J-43

静止画像の改ざん位置検出と訂正を考慮した数論変換に基づく脆弱型電子透かし

Fragile Digital Watermarking Technique Based on Number Theoretic Transform for Localization and Correction of Digital Image Alteration

田森　秀明*　青木　直史*　山本　強*

Hideaki Tamori　Naofumi Aoki　Tsuyoshi Yamamoto

1　まえがき

ディジタル画像は第三者による改ざんが容易であることから，公文書における利用には原本性が十分に保証される必要がある．本来，電子署名がこの目的に用いられているが，画像における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] 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 [4]. 提案手法は改ざんの位置検出だけでなく，改ざん訂正の能力も兼ね備えた手法となっている．

2　数論変換

数論変換について簡単に説明する [5]. 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 [4].

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

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

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することができる．

3　提案手法

3.1　埋め込み処理

原画像を o で表す．o は $wN \times hN$ 画素とする．o を $N \times N$ 画素のブロックに分割し，一つのブロックを $\mathbf{o}_{xy}(x = 0, \cdots, w-1, y = 0, \cdots, h-1)$ で表す．また，$\mathbf{o}_{xy}$ の各画素値を $o_{ij}(i, j = 0, \cdots, N-1)$ で表す．

$\mathbf{o}_{xy}$ に埋め込む署名情報を $\mathbf{s}_{xy}$ とし，差分を取ることで署名情報を埋め込んだブロック $\mathbf{e}_{xy}$ を得る．すなわち，$\mathbf{e}_{xy}$ の各画素値を e_{ij}，$\mathbf{s}_{xy}$ の各値を s_{ij} とすると，

$$e_{ij} = o_{ij} - s_{ij} \tag{3}$$

となる．ここでは $\mathbf{s}_{xy}$ を P, x, y, i, j による以下の関数によって決定している．ϵ を埋め込み強度とすると，

$$s_{ij} = P(x + y + i + j) \pmod \epsilon \tag{4}$$

で決定する．この関数はあらかじめ送信者と受信者の間で決定しておく．

次に，$\mathbf{o}_{xy}$ と $\mathbf{e}_{xy}$ から，このブロックに対応する副鍵情報のブロック $\mathbf{K}_{xy}$ を生成する．$\mathbf{K}_{xy}$ は $\mathbf{e}_{xy}$ の数論変換係数と $\mathbf{o}_{xy}$ の数論変換係数の逆元の積で生成する．すなわち $\mathbf{o}_{xy}$ と $\mathbf{e}_{xy}$ の数論変換係数をそれぞれ $\mathbf{O}_{xy}$，$\mathbf{E}_{xy}$ とし，また $\mathbf{O}_{xy}$，$\mathbf{E}_{xy}$，$\mathbf{K}_{xy}$ の各要素値をそれぞれ O_{ij}，E_{ij}，K_{ij} とすると，

$$K_{ij} = E_{ij}A_{ij}^{-1} \pmod P. \tag{5}$$

以上の処理を $w \times h$ 個の全ブロックに対して行い，埋め込み済み画像 e と，副鍵情報 K を得る．送信者は，認証機関に鍵情報である K と P，受信者に対して e を送信する．なお，正規の受信者のみが認証機関から鍵情報を取得することができるものとする．

埋め込み処理を行う送信者は，主鍵情報となる数論変換のパラメータ P を決定する．ここで，画素値の最大値を o_{max} とすると，改ざん位置検出のために $P \gg o_{max}$ とするのが望ましい．また P を大きくすると，全数探索によって $\mathbf{K}_{xy}$ を同定することが非常に困難となるので，安全性を高めることができる．

3.2　抽出処理と検出処理

受信画像を e' とする．受信者は e' を $N \times N$ 画素のブロックに分割する．このブロックを $\mathbf{e}'_{xy}$ とし，この各画素値を e'_{ij} とする．$\mathbf{e}'_{xy}$ を，認証機関より取得した P に基づき数論変換する．変換後のブロックを $\mathbf{E}'_{xy}$，この各要素値を E'_{ij} とする．次に，式 (5) に基づき，$\mathbf{E}'_{xy}$ と $\mathbf{K}_{xy}$ の逆元との積を取る．この積を $\mathbf{O}'_{xy}$ とし，この各要素値を O'_{ij} とする．すなわち，

$$E'_{ij}K_{ij}^{-1} = O'_{ij} \pmod P. \tag{6}$$

得られた $\mathbf{O}'_{xy}$ を逆数論変換したものを $\mathbf{o}'_{xy}$ とする．署名情報を抽出するため，式 (3) に基づき，$\mathbf{o}'_{xy}$ と $\mathbf{e}'_{xy}$ との差をとる．これを $\mathbf{s}'_{xy}$ とする．つまり，o'_{ij}，s'_{ij} をそれぞれ $\mathbf{o}'_{xy}$，$\mathbf{s}'_{xy}$ の各要素値とすると，

$$o'_{ij} - e'_{ij} = s'_{ij} \tag{7}$$

となる．以上の操作を e' の全ブロックに施す．

$\mathbf{e}'_{xy}$ に改ざんがなければ $\mathbf{e}'_{xy} = \mathbf{e}_{xy}$ となる．この場合は，式 (3)，式 (5) および数論変換の性質から，$\mathbf{o}'_{xy} = \mathbf{o}_{xy}$，$\mathbf{s}'_{xy} = \mathbf{s}_{xy}$ となる．一方で，これらの式が成立しない場合は改ざんがあったと見なす．提案手法では，図 1 のように，$\mathbf{o}'_{xy}$ および $\mathbf{s}'_{xy}$ が，以下の条件を一つでも満たせば $\mathbf{e}'_{xy}$ は改ざんされているとする．

条件 1　$o'_{ij} > o_{max}$ である．

条件 2　式 (4) から署名情報を再度生成し，$\mathbf{s}'_{xy}$ と一致しない．

条件 3　$\mathbf{o}'_{xy}$，$\mathbf{s}'_{xy}$，式 (3) および式 (5) より副鍵情報を再度生成し，受信した $\mathbf{K}_{xy}$ と一致しない．

なお，改ざんされていなければ受信情報から原画像 o を復元することができる．

*北海道大学大学院工学研究科

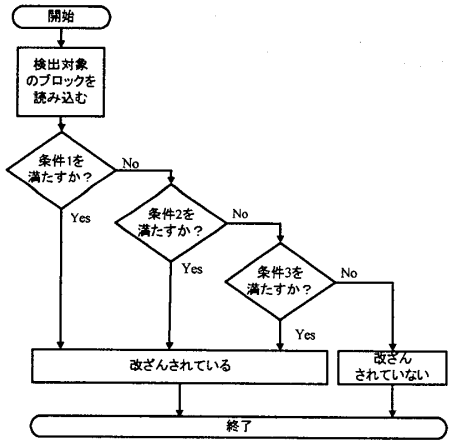

図 1 改ざん検出の処理過程

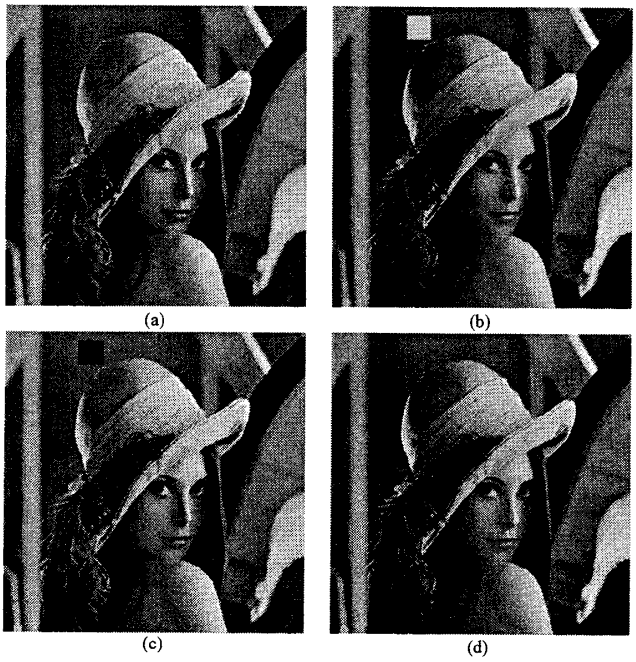

図 2 シミュレーション実験の結果：(a) 埋め込み画像 (b) 改ざん例 (c) 改ざん検出結果 (d) 改ざん訂正結果

4 提案手法による改ざん訂正

提案手法を用いると，改ざん検出のみならず訂正も可能である．3.2 で述べた条件を満たさないブロックは改ざんされていない正規ブロックの場合のみである．ゆえに改ざん訂正には図 1 の条件 1〜3 を満たさないブロックを全数探索すればよい．ただし，全数探索では多大な計算時間を必要とするため，ここでは改ざん箇所近傍の画素値の平均を初期値として探索を開始している．

5 シミュレーション実験

提案手法を LENA（256 × 256 画素，8bit 階調）に適用し，有効性を検証した．実験には，Pentium4 1.7GHz の計算機を用いた．数論変換のパラメータは法 $P = 782,497,813$，ブロックサイズ $N = 2$，根 $\alpha = 782,497,812$ とした．また，埋め込み強度 $\epsilon = 4$ とした．

埋め込み処理を行った画像を図 2(a) に示す．埋め込み強度を小さくしているため SN 比は 43.1 dB となり，画像の劣化はほとんど目立たなかった．

次に，図 2(b) のように改ざんを行った．これは図 2(a) において 20 × 20 画素の矩形領域内を輝度値 200 で塗りつぶしたものになっている．図 2(c) は改ざん検出の結果である．変色した部分が改ざん位置を示しているが，このように提案手法を適用することで，改ざん位置の検出が可能であることがわかった．

さらに，改ざん訂正の有効性について検討した．図 2(b) に改ざん訂正を施した結果が図 2(d) である．改ざん前の画像と全く同じものが得られているが，このように提案手法を適用することで，改ざん訂正が可能であることがわかった．

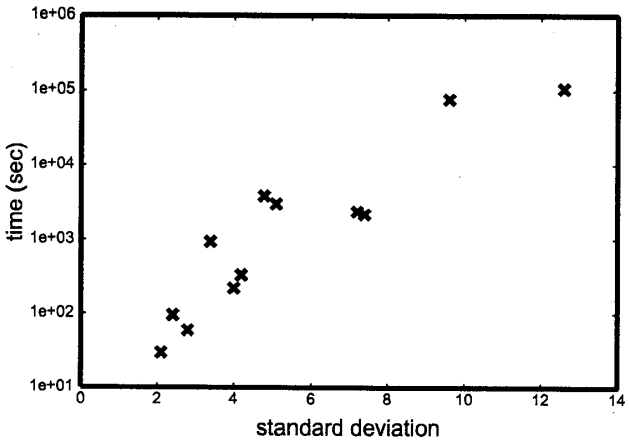

図 3 隣接画素の差分値の標準偏差と改ざん訂正に要する時間

図 3 は改ざん箇所における隣接画素の差分値の標準偏差を横軸に，訂正処理に要した時間を縦軸にとったグラフである．標準偏差が大きいほど訂正には時間がかかることがわかる．ここでは，改ざん箇所近傍の画素値を初期値として探索を開始しているが，真値との誤差が大きくなるにつれ訂正処理に要する時間が増大すると考えられる．

6 まとめ

本研究では，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と訂正について検討した．訂正処理に要する時間を短縮する方法について検討することを今後の課題としたい．また，現時点では考慮していない JPEG などの非可逆圧縮に対する検討を今後の課題としたい．

参考文献

[1] 遠藤直樹，小出昭夫，“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] H. Tamori，N. Aoki，and T. Yamamoto，“A Fragile Digital Watermarking Technique by Number Theoretic Transform，”IEICE Trans. Fundamentals，Aug. 2002.(to be published)

[5] H.J. Nussbaumer（著），佐川雅彦，本間仁志（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.