2005－DPS－122（30）
2005－CSEC－28（30）
2005／3／22

耐性を極大化した電子透かしシステムの提案

大関和夫 1)　　中島道紀 1)　　八十島耕平 2)

1)芝浦工業大学　大学院　電気工学専攻／2)工学部

〒337-8570　埼玉県さいたま市見沼区大字深作３０７

TEL　048-687-5069　　FAX　048-687-5117

E-mail:m102179@sic.shibaura-it.ac.jp

ohzeki@sic.shibaura-it.ac.jp

あらまし：インターネットで各個人が画像・音声の配布をするにあたり，著作権を確保するため，透かし認証の無料化と耐性を最大化する観点で電子透かしシステムを構成した．従来透かしの埋め込みと検出の方式を秘密にするため，透かしの検証により著作権を第三者に対して主張するためには，透かしを公的機関に登録するなどの手続きが必要であったため，事実上透かし挿入検出のために登録経費等が必要となり，個人レベルでは電子透かしによる著作権の主張をすることが困難であった．これに対処するため，検出プログラムを公開し，任意の第三者が透かしの有無を検出できるようにした．これに伴い公開する検出プログラムを難読化しておく処理を追加することにする．電子透かしシステムにはいくつかの評価基準があるが，耐性を最大化するため，埋め込み情報の種類を最小化し，同じ情報を何度も繰り返し埋め込むことにより，埋め込みの冗長度を最大化することを試みた．埋め込みデータは独立と見なし，多数決原理により，透かしの有無を判定する．DFT 領域での QIM 方式に準ずる埋め込みを行い，十分な耐性を確認した．また、難読化の手法を検討し，プログラムの増加量より，複雑度の指標をあげることができた.

キーワード：電子透かし，耐性，著作権，認証，難読化

A Proposal of WaterMarking System with Maximized Resilience

Kazuo Ohzeki1) , Michinori Nakajima1), Kouhei　Yasojima2)

1)Graduate School of Engineering

2)Faculty of Engineering, Shibaura Institute of Technology

307 ,Fukasaku,Minuma,Saitama　337-8570　Japan

TEL　+81-48-687-5069　　FAX　+81-48-687-5117

e-mail:m102179@sic.shibaura-it.ac.jp

ohzeki@sic.shibaura-it.ac.jp

abstract: A new watermarking system which maximizes the resilience and provides authentication method without additional costs for people who distribute their digital image and sound data in the internet. In the conventional methods, embedding algorithm is kept in secret. To insist their copy rights to the others, registering their watermark data to some public institution had been required. this actually charged people registering costs, which made personal watermark embedding difficult. To cope with this, this paper proposes to disclose detection programs. Any third party can detect the watermarks. To carry out this system the detection program is obfuscated. To maximize the resilience, the watermarking system minimizes the embedded information. Assuming the embedded data independent, the majority decision rule authenticates the watermarks. Experiments with the QIM method in DFT region results sufficient resilience and provides higher complexity index than the increasing length of the detection program.

keywords : watermarking, resilience, copyright, authentication, obfuscation

1. はじめに

インターネットで個人レベルでの画像・音声の配布における著作権を確保するため，透かし認証の無料化と耐性の強化を最大化する観点で電子透かしシステムを構成した．従来透かしの埋め込みと検出の方式を秘密にするため，透かしの検証により著作権を第三者に対して主張するためには，透かしを公的機関に登録するなどの手続きが必要であるため，事実上透かし挿入検出のために登録経費が必要となり，個人レベルでは電子透かしによる著作権の主張をすることが困難であった．このため，検出プログラムを公開し，任意の第三者が透かしの有無を検出できるようにした[1,2]．これに伴い公開する検出プログラムを難読化しておくことにする．電子透かしシステムにはいくつかの評価基準があるが，耐性を最大化するため，埋め込み情報の種類を最小化し，埋め込みに際し冗長度を最大化することを試みた．埋め込みデータは独立と見なし，多数決原理により，透かしの有無を判定する．

2．従来の重要な方式

電子透かし化しには多数の方式があるが，本研究に関連した重要な方式を３点取り上げ，概説しておく．

2.1 QIM方式

電子透かしの情報埋め込む方法は，所有者名などのテキストやロゴ画像を直接埋め込む方式に対し，データを量子化することによって，透かし情報を埋め込む方式“ Quantization Index Modulation”(QIM)がある．量子化を一般化し，量子化誤差の解析が B.Chen らによってなされている[3]．データは図１のような量子化パターンで最寄りの代表点に量子化される．量子化点には透かしの有り，無しに対応して２種がある．

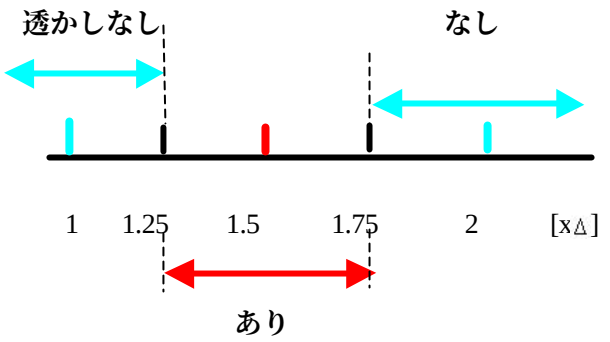


図1. 量子化と透かしデータの有無（QIM 方式）

2.2 埋め込み容量に関する考察

電子透かしに埋め込む情報の量は，画像の場合，画素数と画像信号の分散により定められる[4]．前者は埋め込みに関する標本化の限界から決められ，後者は信号レベルの大きいところにより多くの情報を埋め込むもので，信号対雑音比で規定される．

$$C = W \log_2\left(1+\frac{S^2_{image}}{S^2_{noise}}\right) \quad (1)$$

2.3 PKI 方式による電子透かし化

電子透かしの埋め込みを通信路符号化とみなし，検出を公開鍵暗号方式(PKI)と考える方式が提案されている[5]．

3．提案方式[4]

従来著作権を主張する公開電子透かしは耐性が無いものとして分類されている[6]．電子透かし化がシステムとして成立するためには，目的により限られた資源(劣化要素)を割りつける必要がある．自分で透かし情報を埋め込み，自分で検出をする場合は，方式を秘密にし，耐性を高めればよい．一方，他人に対して著作権を主張したい場合は，相手乃至は第三者が検出を行い，認証できないといけない．第三者にデータの登録を行なうなどが必要となるが検出ソフトを公開することによっても，広い意味で認証が可能な領域に移行したといえる．更に，攻撃と呼ばれる変形に対し，耐性があることが必要であるが，変形の程度が大きくなれば，埋め込み情報は大きく失われるため，耐性が１００%確保されることは難しい．そこで，耐性に関しては，原画の情報が十分残っている状態で評価することが行なわれているが，ここでもその基準を前提としていく．

提案する電子透かし方式は，QIM 方式に準ずる量子化手法によるデータの埋め込みと，検出プログラムの公開を行なうシステムからなる．まず，埋め込み方式について説明する．

図２に提案方式のブロック構成を示す．画質への低影響とロバストネス[7]からフーリエ変換領域での埋め込みを行なう．周波数上での埋込み基準は，視覚的な検知限界(Just Noticeable Difference: JND)より大きい周波数成分に対して埋込みを行い，それより小さい周波数成分に対しては埋込みを行なわない．実測によれば，通常の画像で 1000 ビット程度の埋め込みは十分可能だが，埋め込み位置は画像によって異なるため，本稿では低域から中域の周波数成分が常に大きい部分の 64 ビットを１単位として最小の検討を行なう．64 ビットの埋め込み位置は周波数成分上の 8x8 点の固定ブロックとすることもできるが，更に広い埋め込み可能領域のうちからランダムに選んだ 64 ビットにすることができる．耐性を極大化するため，埋め込み情報の種類を最小化し１種とし，埋め込み有を１，無しを０とする．埋め込み情報容量に対して同じ埋め込み情報を繰り返し埋め込む．埋め込み情報は独立と仮定し，1/2 以上の情報が検出された時，多数決の判定により透かし有りと検出する．

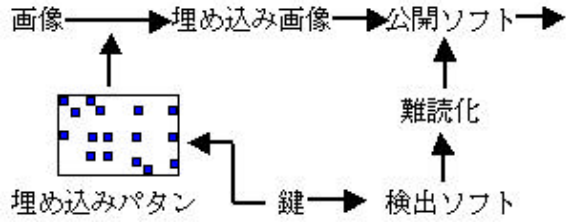


図２　提案する電子透かし化しシステム

埋め込み容量をB，埋め込み可能な位置の数をMとすると，埋め込みパタンの数は ${}_{M}C_{B}$ 個となり，これが鍵の数になる．鍵の種類が膨大な数になるので，方式を公開しても鍵を計算量的に解析不能にすることができる．

今回は２つの透かし埋め込み方式を提案するが，基本となる方式は 3.1.1 である．

3.1.1　周波数成分に対する k 個(以下 k=64 の場合で示す)の透かし埋め込み

透かしの埋め込みの流れを図 3 に示し，その説明を以下に示す．

Step1：Input Image のＹ成分に対して DFT を行い周波数成分に変換．

Step2：周波数成分の高域と低域の中からそれぞれ透かしを埋め込む周波数成分計 64 個を選択し８×８ブロックに配置する．64 個は図２のようにランダムにとることも可能だが、ここではブロックとして揃えてとる場合で説明する。

Step3：取り出されたブロックに対して，透かしを埋め込む．

Step4：取り出されたブロックの周波数成分を各々元の位置に戻す．

Step5：周波数成分全体に対して IDFT を行う．

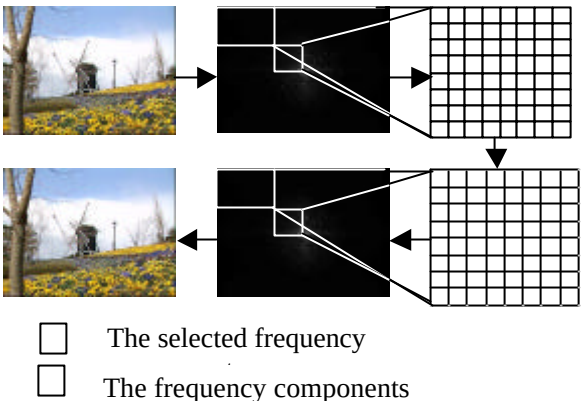


図３．電子透かし埋め込み方式(2.1.1)

この方式では，画像全体だけでなく，画像の一部に電子透かしを埋め込む事も出来る．例えば，オブジェクトがある位置に対して上記の処理を行えば，オブジェクトに透かしを入れることが出来る．

3.1.2　小ブロック単位で少数の透かしの埋め込み

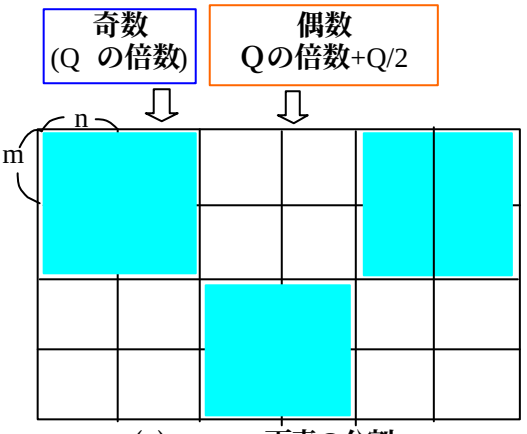
透かしの埋め込みの流れを以下に示す．

Step1：Input Image を n×m サイズのブロックに分割．

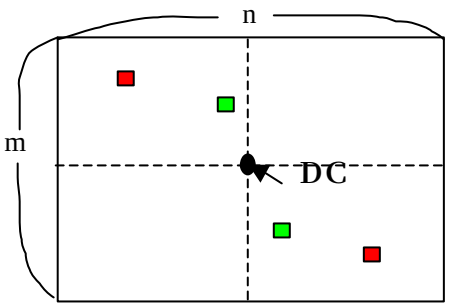
Step2：分割された各ブロックに対して DFT を行い周波数成分に変換．

Step3：４つのブロックを１固まりとして，同じ量子化処理を行なう。(0，0)，(1，0)，(0，1)，(1，1)番目のブッロクの周波数成分の高域と低域(各１成分)に対して，ステップサイズ Q で量子化する．固まりが偶数番目なら量子化後 Q/2 を加える(図４)．

Step4：各ブロックに対して IDFT を行なう．



(a)　n×m 画素の分割



(b)　各 n×m 画素ブロックの DFT 領域処理

図４．ブロック分割と透かし挿入位置の例

3.2　電子透かし検出

透かし判定の流れを以下に示す．

Step1：Input Image に対して DFT を行い周波数成分に変換．

Step2：偶数番目か奇数番目かを判定．

Step3：特定の範囲以内にあるかを判定．(この判定は，偶数番目なら，「Q の倍数+Q/2」を基準に±Q/4 の範囲内にあれば透かし有り，奇数番目なら，Q の倍数を基準に±Q/4 の範囲内にあれば透かし有り，

と幅を持たせている(図5))．

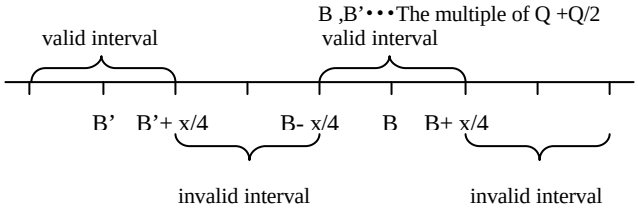


図５　:埋め込まれたデータの検知範囲

3.　実験結果

実験には flwr(704×480 画素，256 階調)を用いた．透かし埋め込み後の PSNR を表１に，透かしの残存率を表 2 に示す．表では，3.1.1 方式で画像全体に透かしを埋め込んだもの(Q=80，高域透かし埋め込み位置(0，0)，低域透かし埋め込み位置(230，340))を 3.1.1(a)，表 2 の画像処理は Paint shop pro 7 を用いた．画像処理は Low pass Filtering-Diameter 3(以下 Low)，Noise Addition10%(以下 Noise)，JPEG Compression-Level30 (990KB→54.7KB)(以下 JPEG)を行った．

表１．電子透かし埋め込み後の PSNR

System	2.1.1(a)	2.1.1(b)	2.1.2
PSNR	47.4768	38.6019	47.7834

表２．電子透かしの残存率

System	Attacks	high region	low region
3.1.1(a)	Low	32/64 (50%)	64/64 (100%)
	Noise	61/64 (95%)	59/64 (92%)
	JPEG	32/64 (50%)	64/64 (100%)

Noise 以外の画像処理について，高域は透かしが消え易く低域は透かしが消えにくい事がわかる．これにより，画像処理などの検知が可能になる．表 2 の 3.1.1(a)と 3.1.1(b)より，画像処理耐性，SNR ともに埋め込む周波数領域の大きさ，Q にほぼ比例していることがわかる．

4．劣化（アタック）との関係と評価

埋め込みデータが種々の処理で劣化していく場合，過大な変形で，透かしが全く検出できなくなる．これに対して，本稿では，劣化は，原画像が高解像度と認識できる程度に保存されているものと仮定し，したがって平均の劣化度は視覚的な検知可能な S/N で 30-35dB 程度以下にはならないものともみなす．その上で，尚且つ過大な変形があり，埋め込みデータが失われる時，透かし検出方式の有効性を調べる．

4.1　劣化と正解率との関係

まず比較的変形が小さいときは，多数決により埋め込みデータのうち過半数のデータは有効で，透かし有りの結果は正しい．次に劣化が過大になり，埋め込みデータの過半数が有効でなくなった場合は，高域の検出成分の劣化から透かし無しの判定になる．表３に劣化と検出との関係を示すが，劣化が小の時は第１種の過誤が発生する確率は，きわめて小さい．

量子化誤差は，一様分布すると仮定できる[8]．まず，量子化幅を Q，劣化（アタック）の変形の最大振幅を d，q=Q/2，正解率を R とすると、

$d \le q$　の場合エラーはないので、

$R=1.0$　(2)

となる．

$q \le d \le 3q$　の場合，q までの幅のデータは正解となり，q から 3q まではエラーとなるため（図６参照），正解率は，

$$R = \frac{q}{d} \qquad (3)$$

となる．同様にして，

$3q \le d \le 5q$　の場合は，

$$R = \frac{d+(d-3q)}{d} = \frac{d-2q}{d} \qquad (4)$$

$5q \le d \le 7q$　の場合は，

$$R = \frac{3q}{d}$$

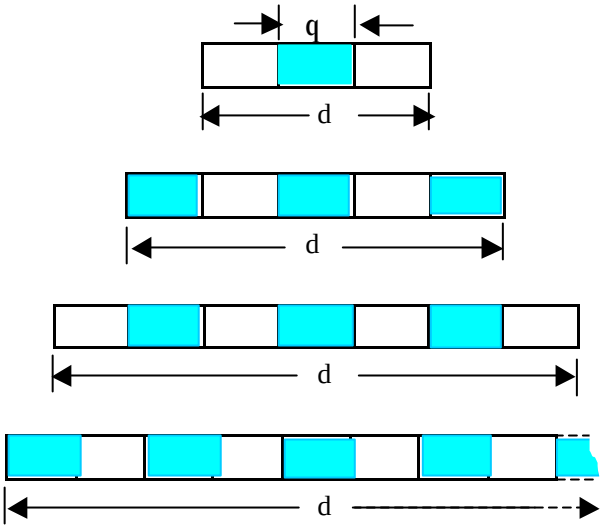


図６．半分の量子化幅 q と変形の最大振幅を d の関係　は正しい領域，　はエラー領域を示す．

$7q \le d \le 9q$　の場合は，

$$R = \frac{3q+(d-7q)}{d} = \frac{d-4q}{d} \qquad (5)$$

となる．これをグラフにすると、図７のようになる．d の増加に伴う各段階で劣化と誤検出が交互に

現れる様子を表３に示した．２階の誤りにより正解とエラーが検出されることを第３種の過誤として説明している．

次に，透かしを埋め込んだことによる劣化はＳ／Ｎ=50ｄＢである．Ｓ＝255 とすると，Ｎ＝0.80638 である．これは８ｘ８=64 点の雑音で，全範囲に拡散すると，704×480/64＝5280 分の１に相当する．

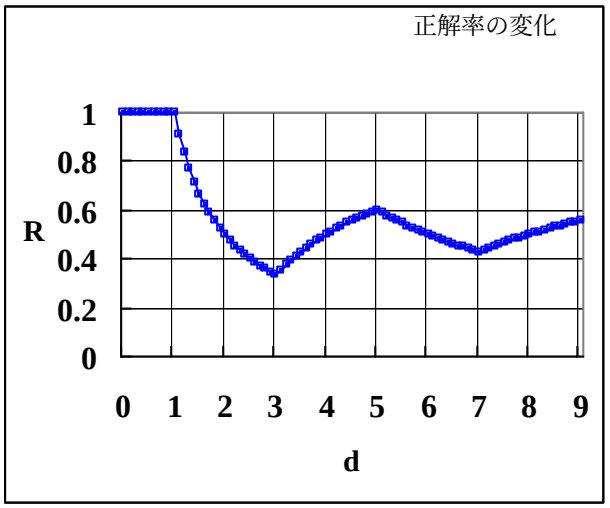


図７．　d と正解率Ｒの関係.

4.2　鍵の個数

透かしは，図１のようなランダムパターンで挿入したり，3.1.1 の Step2 で示したように 8×8=64 個をまとめて扱う場合，3.1.2 の図４し示したように，小ブロックに分散して入れる場合がある．ここでは，図１のようなランダムパターンを作って透かしを挿入する場合の透かしのパターンの数を鍵の数と定義してその概数を求める．

透かしの鍵の数は，

$$ {}_{M}C_{B} \qquad (6) $$

但し，Ｂは DFT 領域で，透かしを挿入可能な位置点の数，Ｍは実際に挿入する透かしの個数である．

画像サイズが 720×480 画素の場合，Ｂは 200×300，またＭは 64 として上記の実験に適合した透かしを挿入できる．このとき鍵の数は，

$$ {}_{60000}C_{64} \cong 4.83\text{x}10^{216} \cong 2^{719} \qquad (7) $$

となる．この式から，700 ビット程度の鍵を設定することが可能であることがわかる．また，埋め込み方式や，難読化した検出プログラムを公開してもそれらを解析して透かしを除去したり，改変するのは

計算量的に不可能になることがわかる．

5.　検出プログラムの難読化処理

透かしを埋め込んだ画像と伴に，検出プログラムを公開し，任意の第三者が透かしの有無を検出することができるようにする．検出プログラムは難読化の処理を行い，埋め込みの位置情報や量子化特性を解読されないようにする．

難読化に関しては，文献[9]に多数の方式が紹介されている．ここでは，それらの内から，多重ポインタによる変数の隠蔽化，条件分岐ないしは並列処理により処理を拡張し難読化を図る手法を用いた．

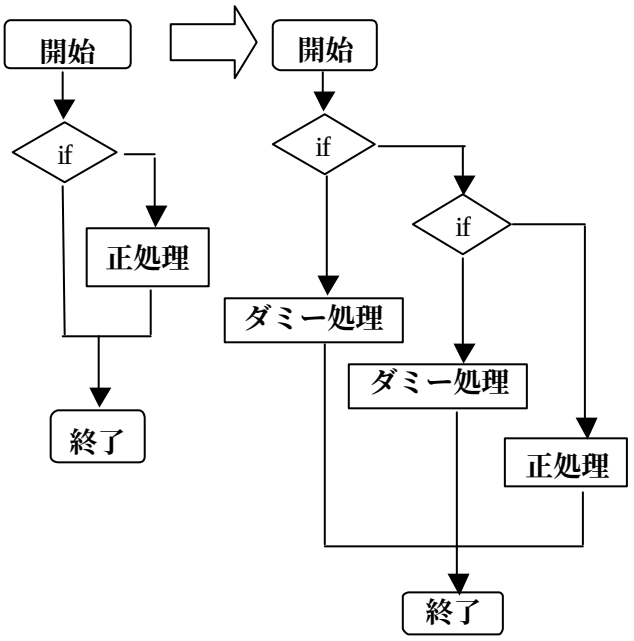


図８．　if 文の追加による難読化

図８は if 文の追加による処理の複雑化[10]の例で，プログラムを解読する際の手間が増加する．図９は条件分岐を増やし，処理の種類が８倍に増加する．後段で結果を参照しその結果に基づいて判断のある統合処理がなされると，参照された処理は解析の対象となり，解読の手間が増大する．この処理の種類の拡張はこのような構成を機械的に追加していくことにより，任意に増加させることができると考えられる．

実際の透かし検出プログラムに対して，難読化処理を行ない，その難読化の程度を McCabe の指標，すなわち
「プログラムの複雑さは，制御構造の複雑さで定まると」の考えで評価した．

この複雑さは基本パスの数で表される．（if 文、for 文、while 文等）複雑度 V(G)はプログラム中の

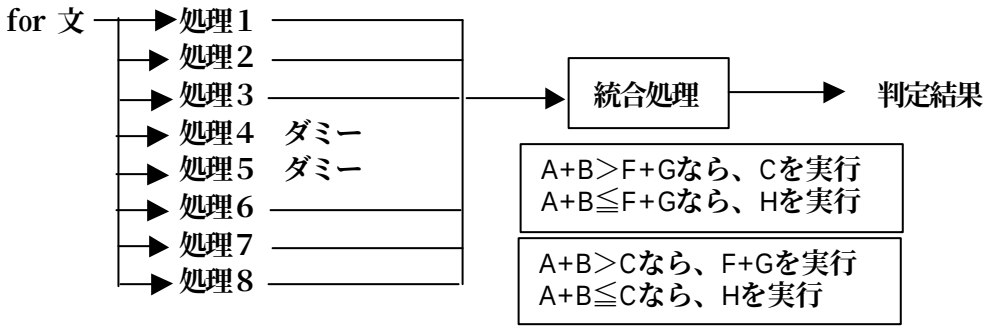


図9．　分岐処理と統合よる判定

表4　難読化の評価

	難読化前	難読化後		難読化前	難読化後	
関数名	総行数	総行数	比率	複雑度	複雑度	比率
main	144	208	1.44	23	44	1.91
hantei	141	978	6.94	17	315	18.53
Quantization	29	53	1.83	7	11	1.57
sukasi	19	34	1.79	6	9	1.50
change	11	37	3.36	3	11	3.67
change2	24	48	2.00	5	11	2.20
合計	368	1358	3.69	61	401	6.57
総合計	593	1583	2.67	97	437	4.51

判定条件の数をπとすると
V(G)＝π＋1
で求められるとされている．
　この複雑度の評価結果は，表4のようになっている．透かしの判定部に特に難読化の処理を多く入れてある．総合的には，プログラムの行数の増加より難読化の指数の増加の割合が多くなっている．

5.むすび

　耐性を極大化した電子透かし化しシステムを提案した．耐性を極大化するため，埋め込み情報を最小化し，1ビットとした．透かしを埋め込む方式は数多くあるが，個人が透かしを埋め込んでもその著作権を主張するために認証を行なうには，従来第三者の公的機関に登録するなどの手続きが必要となり，経費がかかった．これに対し，提案方式では透かしの検出プログラムを公開し，任意のユーザが透かしの有無を検出できるシステムにすることにより，個人が無料で透かしを入れた画像をインターネットなどで配布することが可能になる．DFT 領域で，QIM 方式に基づく埋め込みを行い，具体的耐性評価を行い，十分な耐性を確認できた．また，難読化を行なったうえ，公開する検出プログラムの複雑度を評価し，プログラムの行数の増加より難読化の指数の増加の割合が多くすることができた．

謝辞：本研究は芝浦工業大学のプロジェクト研究助成により行なわれたものである．

＜参考文献＞

[1]K. Ohzeki, M.Nakajima, Y.Sakai, and H.Harashima, “One-Bit Open Watermarking System”, Proc. PCS. S8-14, Dec. 2004.
[2]中島道紀,大関和夫, “周波数領域での多数決による強固な電子透かし方式“, 2004 年映像メディア処理シンポジウム(IMPS)予稿 2-20,
[3]B.Chen et al, “Quantization Index Modulation: ・・・・,” IEEE Trans. IT, Vol.47 no. 4, pp.1423-1443, May 2001.
[4]Zhang Fan et al, “Capacity and Reliability of ・・・・”, Proc of AGEC EPRL pp.162-165, 2004.
[5] F. Hartung and B. Girod, “Fast Public-Key Watermarking of Compressed Video” , IEEE ICIP97, pp.528-531.
[6]Christophe de Vleeschouwer, Jean-Francois Delaigle, and Beboit Macq, “Invisibility and Applicaion Functionalities in Perceptual Watermarking –An Overview”, Proceedings of the IEEE, Vol.90, No. 1, Jan. 2002.
[7]J.Cox, J. Kilian, F.T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia”, “IEEE Trans. Image Processing, vol.6, pp1673-1687, Dec. 1997.
[8]酒井 善則, 吉田 俊之,　映像情報符号化」オーム社　2001.
[9]Christian Collberg, Clark Thomborson, and Doulas Low, “A taxonomy of obfuscating transformations, technical report #148 Dept. of Computer Science, The Univerity of Auckland., New Zealand.
[10] 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)