合、画像情報はJPEGなどで圧縮されたストリームデータとして扱われるので、幾つかの電子透かしの方法はそのような表現に直接情報を埋め込んでいる[1,2]。この情報は、通常、画像情報が元のストリームの形態である限り失われることはないが、ビットマップの形態に復号された画像の中にそれが残存することは一般に保証されない。特に、「壊れやすい透かし」を利用した電子透かしの場合には、復号の影響を一層強く受けるため、情報の消失を回避する何らかの手段が必要である。

本稿では、文献[2]に提案された真正性証明のための電子透かしを対象として、これを埋め込んでJPEG符号化されたDCT係数を電子透かしの情報を失うことなく復号する方法を提案する。この方法は、復号されたベクトルが画像として表現可能な値の範囲に収まる条件とそのベクトルに透かしが残存する条件を与え、凸射影法[4]の考えに基づいて、二つの条件を同時に満たす整数ベクトルを得ようとするものである。計算機実験により、二つの条件の交わりを十分大きくとれば、高い確率で解が得られることを示す。

2．電子透かしの埋め込みとJPEG符号化

電子透かしは、64次元(8×8)の画素値のベクトルxのDCT係数を量子化ベクトル

$$Q_w = \{q_0^w, q_1^w, \cdots, q_{63}^w\} \qquad (2)$$

で量子化し、ジグザグスキャンの最後の係数の量子化インデックスを±1とすることによって埋め込まれる[2]。電子透かしが埋め込まれた量子化インデックスのベクトルを$\hat{y}_w$とする。同様の操作をN個のブロックに施せば、Nビットの情報を埋め込むことができる。この情報をN個のブロックの他の係数の量子化インデックスに依存するように決めておけば、量子化インデックスに変化があった場合にそれを検知することできる。

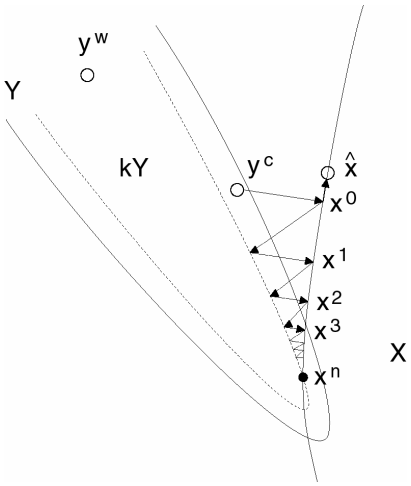

図1　凸射影法による復号ベクトルの探索

このブロックを符号化するには、符号化のための量子化ベクトル

$$Q_c = \{q_0^c, q_1^c, \cdots, q_{63}^c\} \qquad (1)$$

を用いてxのDCT係数を量子化し、得られたインデックスのベクトル$\hat{y}_c$を可変長符号化してビットストリームとする。ただし、$\hat{y}_c$は、

$$Q_w(Q_c^{-1}(\hat{y}_c)) = \hat{y}_w \qquad (2)$$

を満たす全ての量子化インデックスの中で、

$$d = \left| Q_c^{-1}(\hat{y}_c) - T(x) \right| \qquad (3)$$

を最小とするものである。上式で、$Q(\cdot)$と$Q^{-1}(\cdot)$はそれぞれ量子化と逆量子化の演算子、$T(\cdot)$はDCTの演算子を表す。

ここで、量子化ベクトルについて二つの制限を設ける。まず、Q_cとQ_wの間に、

$$q_i^c \le q_i^w \text{ for } i = 0, \cdots, 63 \qquad (4)$$

が成り立つとする。この制限は式（2）を満たす$\hat{y}_c$が常に存在するための条件である。また、Q_wについて、

$$q_i^w \ge 8 \text{ for } i = 0, \cdots, 63 \qquad (5)$$

が成り立つとする。これは、以下に述べるJPEG復号を容易にするための条件である。

A Decoding Scheme of Watermarked JPEG Images based on Convex Projections
Hiroshi Ito, Koichi Magai, Ryousuke Fujii, Mitsuyoshi Suzuki
Mitsubishi Electric Co., Information Technology Laboratories

３．凸射影法による JPEG の復号

受信した $\hat{y}_c$ を復号するには、Q_c による逆量子化と逆 DCT を施し、その成分を整数に丸めてベクトル

$$\hat{x} = \mathrm{int}(T^{-1}(Q_c^{-1}(\hat{y}_c))) \qquad (9)$$

を得る。ただし、$T^{-1}(\cdot)$ は逆量子化の演算子である。このベクトルの成分がすべて[0:255]の範囲に入っていれば、この $\hat{x}$ を復号ベクトルとし、そうでない場合は、その範囲に値を修正して復号ベクトルとする。この修正をクリッピングと呼ぶ。

今、その成分が全て[0:255]の範囲内であるようなベクトルの集合を

$$X = \{x = (x_0, \cdots x_{63}) \mid 0 \le x_i \le 255\} \qquad (10)$$

とし、DCT 係数を Q_w で量子化したときに $\hat{y}_w$ に等しくなるようなベクトルの集合を

$$Y = \{x \mid Q_w(T(x)) = \hat{y}_w\} \qquad (11)$$

とすれば、復号において $\hat{x} \in X$ は常に成り立つが、$\hat{x} \in Y$ は保証されず、$\hat{x} \notin Y$ のときに透かしが消失する。そのような一つの例を図１に示した。図において、$\hat{x}$ はクリッピングによって集合 Y の外に復号されている。

ここで、集合 X と集合 Y は凸集合であるから、図１に示すように、$y_c = (Q_c^{-1}(\hat{y}_c))$ を初期値として、X と Y への直交射影を繰り返すと、二つの集合の共通の要素が求められる。この繰返しは唯一解 x^n に収束することが知られている[4]。ここで、x^n は実数ベクトルなので、これを整数に丸めたベクトルを $\hat{x}^n$ とするとき、$\hat{x}^n \in Y$ ならば、$\hat{x}^n$ は求めるベクトルである。$\hat{x}^n \notin Y$ ならば、$X \cap Y$ のより深くに新たなベクトルを探索する。これは、図１に示すように、集合 Y の代わりにその範囲を k (k<1)倍に縮小した集合(kY と表記する)を取り、これと集合 X の間で直交射影を繰り返すことで実行できる。このことから、次の復号アルゴリズムを得る。

復号アルゴリズム

Step1 $k \leftarrow 1, y \leftarrow Q_c^{-1}(\hat{y}_c)$.

Step2 $x \leftarrow P_X(T^{-1}(y))$.

Step3 if $|x - T^{-1}(y)| < \varepsilon$, then go to Step5.

Step4 $y \leftarrow P_{kY}(T(x))$, go to Step2.

Step5 if $Q_w(T(\mathrm{int}(x))) = Q_w(Q_c^{-1}(\hat{y}_c))$, then stop.

Step6 $k \leftarrow rk$, go to Step4.

ここで、$P_X(\cdot)$ は集合 X への直交射影の演算子である。このアルゴリズムが解を持つためには、$X \cap Y \neq \phi$ でなければならない。この条件は、電子透かしの埋め込みの前に、画素値の範囲を[m:255-m](m>0)に制限しておくか、または、文献[3]の手法を用いることによって満たされる。

５．計算機シミュレーション

標準画像の N2（カフェテラス）に対して、電子透かしの埋め込みと JPEG 符号化を行い、これを提案するアルゴリズムで復号して、収束性の評価を行った。表１は、解が得られた時点の k の分布をブロックの数で表示したものである。量子化の細かさは 3 通りに変えた。また、画素値は[m:255-m]に制限し、m の値は適応的に設定した。全ての場合について、$k = 0.663$ までに解が得られていることがわかる。

表１　収束性の評価

n	k	N2.bmp		
		q=1.0	q=0.1	q=0.01
0	1.000	81787	81772	81470
1	0.950	77	8	0
2	0.903	48	11	0
3	0.857	6	24	0
4	0.815	2	14	0
5	0.774	0	8	0
6	0.735	0	54	363
7	0.698	0	27	86
8	0.663	0	2	1
計	-	81920	81920	81920

６．まとめ

電子透かしが埋め込まれた符号化データを情報を失うことなく復号する手法を提案した。この手法は MPEG やウェーブレット符号化にも有効と思われる。解を得るための十分条件を明確にすることは今後の課題である。

参考文献

[1] 小林他、「JPEG 符号化列へのバイナリデータの埋込み法」、信学論 D-II、June 2000.

[2] 伊藤他、「JPEG 画像の真正性を証明する電子透かしの方法」、信学総合、March 2003.

[3] 渡辺他、「直交変換利用型電子透かしにおける無攻撃時の透かし情報消失防止についての検討」、画像電子学会誌、Jan. 2003.

[4] 西他、「超解像に見る多次元信号処理と逆問題」、計測と制御、Sept. 1992.

[5] F.Bartolini et al., “Image Authentication Tecnhiques for Surveillance Applications,” Proc. IEEE, Oct. 2001.

[6] B.Shneier, Applied Cryptography, John Wiley & Sons, 1996.