

表関数による難読化方式を用いた電子透かし埋込方式

watermarking system with obfuscation method using table function

魏 遠玉

Yuanyu Wei

芝浦工業大学

Div. FCS, Grad. School of Eng. Shibaura Institute of Technology

大関和夫

Kazuo Ohzeki

機能制御システム専攻

大学院

1 はじめに

電子透かしの埋込みや検出のプログラムを難読化することによって、解析によって埋込みの方式を推定することが難しくなる。計算量を制御して処理量を多くして難読化する手法は[1]、通常の計算も増加する問題がある。難読化の研究には、Chowらのアフィン変換の乗算部を表化する[2]手法や大関らのROM構想[3][4]がある。本報告では、埋込みや検出処理のすべてを1つの表(ひょう)にして、入力と出力以外の全てを隠蔽する。これにより、計算をあらゆる手がかりが隠れることになる。電子透かしの誤差評価、耐性評価などを行っていく。

2 難読化方式

埋め込み者が作る検出器を難読化して、公開し、動作はするが、処理のアルゴリズムが解析しにくい形にする。難読化に関しては、まず、周波数変換と量子化を行う計算処理に表関数を用いて演算処理をする。離散コサイン変換のように周波数領域に変換し、低中域の一部にある幅の量子化を行い、透かしとしてのマークとするものである。

次に、逆解析の計算は、入力と出力の関係が得られるにもかかわらず膨大なものとなる。ROM「Read Only Member」化すれば、入力値と出力値の対応関係を多数求めても、大規模な多変数の解析となりうる。最後、表関数には、4画素の画像配列に対して、電子透かしを埋込む処理と検出する処理のプログラムを構成し、次に難読化したものを構成する。

図1は電子透かしの埋込み処理である。計算を表にするため、変形離散フーリエ変換の次数を4に制限して、変換係数を変化させることで埋込み手法を隠蔽するものである。入力画像のモノクロ成分4画素を1ブロックとし、離散コサイン変換によって周波数領域へ変換する。中間周波数に相当する2個目3個目の成分を所定の特性で量子化器Quantで量子化し、DCTで逆変換され、画像に戻す。

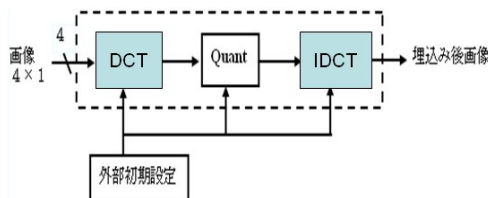


図1 4次元電子透かしの埋込み処理

図2は4画素のデータの変換を16ビットから24ビット入力で16ビット出力の3個の表により構成する例を示す。各表の16ビットの出力は出力前に値の並べ替えがなされ、この途中結果の値を観測しても関数関係は推定できない。量子化後の逆変換も同様の構成で実行できる。表関数の容量の見積もりを表1に示す。ROM1は128KBで、ROM2,3が16MBになる。量子化器QuantはROM1と同容量で、逆変換は正変換と同じである。以上より、埋込み処理の総容量は128MB強となる。検出の方は、48MB×4=192MBで構成できる。

表1 データ容量の見積もり

	入力	ROM1	ROM2	ROM3
入力アドレス	8×4 (32)	16	24	24
出力	1	16	16	16
容量 (bits)	2^{16} = 65536	$2^{16} \times 16$ = 1048576	$2^{24} \times 16$ = 16777216	$2^{24} \times 16$ = 16777216
概数	64KB	128KB	16MB	16MB

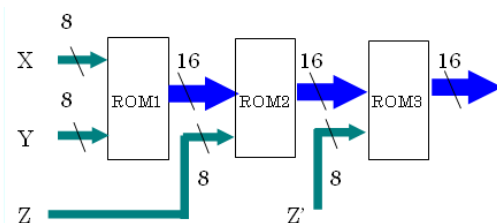


図2 4次元変換のデータフロー

3 4次元変換

4次のDCTとして、(1)式に変換を、(2)式にその逆変換を示す。

$$DCT_4 = \begin{bmatrix} 0.5000 & 0.5000 & 0.5000 & 0.5000 \\ 0.6533 & 0.2706 & -0.2706 & -0.6533 \\ 0.5000 & -0.5000 & -0.5000 & 0.5000 \\ 0.2706 & -0.6533 & 0.6533 & -0.2706 \end{bmatrix} \quad (1)$$

$$IDCT_4 = \begin{bmatrix} 0.5000 & 0.6533 & 0.5000 & 0.2706 \\ 0.5000 & 0.2706 & -0.5000 & -0.6533 \\ 0.5000 & -0.2706 & -0.5000 & 0.6533 \\ 0.5000 & -0.6533 & 0.5000 & -0.2706 \end{bmatrix} \quad (2)$$

4 実験



図3 実験画像 (1013kb, 720×480 画素, モノクロ)

表3 埋込みと検出データ(a-d は画素値)

	配列位置	1	2	3	4
a	原画像	48	43	43	45
b	埋込み後	57	47	39	36
c	JPEG 1/20 圧縮	51	44	34	44
d	JPEG 1/25 圧縮	46	46	46	32

図3の画像の(299,199)から横に4画素抽出する4個を変換して,2個目に埋込む.横に並ぶ4画素について,式(1)の変換を用いる場合を示す.表3に埋込み処理結果と検出処理の一部を示す.埋込みは4カ所しか無いため,交流成分の絶対値平均最大の第二位置に行う.他にDCに入れる等も可能である.変換後の第二位置に変更を施すもので,0は $lq=16$ にして埋込みを示している.埋込み後のデータに対し,JPEG圧縮を行って劣化した結果をc,dに示す.検出は,再度変換のみを行い,第二成分の値が,±8の範囲にあれば,検出されたと判定する.

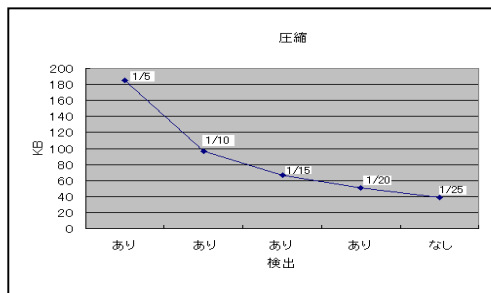


図4 透かしの耐性評価(a)(4次DCT,JPEG圧縮)

実験環境:ソフトPaintShopProでJPEG圧縮する.ソフトウェアMicrosoft Visual C++ 2008 Express Edition.

図4(a)はJPEGによる電子透かしの耐性である.横軸は検出の判定であり,縦軸は画像の容量(kb)である.圧縮率は1/20まで透かし情報が残っている.

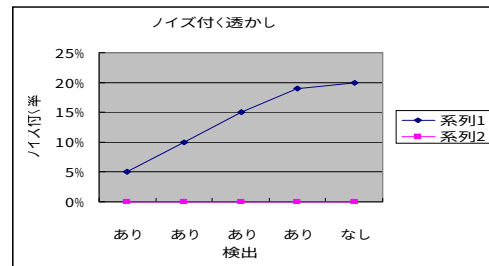


図4 透かしの耐性評価(b)(4次DCT,ノイズ付加)

図4(b)はノイズ付加の透かしの耐性である.横軸は検出の判定であり,縦軸はノイズ付加率である.画像に全体的にノイズを加える.ノイズ付加率は19%まで透かし情報が残っている.静止画像に透かしの埋め込み手法により,16の倍数での変更すれば,数値の変化もそれほど大きくないので,ほぼ原画像と見た所ではわからない.変更によって,値が大きく変わると,変更の単位が大きくなればなるほど,透かし情報を埋め込む際の値の変化も大きくなり,画像の変化も大きくなった.画像(透かしあり)を圧縮(JPG)しても,ノイズを付けても,透かしが残っているから,表関数を用いて埋め込む変更の手法で透かしの耐性があることがわかった.

5 考察.結論.今後

表関数を用いて,DCTを用いた計算の手法を隠蔽した電子透かしの埋込み器と検出器を構成した.4次の変換により,埋込み位置を画像の内側に設定できるため,画像の周辺部を切り取る様な攻撃にも耐性があり,基本性能が確認された.

埋込み位置では,中域の成分が現れる様なものに変更することにより,より効率が上がり,耐性も向上すると考えられる.検出器は128MBで有るため,さらに埋込み画素のブロックサイズ4を拡大することが可能である.難読化の種類は,形式的には,入力アドレス数である24ビットになっている.演算処理の種類は,未知のパラメータを多数含む非線形の関数とすれば,数値計算による推定の解析演算量は膨大になる.今後は,この次数を増加させる方がよい.電子透かしの埋込みと検出のソフトウェアの難読化では,埋込み方式である関数の形式乃至は埋込み処理の形式まで判明しないと,埋込みを除去することができない.

参考文献

- 1) 魏遠玉「読化を施した検出器公開型の電子透かしの計算量」IMPS 1-6-14, 147-148, 2009, 10
- 2) Stanley Chow, "White-Box Cryptography ...", LNCS2003, Volume 2595/2003, pp, 250-270.
- 3) 大関和夫, 叢力, 「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」CSEC-32, pp, 61-66, 2006年3月.
- 4) Yuanyu Wei and Kazuo Ohzeki, "Obfuscation Methods with Controlled Calculation Amounts and Table Function" MMAP pp, 775-780 Oct, 2010.