社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－DPS－126（11）
2006－CSEC－32（11）
2006／3／16

計算量的難読化を仮定した、不特定第三者の認証に依存する電子透かし方式

大関 和夫† 叢 力†

†芝浦工業大学 大学院 工学研究科 〒337-8570 埼玉県さいたま市見沼区大字深作 307

E-mail: †{ohzeki, m105075}@sic.shibaura-it.ac.jp

あらまし メディアに電子透かしを埋込む方式において、埋込み方式を秘密にし、埋込んだメディアとともに検出プログラムを難読化して公開し、公開領域にて不特定第三者の協力により埋込んだ透かしの検出を行なうシステムを考える。諸問題のうち、難読化を一定の処理が計算量的にあるレベルだけ複雑化する手続きを繰り返すことにより行なえると仮定し、任意のレベルの難読化を達成できるとする。耐性に関しては、一度埋込んだメディアに再度別の透かしを埋込む上書き処理をした場合の特性の解析を行なっている。

キーワード 電子透かし、難読化、認証、計算量的、第三者

Fingerprinting System Depending On An Anonymous Third Party Authentication Using An Assumption of Computationally Measurable Obfuscation

Kazuo OHZEKI† and CONG Li†

†Graduate School of Engineering, Shibaura Institute of Technology

307 Fukasaku, Minuma-ku, Saitama, Saitama, 337-8570 Japan

E-mail: †{ohzeki, m105075}@sic.shibaura-it.ac.jp

Abstract The authors propose an fingerprinting system which hides embedding method and disclose detection software. The system depends on anonymous the third party in open area for detecting embedded fingerprint. The obfuscation is assumed to be computationally measurable. The detection software is able to have an arbitrary complex level by iteratively adopting the obfuscating process.

Keyword Fingerprinting, Obfuscation, Authentication, computationally complex, the third party

1. まえがき

電子透かし方式は、映画やＣＤ音楽等を広く販売する際に埋め込む用途のような、大規模なシステムでは実用化されているが、インターネットで個人が小規模に画像を公開するような場合には、認証のための登録経費が大きくなり、事実上運用することは難しい。本研究では、個人レベルが認証のコストをかけることなく、電子透かしを埋め込んだ画像、音声メディアを公開し、その著作権を広く主張し続けることができるようにする方式を提案している。電子透かしは画像処理により劣化、消失するため、その耐性の定量的な評価をすることと、任意の第三者に著作権を主張するための認証性を有することが重要な事柄である。電子透かしの埋込みに認証性を付与するために、検出ソフトウェアを公開領域に提示し、任意の第三者が埋込んだ電子透かしを検証できるようにすることにより、その認証性を確保しようという提案をしている。検出ソフトを公開するにあたり、計算量的な難読化を組み込み、公開鍵暗号方式が、暗号鍵を公開しても、復号鍵を求めるのは計算量的に不可能に近くなるのになぞらえ、難読化に計算的な処理を組み込み、所定の計算を行なう方式にしておく。これにより、検出ソフトを公開しても、埋込みアルゴリズムを容易には逆算できなくなる。この仕組みを組み込んだ電子透かしシステムに対し、耐性とその認証性の度合いを定量的に評価

していく。

電子透かしの方式を認証性の機能の観点から分類すると、

(1) 情報隠蔽（埋込み者１人のみの処理）

(2) 秘密通信（Steganography :送信する埋込み者と受信する相手の 2 者の間の処理：１対１）

(3) 著作権主張（任意の第三者に対する著作権を主張する認証性を必要とする処理：１対多数）

に分けられる。(1)は電子透かしの埋込み者自身が検出を行い、全ての処理を秘密にできるが、著作権を主張するための認証性は備えていない。(2)は自分と相手と２者いるが、その間でのみ秘密が共有されていて、それ以外の外部に対する著作権主張はできない。(3)は埋込んだ電子透かしを単に自分で検出するのでなく、一般に任意の第三者に対し、著作権を主張しようとするもので、埋込んだ情報から改竄されずに完全に著作権を主張するという認証性を確保することは、条件が不足するため難しいことと考えられている。

これら[1][2]をもとに、本研究では、公開鍵暗号方式をそのまま適用するのでなく、電子透かしという信頼性の低いアナログ回線のような媒体に適合させるため、難読化という処理を介在させる。難読化に対しては、文献[3-6]などがあり、ある程度の難読化を行なうことができる。ここでは、それらの研究を発展させ、計算量的に複雑化する難読化を定義し、解読を計算量的に不可能にする方式の開発を目指す。

電子透かし方式は、メディアに埋め込んだ透かしによりメディアに対する著作権等を主張するためには任意の第三者に対して埋め込んだ情報を正しく抽出できることを示す必要がある。そのためには、透かしを埋め込んだ者が自分で検出するのではそのような証明はできないため、認証性は無いといえる。認証性を確保するには、守秘義務を履行できる公的な第三者機関に公正な検出を委託するか、検出器を公開するなどの策が必要になる。企業などが、画像などのメディアを配布するに当たっては、その著作権の認証を公的団体を作って行なわせることが可能だが、個人がインターネットで画像を配布するような場合は、そのような大がかりなことはできず、事実上著作権フリーの状態で配布せざるを得ない。本研究では、個人がメディア配布をする際にも、コストをかけずに電子透かしを埋込み、またその検証を埋込み者本人だけでなく、任意の第三者が行なえる形にすることにより、認証性の確保を行なうものである。難読化に関しては検討されたが[4-6]、検出ソフトは難読化しても、リバースエンジニアリングにより解読される可能性が高いと考えられてきた。

ここでは、難読化をプログラムを単なる複雑化したり、ランダム化するなどの小手先の処理をするのでなく、単純であっても、公開鍵暗号の復号鍵の探索を類推した、計算量的に難読化を施す事により、任意の与えられた難易度対し、それを達成する計算量をもった難読化を行うことを目指す。また、埋込み画像とともに検出器を提示するため、埋込みデータは通常の電子透かしのように具体的なロゴマークのようなものでなく、最小の記号でよいことになる。そこで、埋込み情報を最小の１ビットとし、耐性の方を最大化することができる。これまでの実験で、耐性が通常の電子透かしより大幅に高いことが調べられている。また関連して、透かしが１回埋込まれた画像に対し、同種の埋込みソフトで再度透かしを埋込む時に、上書き効果により１回目の透かしが破損ないしは消失する可能性がある。そこで今回多重の埋込みによる耐性についての検証も行なった。

2. 提案方式

図１に本研究方式の全体構成を、図２にそのうちの埋め込み、検出ソフト難読化等の部分の詳細を示す。画像は、デジタルカメラ画像や独自制作したＣＧ画像、ビデオ、印刷画像をスキャナで読み込んだものなどが入力される。電子透かしの埋込みと公開する検出ソフトは埋込み者が行なうが、詳細は図２に示されている。電子透かしを埋込んだ画像と検出ソフトは、web サーバにて公開される。埋込み方式は埋込み者のみが知り、秘密にされる。検出ソフトは、計

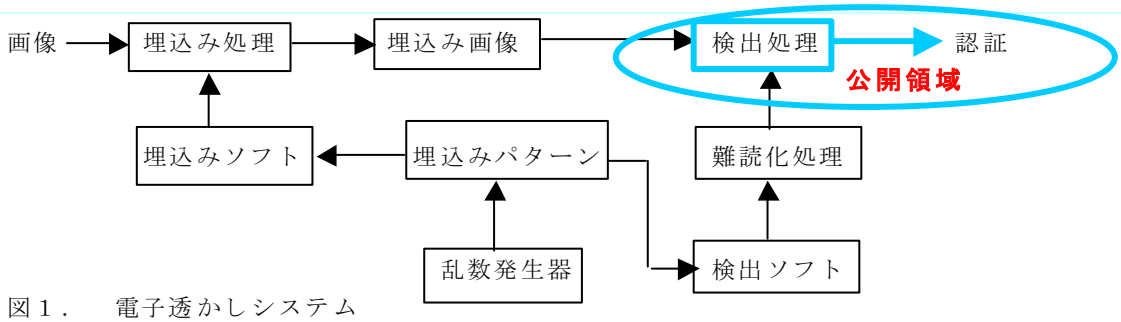

図１．　電子透かしシステム

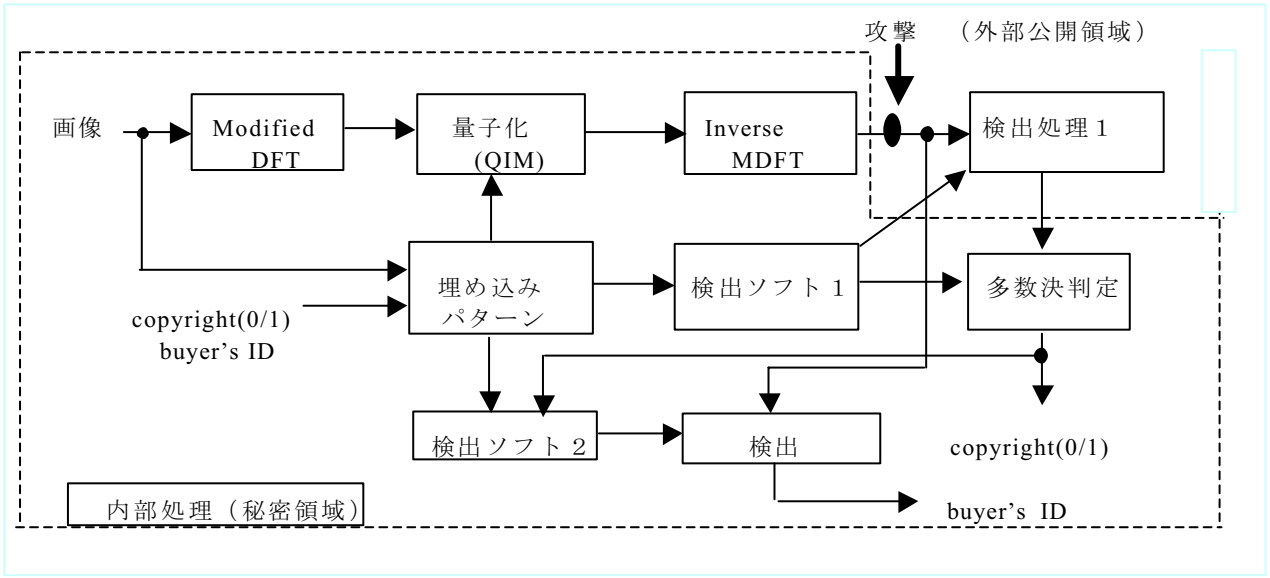

図２．　埋込み部の詳細構成

算量的に難読化され、公開鍵暗号方式の鍵探索に類似した手続きを取り込み、解読には膨大な計算的試行を要する方式になっているものとする。

透かしを埋込んだ画像は、画質の劣化を評価し、標準的な攻撃への耐性を評価し、また難読化の解読を行い、検出データから更に鍵の探索を行い、埋込みデータの抽出を行い、総合的な画質劣化と耐性評価、認証性の有無を定量的に評価していく。

電子透かしは、まず変形離散フーリエ変換(MDFT)で周波数領域に変換される。MDFT はフーリエ変換の変種で、鍵の種類に対応する方式パラメータの種類を増大するために導入してある。周波数領域で、埋込みパターンに対応して量子化される。埋込みパターンは図２の例の場合、画像メディアの購入者の符号(buyer's id)と全購入者に共通の符号の２段階の構成になっている。量子化は基本的には QIM 方式で行ない、更に個別変動なども可能である。埋込み後のデータは逆 MDFT され画像に戻る。埋込みにパターンに対応した個別検出ソフトは難読化され、電子透かしを埋込んだ画像とともに外部領域に公開される。埋込みデータは検出ソフト１により、全購入者に共通な著作権情報を抽出する。更に、購入者を登録して異なる id を埋込んだ場合は、第２段階目として、検出ソフト２により購入者ごとに異なる id を検出する。後者に対しては、いわゆる結託攻撃による、購入者 id の改竄や、除去を防ぐため、原画像の微小変動などの技術が使用できる。

3. 難読化手法

検出器を公開する上での重要な根拠となる難読化について検討する。

3.1 演算のディジタル変換方式

従来の難読化は、プログラムのある実行文を複数の実行文に変換したり、if 文を加え解析に複雑さを加えるというものが多い[4-6]。例えば、

x+y

という演算を

(x*2+y*2)/2

sqrt(x*x+2x*y+y*y)

などに置き換えるなどの複雑化処理が考えられるが、何らかの計算をしているという観点で調べれば、2 変数に関する線形連立方程式を解くことにより、演算のしかたが分かる。加算をやっている限りは、線形連立方程式より難しい難読化はなされない。また、if 文を加えても、はじめの加算の演算に条件が存在しない以上、意味のある条件分岐は発生しない。これはある演算が確定的な別の演算に１：１に対応した形で変換されたことによっているため、演算のディジタル変換と呼ぶことにする。

3.2 演算のアナログ的変換方式

3.2.1　方式１

そこで、次に演算を１：N (N≧2)になるように変換する手法を検討する。例として、

x+y

なる演算に対し、複数の変換

x+y

x+y+ε　　(1)

（但しε＝0.00000001 等）

を用意すれば、一つの演算が２種の演算に増加したため、難易度は確実に向上したと見なせる。これらを if 文で分けて意味のある条件分岐にすることができる。

3.2.2　方式２

上の方式は、演算誤差が加わることになるが、倍精度演算や一般には n 倍精度演算にすることにより実行でき、有限の演算回数による誤差の累積は、演算ビット数の増大により吸収可能にできる。

さらに、微小値を切り捨てて元の演算を取り出す手法に対し、下位の桁に正しいデータを埋込み上位桁をダミーとする入れ替えを行なえば、演算精度を保って演算をする必要が出る。

例えば、

x+y に対し、

Ｌ+x/1024+y/1024

(L=1024 等)

とし、適当な場所でＬを除く処理をすれば、下位の桁を切り捨てることができなくなる。

3.2.3　方式３

次は、ＲＯＭ演算ともいえるもので、演算を数表にして結果を与える形にするもので、法則的な解析ができなくなる。数表は誤差を含むものであるため、解析には、他変量解析のような数値計算が必要となる。

例えば、

x+y　(０≦x,y≦10)

なる演算に対し、片方の変数 x は例えば図３のような数値で定義されるアナログ的変換を受けるものとし、中間の値は補間で求めることにする。図３は考えやすくするため、誤差の大きい場合の例を示してある。

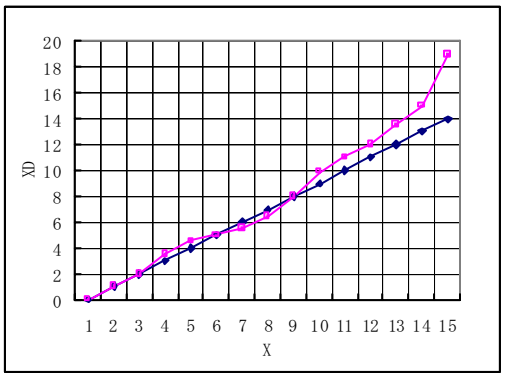

図３　誤差付き変換例

3.2.4　誤差の評価

式(1)に表されるような誤差を難読化の変換のたびに行なう時、その誤差はεとして LSB の±１ビットを与えた場合、難読化変換回数を K 回とすると、その最大値は、K

となる。演算を 32 ビットの整数演算から 64 ビットの倍精度整数演算に拡張した場合、下 32 ビットの演算余裕度が出る。下 32 ビットが飽和するのは、最悪の場合でも、

$$K \le 2^{32} = 4.294967296 \times 10^{9}$$

となる。
従って、LSB の誤差追加により難読化変換を 10 の 9 乗回以上反復的に行なうことができることになる。

4. 埋込みと検出実験

図 2 の構成の電子透かし方式の埋込みと検出実験を行なった。MDFT については、今回は標準の離散フーリエ変換（DFT）の場合のみ行なった。検出器を公開する前提で、埋込みは透かしが有るか無いかを判定するためだけのものとして最小の 1 ビット情報を埋込んである。但し、その 1 ビットを 64 ビットに拡大し、検出では、64 個の検出結果の多数決により 1 ビットを取り出している。拡大は、単に 64 個の異なる場所に同様の手法で繰り返し埋込むことで行なっている。

この方式の埋込みによる劣化と耐性の基本特性は文献[7]等に報告した通り、十分な性能を有している。つまり、1 回の埋込みによる劣化は、信号（ピーク値）対雑音（平均 2 乗誤差）比で 47dB 程度あり、低域通過フィルタ（ぼかし）、ランダムノイズ付加、JPEG 強圧縮などの攻撃に対しても、検出が可能であった。

ここでは、本埋込みソフトウェアで一度埋め込まれた透かし入り画像に別人らが再度透かしを埋め込む時、はじめの透かしが上書きされて消えてしまう効果について調べる実験をした。1 回目の埋込みの埋込みパラメータはその埋込み者のみが知り、またその埋込みパターンは十分多いため、別人が埋込み場所を特定することは困難である。ここでは変換 MDFT は簡単のため DFT のみとしたが、この変換係数だけでも十分なパターン数がある[8,9]。そこで、別人は同じ埋込みソフトウェアを使用するが、その埋込みパラメータはランダムに異なるものを選択したとして、数回から 10 回程度までの多重の埋込みを行なった。

埋込み回数に対する、劣化の例を図 4 に、埋込み回数に対する検出率の変化を図 5 に示す。

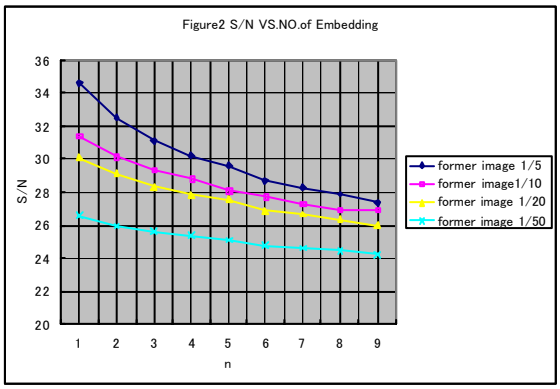

図 4　埋込み回数と劣化(SNR)

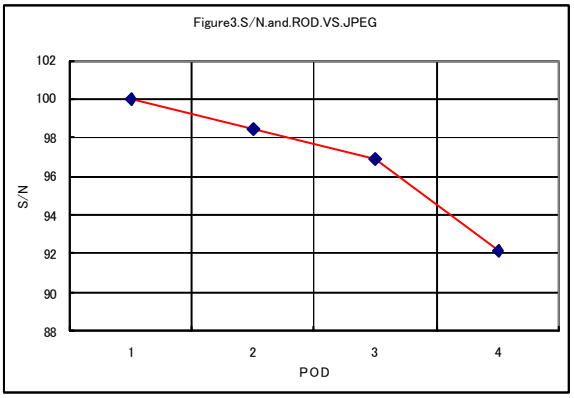

図 5　埋込み回数と平均検出率の変化

図 5 は複数結果の平均値で、埋込んだ情報のうち検出できた情報の割合を表示してある。従って、この数値が 50%以上のうちは、多数決原理により埋込んだ透かしが検出できると判断する。

埋込みは、離散フーリエ変換領域で 8x8 個のサンプルから成るブロックごとに埋込みをしていくため、埋込み回数が増加すると、8x8 のブロックに重なりがでて来る可能性も増加する。重なりが出ると、劣化は少なめになり、一方検出率は低下することになる。これらは少ない結果ではあるが、

埋込み回数に対して、検出率の劣化は平均２～３％であるのに対し、画質の劣化の方は２回目で２～３dB程度と大きい。多数決原理が正常に動作するかぎりは、劣化の方ガ大きくなり、多重の埋込みは画像の価値が損なわれて行き、10回程度までの多重埋込みまでは、多数決原理が動作するような予想が期待できる。また、埋込みを8x8のブロック単位でなく、１サンプル単位の乱数にすれば、埋込みの重なりはよりランダムになり、上書きにより透かしの50%以上を書き換えることができる確率は低いと考えられる。

5. まとめ

検出器ソフトウェアを難読化して公開領域にて不特定第三者の協力に依存して認証を行なう電子透かしシステムの各要素を検証してきた。今回、演算を誤差を含む難読化した演算に変換するアナログ的変換を行なうことより、反復的に10の9乗回程度まで難読化を行なうことができる例を示した。また、従来検証実験に加え、同じ埋込みソフトウェアを使い一度埋込んだ透かし入り画像に対し、再度埋め込んでいく時の上書き作用の影響を調べ、数回ていどまでの上書きの試行では画像の劣化があり、また検出率は保たれる見通しを得られた。

今後は、これらの実験の数量を増やし信頼性を確立すること、切り取りなどのサイズが変化する攻撃への対処、公開する検出ソフトウェアの改竄やタイムスタンプ情報の維持、バージョン管理などが次の段階の課題として考えられる。

文　献

[1]J.Cox, et al., “Secure spread spectrum watermarking for multimedia”, “IEEE Trans. Image Processing, vol.6, pp1673-1687, Dec. 1997.

[2] F. Hartung and B. Girod, “Fast Public-Key Watermarking of Compre...”, IEEE ICIP97, pp.528-531.

[3] T.J.McCabe, “A complexity measure”, IEEE Trans. on Software Engineering, 2(4):pp.308-320., Dec., 1976.

[4] 坂本憲昭、岡本栄二“耐タンパー技術のためのアルゴリズム難読化の一提案”、情報処理学会研究報告 Vol.1998 No.108, CSEC-003.

[5] 門田暁人、高田義広、鳥居宏次“ループを含むプログラムを難読化する方法の提案”、電子情報通信学会論文誌(1997)

[6] 村山隆徳、満保雅浩、岡本英司、植松友彦“ソフトウェアの難読化について”、電子情報通信学会技術報告 ISEC95-25, pp.1-6, 1995年11月(1995).

[7]大関和夫，中島道紀「耐性を極大化した電子透かしシステムの構成と評価」情報処理学会学会、第28回コンピュータセキュリティ研究会、CSEC Vol.2005, No.33, 2005-CSEC-28, pp169-174, March 22, 2005.

[8] kazuo Ohzeki, Michinori Nakajima, Yoshinori Sakai and Hiroshi Harashima, “One Bit Open Watermarking System”, Proc. Picture Coding symposium Dec. 2004.

[9]Ohzeki and Cong Li “Consideration on Variable Embedding Framework for Image Watermark against Collusion Attacks”, Contribution to WaCha June 9, 2005