I-060

数論変換を用いた改ざん位置検出可能なJPEG画像に対する電子透かし

A Digital Watermarking Technique for Detecting Alteration on JPEG Images Using Number Theoretic Transform

田森　秀明*　　山本　強*

Hideaki Tamori　Tsuyoshi Yamamoto

1　まえがき

ディジタルデータは第三者による改ざんが容易であることから，公文書や証拠における利用では原本性が十分に保証される必要がある．従来から電子署名がこの原本性保証に用いられているが，画像においては改ざんの有無のみならず改ざん位置の検出を目的として，電子透かし技術の可能性が検討されている．これは，攻撃に対して意図的に壊れやすくした脆弱型電子透かしを小さなブロック単位で埋め込み，破壊された電子透かしの位置を同定することで改ざんの位置を検出するものである [1]．

電子透かしによる改ざん位置検出には，ハッシュ関数を利用したもの [2][3][4] がこれまでに提案されているが，我々は全く別のアプローチとして，数論変換を利用した新たな手法を提案している [5][6]．変換領域に署名情報を埋め込むことにより，安全性が比較的高い手法となっている．本稿では，JPEG 画像に対する数論変換を用いた脆弱型電子透かし法を提案する．また実験により，提案手法の有効性を検討する．さらに提案手法の安全性について議論する．

2　数論変換

ここでは，数論変換を紹介する [7]．P, α を正の整数，N を $\alpha^N = 1 \pmod P$ となる最小の正の整数とする．ここで，$\phi(P)$ を Euler 関数とすると，$N = \phi(P)$ となる α を位数 N の原始根と呼び，$N < \phi(P)$ となる α を単に位数 N の根と呼ぶ．

ここで，α を用いた次のような変換対を考える．

$$X(k) = \sum_{n=0}^{N-1} x(n)\alpha^{kn} \pmod P \tag{1}$$

$$x(n) = \frac{1}{N}\sum_{k=0}^{N-1} X(k)\alpha^{-kn} \pmod P \tag{2}$$

これらの計算は，P を法とする剰余数系ですべての演算が可能であり，丸め誤差を一切生じない．なお，P は素数のべき乗となるあらゆる任意の合成数を取り得る．電子透かしへの応用を考えたとき，P を知らない第三者は期待する変換結果を得ることができないことから P を鍵情報として利用できる．

3　提案手法

3.1　埋め込み処理

基本 DCT 方式の JPEG 圧縮では，YC_rC_b 表色系へ変換した原画像をブロック分割し，各ブロックで 2 次元離散コサイン変換 (DCT)，DCT 係数の量子化，そしてランレングス符号化とハフマン符号化を行う．提案手法の埋め込み処理は図 1 の様に，JPEG 符号化過程において，Y 成分の量子化 DCT 係数を操作することにより実現する．

Y 成分の量子化 DCT 係数の各ブロックを Y_{ij} とする．ここで，i は画像に対し横方向のブロック位置，j は縦方向のブロック位置とする．図 2 の様に，Y_{ij} からさらに $N \times N$ の正方行列を切り出す．ここで，N は Y_{ij} のブロックサイズより小さな偶

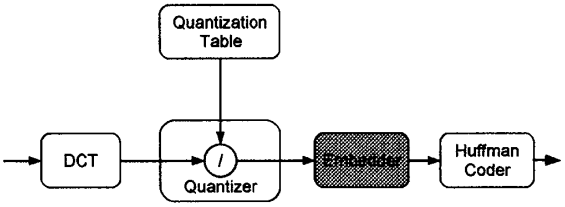

図 1 JPEG 符号化過程と提案手法における埋め込み処理の位置

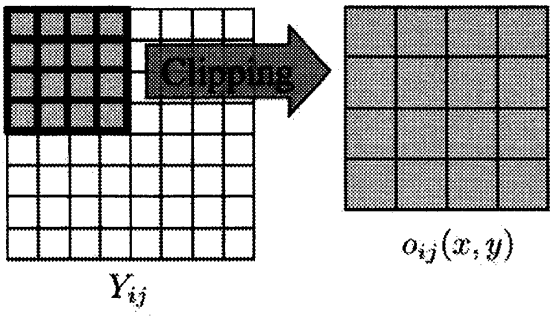

図 2 低周波成分からの $o_{ij}(x,y)$ の切り出し ($N = 4$)

数から選択する．この正方行列を $o_{ij}(x,y)(x,y = 0,\ldots,N-1)$ で表す．$o_{ij}(x,y)$ は埋め込み処理により値が変化するため，埋め込み処理による画像の劣化を考慮すると低周波領域から選択する必要がある．

次に提案手法の鍵情報となる，数論変換のパラメータである法 P を決定する．P は十分に大きな奇数から選択する．P と N より，根 α が決定される．これらのパラメータは非公開とする．

$o_{ij}(x,y)$ を決定したパラメータに基づき 2 次元数論変換し，これを $O_{ij}(u,v)(u,v = 0,\ldots,N-1)$ とする．次に $O_{ij}(u,v)$ から，署名情報を埋め込む要素を一つ選択し，これを $O_{ij}(u',v')$ とする．ϵ を埋め込み強度，$g_{ij} \in \{0,1\}$ を埋め込む署名情報として，

$$O_{ij}(u',v') + \delta = g_{ij} \pmod \epsilon \tag{3}$$

を満たす，絶対値が最小の整数 δ を計算する．そして $O_{ij}(u,v)$ のすべての要素に埋め込み操作を行い，これを

$$E_{ij}(u,v) = O_{ij}(u,v) + (-1)^{u+v+\theta}\delta \tag{4}$$

$$\theta = u' + v' \pmod 2 \tag{5}$$

で得る．$E_{ij}(u,v)$ の逆変換系列を $e_{ij}(x,y)$ とすれば，数論変換の計算性質から [6]

$$e_{ij}(x,y) = \begin{cases} o_{ij}(x,y) + \delta & x,y = N/2 \\ o_{ij}(x,y) & \text{otherwise} \end{cases} \tag{6}$$

となる．最後に $e_{ij}(x,y)$ を Y_{ij} の，$o_{ij}(x,y)$ を切り出した部分に上書きし，埋め込み済みのブロック Y'_{ij} を得る．この操作を

*北海道大学大学院情報科学研究科

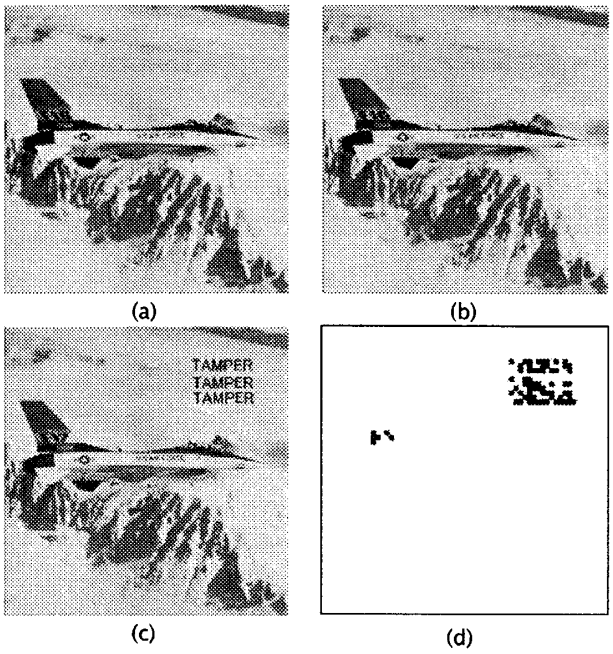

図 3 実験結果：(a) 原画像，(b) 埋め込み済み画像，(c) 改ざん画像．(d)(c) から取り出された署名情報

全ての Y_{ij} に行い，埋め込み済み画像を得る．なお，提案手法ではひとつの Y_{ij} に対し 1bit の埋め込み処理を行うことから，ij(bit) の署名情報を埋め込むことができる．

3.2 署名抽出処理と検出処理

署名情報の抽出処理は $E_{ij}(u',v')$ の ϵ による剰余をとることにより行う．つまり，

$$g_{ij} = E_{ij}(u',v') \pmod{\epsilon} \tag{7}$$

となる．

ここで埋め込み済み画像に改ざんがなければ正規の署名情報が抽出できる．一方で，鍵情報である P が不正であるか，埋め込み済み画像に改ざんがある場合，改ざんされた場合の $E_{ij}(u',v')$ は数論変換の性質から正規のものと大きく異なる．ゆえに，それから抽出される署名情報は破壊されている可能性が高い．破壊部分を認識することにより，改ざん位置を特定する．

4 シミュレーション実験

提案手法を airplane（512×512 画素）に適用し，有効性を検証した．実験には，数論変換のパラメータは法 $P = 13,512,341$，ブロックサイズ $N = 4$ とし，埋め込み強度は $\epsilon = 2$ とした．また，埋め込む署名情報の値はすべて 1 とした．

埋め込み処理を行った画像を図 3(b) に示す．埋め込み強度を小さくしているため SN 比は 54.7 dB となり，画像の劣化はほとんど目立たなかった．

次に，図 3(c) のように改ざんを行い，図 3(d) は図 3(c) から抽出した署名情報を図にしたものである．改ざんされたブロックからは不正な署名情報が抽出され，改ざん位置が認識できることが示唆された．

5 安全性についての議論

本節では，提案手法のアルゴリズムが既知である場合の安全性について議論する [6]．

5.1 鍵の全数探索

提案手法では，数論変換のパラメータの一つである P が鍵情報となり得るが，P は素数のべき乗による任意の合成数が選択することができるため，理論上無限大の探索空間となり，全数探索は困難であると言える．

5.2 任意の部分的な改ざん

提案手法では，署名情報は $E_{ij}(u',v')$ の ϵ による剰余から抽出される．これは，任意に改ざんを行った場合，1 つのブロックにつき ϵ^{-1} の確率で正規の署名情報を得られることを意味する．一般に，画像の冗長性から複数ブロックを改ざんする必要が生じる．T 個のブロックを改ざんした場合，そのすべての改ざんが成功する確率は ϵ^{-T} となる．ϵ が大きいほど改ざんの成功する確率は小さくなり，これは埋め込み強度となり得る．一方で提案手法では ϵ が大きいほど画像の劣化も大きくなることから，安全性と画像の品質はトレードオフとなる．

5.3 埋め込み済み画像への JPEG 再圧縮

提案手法ではブロック化した DCT 係数を数論変換し，その変換系列の要素の一つである $E_{ij}(u',v')$ に署名情報が埋め込む．埋め込み済み画像の JPEG 再圧縮を行った場合，圧縮過程による計算誤差があれば，再圧縮後の画像においては $E_{ij}(u',v')$ の値が変化する．ゆえに，画像全体で改ざんが認識される．

5.4 ブロックの入れ替えによる改ざん

同一画像内，あるいは同じパラメータを用いて埋め込み処理がされた画像で，Y'_{ij} 単位で切り貼りを行い，改ざんを行った場合を考える．埋め込み位置 u',v' が固定で決定されている場合，この改ざんは成功するが，u',v' が周辺ブロックの値により決定される変数と定義すれば，このような改ざんにも対応できると考える．

6 まとめ

本稿では，JPEG 圧縮画像に対応した，数論変換による脆弱型電子透かしを用いた改ざん位置の検出手法を提案し，シミュレーション実験を通じその有効性について検討した．鍵が秘密鍵であることから運用の利便性が欠けるため，今後は公開鍵暗号の適応について検討したい．

参考文献

[1] 遠藤，小出，“コンテンツ配信と不正コピー防止，”信学会誌，Vol. 83，No. 2，pp.117-121，Feb.2000.

[2] P.S.L.M. Barreto，H.Y.Kim，and V.Rijmen，“Toward A Secure Public-Key Blockwise Fragile Authentication Watermarking，”Proc. IEEE Int. Conf. Image Processing，vol.2，pp.494-497，2001.

[3] P.W.Wong，“A Public Key Watermarking of Image Verification and Authentication，”Proc. IEEE Int. Conf. Image Processing，vol.1，MA11.07，1998.

[4] 汐崎，“公開鍵暗号を用いた JPEG デジタル写真の改ざん位置特定可能な電子透かし法，”FIT2006，J-053，2006.

[5] H. Tamori，N. Aoki，and T. Yamamoto，“A Fragile Digital Watermarking Technique by Number Theoretic Transform，”IEICE Trans. Fundamentals，vol.E85-A，no.8，pp.1902-1904，2002.

[6] 田森，青木，山本，“数論変換による脆弱型電子透かしを用いた改ざん位置検出法”，信学会誌，vol. J86-A，No.8，pp.872-879，2003.

[7] H.J. Nussbaumer（著），佐川，本間（訳），高速フーリエ変換のアルゴリズム，科学技術出版社，東京，1989.