I-074

数論変換を用いた改ざん検出可能な非対称電子透かし

An Asymmetric Fragile Watermarking 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．そこで従来から原本性を保証する技術として，改ざんの有無のみならず位置の検出が可能な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位置を検出するものである．

電子透かしによる改ざん位置検出には，画素値から得られたハッシュ値と画素成分の LSB とを置き換える手法など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きた [1]．これは数論変換の性質である変換領域のランダム性や計算上の厳密性を利用したものであるが [1, 4]，秘密鍵を用いた手法であったことから，鍵の扱いが課題であった．一方で，鍵の扱いを容易にするため，署名情報の埋め込みと抽出でそれぞれ異なった鍵を用いる方式，すなわち各々の処理でアルゴリズムが非対称となるものが検討されている [2]．そこで本稿では数論変換の性質を利用した，アルゴリズム非対称型の脆弱型電子透かし方式を提案する．特徴として，数論変換で得られる相関関数を利用して署名情報の抽出を行うことがあげられる．提案手法についてシミュレーション実験を行い，その有効性について検討した．

2　数論変換

ここでは，数論変換を紹介する．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数学的な厳密性を持つ．また，変換領域には物理的意味は持たないが，フーリエ変換と同様に畳み込みの性質を持ち，フィルタリングや相関関数の計算，暗号に応用できる [3, 4].

3　提案手法

3.1　埋め込み処理

埋め込み処理を図 1(a) に示す．まず，処理に必要な数論変換で使用する位数 N と法 P をそれぞれ決定する．N は埋め込み処理の単位となるブロックサイズである．また，P は数論変換の条件から，a を任意の自然数として，$P = aN + 1$ を満たす，画素値の最大値より大きな素数とする [1].

元画像を $N \times N$ のブロックに分割したものの一つを f とする．f にランダム系列 r を与え，これを g とする．f，g をそれぞれ数論変換し，これらを F, G とする．F の要素それぞれの逆元を

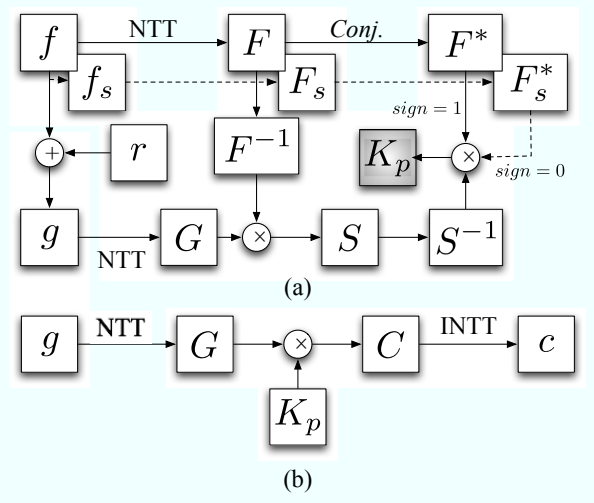

図 1　提案手法:(a) 埋め込み処理，(b) 抽出処理

とり，これを F^{-1} とすると，

$$S = F^{-1}G \tag{3}$$

となる S を得る．ここで S は F と G の逆畳み込みとなっている．

次に提案手法で公開鍵となる K_p を式 (4) により求める．

$$K_p = \begin{cases} F^*S^{-1} & \text{if } sign = 1 \\ F_s^*S^{-1} & \text{if } sign = 0 \end{cases} \tag{4}$$

ここで，F の共役を F^*，S の要素それぞれの逆元から構成される系列を S^{-1}，f の第 1 象限と第 4 象限，第 2 象限と第 3 象限を入れ替えた f_s を数論変換しその共役を F_s^*，このブロックに埋め込むべき 1bit の署名情報を $sign$ とする．

式 (3) より，

$$G = FS \tag{5}$$

であり，すなわち G は F と S の畳み込みである．G を逆数論変換すると，その誤差のない性質から g と全く同一の系列が得られ，これが埋め込み済み画像の一つのブロックとなる．

3.2　抽出処理と検出処理

抽出処理を図 1(b) に示す．受信画像を $N \times N$ のブロックに分割し，g を得る．g を数論変換し G を得て，K_p との畳み込み演算を行い，これを C とする．すなわち，改ざんがない場合，式 (4)，(5) より，

$$C = \begin{cases} FF^* & \text{if } sign = 1 \\ FF_s^* & \text{if } sign = 0 \end{cases} \tag{6}$$

となる．さらに得られた C を逆数論変換し，c を得る．

$sign = 1$ の場合，c は f の自己相関関数となっており，図 2(a) のように，系列の中心が最大となる．一方で $sign = 0$ の場合，f と f_s の相互相関関数となり，図 2(b) のように，系列の端が最大になる．このように c を判定することで g に埋め込まれている $sign$ を抽出する．

*北海道大学大学院情報科学研究科

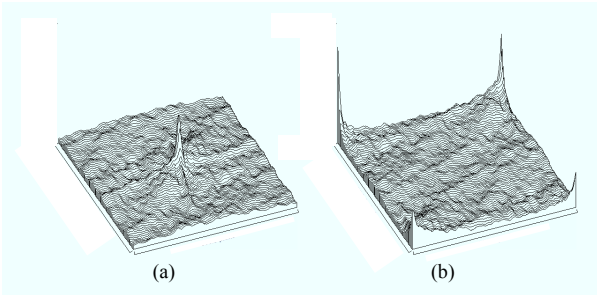

図 2 相関関数による判定：(a)$sign = 1$，(b)$sign = 0$

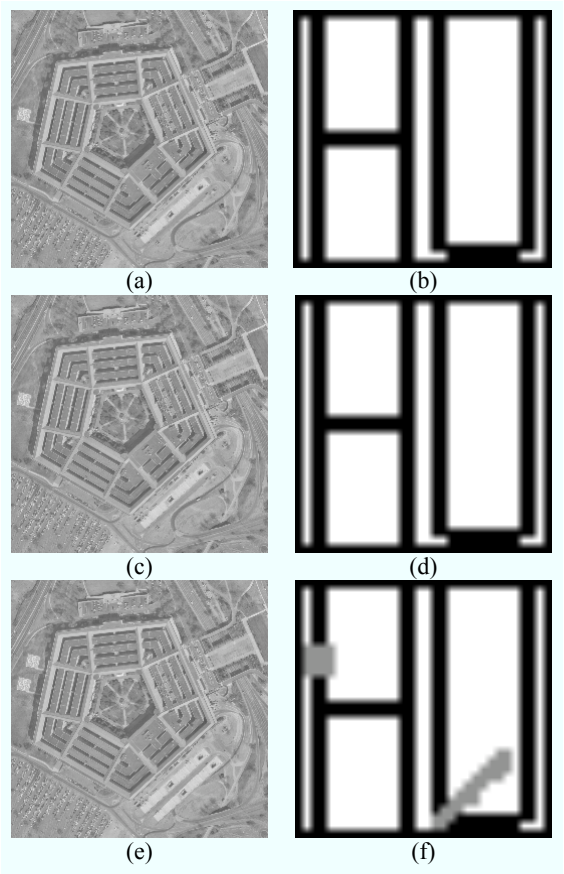

図 3 実験結果：(a) 元画像 (256×256)，(b) 署名画像 (32×32)，(c) 埋め込み済み画像，(d)(c) から抽出した署名画像，(e) 改ざん画像，(f)(e) から抽出した署名画像

一方で，g に改ざんが行われていた場合は，c は相関関数をなさず，$sign$ が判定できない．よって，$sign$ が抽出できないブロックを改ざん箇所とすることができる [1]．

4 シミュレーション実験

256×256 画素，画素値が 8 bit の画像である図 3(a) に対し，図 3(b) で示す 32× 32 画素，1 bit の署名画像を提案手法により埋め込み，その有用性について検討した．

実験で用いた数論変換のパラメータは法 P が 64 bit で構成される素数，ブロックサイズ $N = 8$ とした．また，ランダム系列 r は $\{-1, 0, 1\}$ で構成されるものとした．

埋め込み済み画像を図 3(c) に示す．PSNR は 50.2 db となった．また，図 3(c) から抽出された署名画像を図 3(d) に示す．数論変換の計算誤差の無い性質により，図 3(b) と同一のものが抽出された．

図 3(c) に対し図 3(e) の様な改ざんを行い，これから抽出された署名画像を図 3(f) に示す．$sign$ を判定できなかった部分が灰色の部分とした．改ざん位置と一致していることから，署名画像を視認することにより改ざん部分を特定できる可能性がある．

5 安全性についての議論

前提条件として，公開されているのは処理アルゴリズム，数論変換パラメータ，K_p，埋め込み済み画像とする．公開鍵 K_p は PKI により保証され，Man-in-the-Middle 攻撃は考慮しないものとする．よって，本章では攻撃を，抽出される署名情報 $sign$ が破壊されないように改ざんを行うことと定義する．攻撃を行うためには，

条件 1 g を攻撃者が意図する改ざん g' になるように変更する

条件 2 g' の全ての要素が画素値の最大値を超えない

条件 3 g' の数論変換系列 G' と K_p の畳み込み演算結果 c' が，抽出処理において $sign$ と判定される系列になる

ことが必要である．

t を改ざんによる画素値の増減とすると，$g' = g + t$ である．また，T を t の数論変換系列とすると，$G' = G + T$ となる．例えば $sign = 1$ のとき，

$$C' = G'K_p = F^*(F + TS^{-1}) \tag{7}$$

となる．よって，

$$TS^{-1} = \mathbf{0} \pmod{P} \tag{8}$$

となる T であれば条件 3 を満たす．提案手法においては $S^{-1} = \mathbf{0}$ とはならず，また非公開である．よって条件 2 を満たすには，K_p より S^{-1} を求め，式 (8) を満たす T を計算すればよい．これには K_p を素因数分解して F^* と S^{-1} を求めることとなるが，いずれも非公開であるから素因数の全ての組み合わせを全数探索しなければならない．求められた場合でも，n は式 (8) と条件 1，2 を同時に満たすものに制限されるため，提案手法は上記の条件を同時にを満たしにくい手法であると考える．ここで，P が大きいほど S^{-1} の探索範囲も大きくなる．また，t が条件 2 を満たしにくくなることから，提案手法では攻撃に対する安全性は P の大小に依存すると言える．

6 まとめ

本稿では数論変換を用いた，埋め込み処理と抽出処理のアルゴリズムが非対称な脆弱型電子透かしについて提案した．今後の課題として，非可逆圧縮されたディジタル画像への応用と安全性についての更なる検討があげられる．

参考文献

[1] 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.

[2] T. Furon, and P. Duhamel, “An asymetric watermarking method,” IEEE Trans. on Signal Processing, vol.51, no.4, pp.981-995, April 2003.

[3] S. Xu, L. Dai, and S.C. Lee, “Autocorrelation analysis of speech signal using fermat number transform(fnt),” IEEE Trans. on Signal Processing, vol.40, no.8, pp.1910–1914, August 1992.

[4] 比良田，高橋，三村，“画像マッチングに適用可能なキャンセラブル生体認証方式の脆弱性分析と安全性向上，” SCIS 2007, 3C1-2，佐世保，January 2007.