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

2008－CSEC－42（40）
2008／7／25

疑似的な一方向性関数を用いた電子透かし

大関 和夫　魏 遠玉‡
芝浦工業大学大学院電気電子情報専攻 〒135-8548 東京都江東区豊洲3-7-5
E-mail: ohzeki@sic.shibaura-it.ac.jp, ‡ m108048@ sic.shibaura-it.ac.jp

あらまし 電子透かしの認証に対して，「Inversion Attack」といわれる攻撃手法がある．これは，一旦電子透かしを埋込んだ後にその電子透かしの存在を無効にする手法である．電子透かしの埋込みが加算演算であり，逆演算である減算が存在すれば，Inversion Attackは可能とされている．そこで，加算は可能だが，減算は困難性が高くなる一方向性関数の性質を有する埋込みを行なえば，Inversion Attackは抑圧できる．本研究では，この一方向性関数を作り出すため，まず疑似一方向性関数を定義し，その埋込み後の劣化と耐性について検証した．特異値展開(Singular Value Decomposition)を用いた疑似一方向性関数により，埋込む手法を提案し，その耐性を計算機実験により検証した．画像のサイズが小さいと電子透かしの埋込み情報量が少なくなるが，256x256画素程度で従来方式と同等程度の性能があり，500x500画素以上ならば，従来方式よりかなり高い耐性を有することが確かめられた．主に疑似一方向性関数とＳＶＤを用いた電子透かしとその耐性について述べる．

キーワード Watermark, One-way function, SVD, Robustness, Inversion Attack

Watermarking Method with a Quasi-One-Way Function

Kazuo OHZEKI and Engyoku GI‡
Dept.of EE and CS, Graduate School of Engineering. 3-7-5 Toyosu, Koutou-ku, Tokyo 135-8548 Japan
E-mail: ohzeki@sic.shibaura-it.ac.jp, ‡ m108048@ sic.shibaura-it.ac.jp

Abstract This paper describes the one-way function for use in an image watermarking to improve authentication ability. The one-way function is popular in cryptography. The one-way function can prove encrypting security. The existence of the one-way function has not been proved yet, while public key encryption procedure is widely used in practical commerce. The authors proposed quasi-one-way function, which is weakly defined for practical use. Difference between the strict one-way-function and the proposed quasi-one-way function is discussed. Applications of the quasi-one-way function to image watermarking are shown. Robustness of the proposed watermarking method is high..

Keyword Watermark, One-way function, SVD, Robustness, Inversion Attack

1. はじめに

電子透かしの埋め込み処理過程を一方向化できればセキュリティの向上が図れる．電子透かしのように埋め込みビット数に制限があり，伝送路としての品質が確保されていないメディアを介するシステムに於いては論理的な体系を構築するのが難しい．完全なるセキュリティ性や非解読性を確保することが難しいため，不完全ではあるがある程度の計算コストがかかることをもって防衛力とする方式を考えることが実用的である．そこで，埋め込みビット数と，誤り率が一定の値まで確保される事が保証されていると仮定し，有限の枠組みの中で，演算量の大小を評価してコスト表示するような方式が有効である．電子透かしの場合埋め込み処理の複雑化，検出ソフトの難読化，埋め込み手続きの一方向性の強化などが考えられる．

電子透かしの攻撃法として，Inversion Attackがあるが[1]，これは電子透かしの埋め込みが原画に対する変化分を加算したことによっている事から，他の加算を埋め込みの後から宣言することが可能であることが原因となって実行される．従って，基本的には加減算を基本とする全ての演算領域で実行可能となる．そこで，加減算を文字通り行わないような演算領域を定義すれば，その領域範囲においては，Inversion Attackが難しくなると考えられる．そこで，筆者らは，特異値展開の結果が0と正数の特異値に展開され，負の数が現れないことを利用した，特異値展開領域での埋め込みを行う条件を付した電子透かしの埋め込み方式を提案して，その耐性の検討をおこなってきた[2]．

特異値展開（SVD）は画像の要素から成る行列の積から求まる対称行列を行列積により対角化し，非対角の成分が0になるような直交行列を求めることである．0となる非対角成分に透かし信号を重畳することは，一方向的加算演算であり，いわゆるInversion Attackへの対策として有効である．Inversion Attackに関してはいままで多くの研究がなされてきたが，画像でなく乱数系列への埋め込みや，誤り感度が高く使用ができそうもない暗号化，ゼロ知識証明を直接組み込んだものが発表されて来たが[3]，有効なものはほとんどな

いと考えられる．

以下，画像情報と電子透かしの埋め込みの関係を再考し，電子透かしの問題点を再確認する．次に疑似一方向性関数の提案を行い，SVD 電子透かしとして適用する場合の手法と，埋め込み例，耐性評価について述べる．

2. 画像情報と電子透かし

画像の電子透かしは画像のサイズが小さため，埋め込まれるビット数も少ない範囲に留まる．また，攻撃は伝送路エラーと考えた場合，高い誤り率に相当するものになる．従って，電子透かしの埋め込みにより，埋め込まれた透かし情報のみから認証性を確保するのは難しいと考えられる．そこで，耐性に重点を置き，ある程度の少ないビット情報のみが得られるとし，認証性等の機能を外部化することにより，電子透かしの機能を確保し，更に認証性を確保していく事が可能と考えられる．表 1 は画像の処理により付加される情報量，変化（劣化）とセキュリティ性の関係を示すものである．WM2 は WM1 よりセキュリティの高いものとする．JPEG 等圧縮は劣化のある圧縮で，復号手法の不明な独自方式を想定し，暗号化は原画像を隠蔽し，所有者しか閲覧もできないもので，他の圧縮も同様に画像を直接見れないものとし，画像の販売などの分野で使用される．

表 1．処理と情報量，劣化，セキュリティ性の変化程度の異なるものを 1 ランクずつ変えた

	情報量	劣化	セキュリティ
アナログ	0	0	0
デジタル 8bit	1	－1	0
WM1	1	－2	2
WM2	1	－2	3
ロスレス圧縮	0	0	1
JPEG 等圧縮	－1	－1	1
暗号化	0	0	4

次に，電子透かしに埋め込む情報の量に関しては，画像の場合，画素数と画像信号の分散により定める手法とがある[4]．前者は埋め込みに関する標本点数Mの限界から多くともM／2と決められ，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，次のように信号対雑音比で規定される．ここで，W＝M／2 であり，σimage は画像の局所分散に対応した noise visibility Function(NVF)から求まる σ noise は変形の程度を表す．

$$C = W \log_2 \left(1 + \frac{\sigma_{image}^2}{\sigma_{noise}^2} \right) \qquad (1)$$

実際の埋め込みビット数は，攻撃に対する耐性を確保するため，この値より大幅に削減される．透かしの埋め込みと検出を通信路符号化とみなし公開鍵暗号方式（PKI 方式）になぞらえて定式化した，方式が提案されている[5]．しかし電子透かしシステムを考える場合は，理想的な骨組みにおいてはシステム自体が 1 ビットでも壊れると，全体の仮定が崩れる．耐性を十分確保する必要があり，冗長度を最大にして埋め込みビット情報は最小化する必要がある[6]．

また，耐性の程度は，埋め込み画像がその画像品質を保つ程度に劣化が小さい範囲で検出に必要な情報が100%残り，画像劣化が大きいと判定できるような劣化の下には埋め込んだ透かしが失われ，つまり耐性が無い状態になっても仕方がないというコンセンサスがあるものと考える．

2.1 Inversion Attack

図 1 に示すように，原画像 G に透かし W を埋め込む処理は，画像信号値に透かしの成分を加算することになり，埋め込み後は Gw=G+W となる．この結果にに対し，別の攻撃者が同一の埋め込み手法で生成した別の透かし成分 W'を用意し，Gw'－W"を新たなる原画像と見立て，それに透かし W"を埋め込んだことにすれば，（Gw－W"）＋W"が攻撃者の透かし W"が埋め込まれた画像となる．これは Gw と一致しているので，任意の透かし埋め込み画像に対して，別の者が別の透かしを入れていたと主張ができることになる．これが Inversion Attack で，単純加算で埋め込まれた画像に対しては常に成り立つ攻撃である．そこで，埋め込みが単純加算でないもの，又は，埋め込みの処理系を単純加算が無い領域に変換するなどして行う，などの工夫により，Inversion Attack を回避するようにする必要がある．

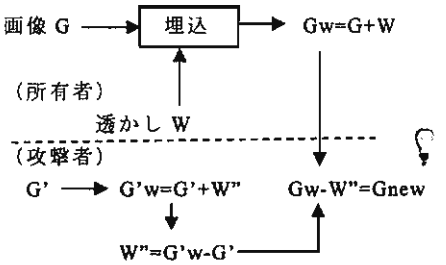


図 1　Inversion Attack の動作

2.2 認証性

電子透かしの認証は，検出された透かし情報が，真にその画像から検出された手続きを行ったという証明

や，検出された透かし情報が正しかったことの証明を行う必要がある．手続きを公開すれば，検出や埋め込みの過程が分かる元になり，そこから透かしが分かれば，それ以後透かしを除くことができることになる．また，検出された透かしが正しいものである事の証明を公開すれば，また，その透かし情報から透かしを除去した画像を作れることになるため，本来，これらの情報を公示せずに証明を行う必要がある．証明にゼロ知識証明を用いた電子透かしが提案されているが[3]，画像の代わりに乱数データを仮定するなどしており，画像に埋め込む方式は見当たらない．誤り率の高い状況で，限定されたビット数しか無い電子透かしにおいて，公開鍵暗号とゼロ知識証明を用いた認証系を構築するのは困難度が高く，当面実現性が無い．そこで，webでの画像公開時に著作権を確保するようなゆるやかな基準の応用に対して，完全性は無いが，攻撃には一定のコストがかかるような規格化ができるアナログ的な電子透かしを考え実用的に使用する事をめざす事が有効と考えられる．ここでは，完全無欠の認証性では無く，一定量の計算コストを表記するコスト付きで有限の認証性のある透かし方式を検討する事にする．認証はU,Vを示す，又は第三者に立ち会いを依頼するなどのone-time型を当面使うことにする．

2.3 埋め込み後の信号処理

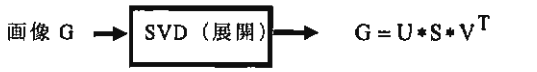
電子透かしを画像メディアの販売流通における著作権保護という観点で考えると，無限に広がる保証をするため完全な認証性を確保する必要性が出てくる．そこで，埋め込みビット数の確保や認証性の確保のため，埋めこみ画像や圧縮後の画像，暗号化された後のファイルに対し，埋めこみなどを意図した信号処理を施していく事が検討されている[7]．表1に示した圧縮や暗号化，透かし埋込み等を行なったあと，信号処理処理を加える手法を検討している．ある種の加算や乗算が準同型の演算として定義可能である事が示されている．しかし，具体的に有効な実例の提示には至っていない．

本報告では，企業などが高い認証性を必要とする仕組みを電子透かしに組み込むような応用では無く，個人がホームページに画像を公開する時に，自分で納得できるような程度ではあるが，一定限度の認証性のある電子透かしを埋め込むための方式を検討することにする．公開鍵暗号の基盤となる一方向性関数については，現在の研究成果では十分大きな素数では計算不能であるとの仮定の下に，証明はできないまま，広く実用化が進んでいる．同様に電子透かしについても，疑似的な一方向性関数を作っていき，完全性を外した有限の中での検討にすれば，その中で厳密な議論を開始できるという効果が期待できる．

3. 画像への埋めこみに関する一方向性関数

3.1 疑似一方向関数の導入

電子透かしの埋込み過程における一方向性とInversion Attackの関係を検討する．ここで一方向性を分離して考えるため，透かしWを示してその逆演算の難易度を考えることにする．実際の運用では，常時公開はしないようにしてもよい．必要な電子透かしWと埋込み後の画像Gwが与えられた場合，埋込み関数fに対する逆関数は加算の反対として，容易に求まる．また，周波数領域での埋込みを行なう方式でも，単にフーリエ変換するだけの基本的な方式においては，周波数領域での透かしW_Fが加算されていると見立てれば，その逆演算を行なうことができる．電子透かしWが与えられた時，それが加算によるものである時，埋込み処理（加算）関数の逆関数（減算）が容易に求まる．通常画像は0-255の整数で表現された数値であるため，如何なる透かしも何らかの加算として表される．そこで，最終的には加算であっても，その透かしがある拘束条件の領域に変換された後に埋め込まれるものであれば，示された透かしから，画像領域での透かしを求めることが困難になる．この考えを行なっているのが特異値展開(SVD)領域における電子透かしである[2]．図2にSVD電子透かしの構成を示す．画像Gから求まる展開行列U,Vにより対角化がなされる．展開後得られる行列Sは対角行列で，対角線上に特異値が並び，非対角成分は0である．そこで，非対角成分に非0の値を持つ透かしW_Sを加算し，U,Vで逆変換（合成）して得られた画像Gwを考える．このGwを再度特異値展開すると，U,Vとは異なる展開となり，そこで透かしW_Sを差し引いても原画像は得られない．逆演算を行なうためには，SVDとは異なる展開を求め，W_Sを当てはめていかないといけない．実際には，これだけでは，線形代数の関係から，U,Vを求めたり，W_Sとは異なる透かしをあとから想定するInversion Attackも量子化誤差を除き可能であるなどの問題点は残る．その対策は後半で述べる．しかし，実際にはGwが整数値に(四捨五入などで)量子化されているため，整合する別のU,Vを求めてInversion Attackを行なうのは反復計算を要すると考えられる．



Sは対角行列，

透かし W_S は非対角成分に非０の値を持つ

$$G_W = U * S_W * V^T,\ S_W = S + W_S$$

図２　SVD領域における電子透かし埋込み

3.2 一方向性

電子透かしの埋込み関数に関して，ある種の一方向性を考えることができる．ここで，一方向関数の定式化が必要となる．一方向性関数は，暗号化において特に検討され，素数の積を行なう演算に対し，その逆演算である素因数分解は計算が困難であるという研究から，それを拠り所にした，公開鍵暗号方式がある．一方向関数の定義は式(2)に示すような形式でなされている．一方向性関数の存在は証明はされていないが，数学者の研究から，素因数分解は困難度が高いため，公開鍵暗号として広く実用化されている．そこで，ここでは，一方向性関数の定義をゆるめた疑似一方向性を導入し，完全性は保証できないが，実用上の解読困難度や解読コスト増加を評価して積極的に使用することの提案と，その評価法の検討を行なう意義について考えていく．

一方向性関数の定義[8]：式(2)は Goldreich による定義で，任意の多項式時間確率のチューリング機械 M と任意の n 次多項式 p(n)に対し，十分大きな全ての $n \in N$ の下で，(2)が成立する．ここで，確率は Un という一様分布に従う確率変数と，Mの中でとられるコイントスによってとられる[8].

$$\Pr\left(M\left[f(U_n),1^n\right] \in f^{-1}f(U_n) \cap \Sigma^n\right) < \frac{1}{p(n)} \qquad (2)$$

3.3 疑似一方向性関の定義：

疑似一方向性の用語は，Whitfield Diffie らにより，quasi one-way-function として，述べられている[9]．即ち，「a *quasi one-way function* is not one-way in that an easily computed inverse exists. However, it is computationally infeasible even for the designer, to find the easily computed inverse. Therefore a quasi one-way function can be used in place of a one-way function with essentially no loss in security.」とあり，数学的な一方向性の証明が無くても，実際に計算量的に算出が困難であれば，十分セキュリティ上一方向性と言えると言うことになる．ここでは，計算量的に逆関数が求まらないだけでなく，正方向関数演算より，逆方向演算の方が手間がかかるものを疑似一方向性関数と呼ぶことに拡張し，その逆方向演算の計算量の最小値を評価していくことにする．

任意の y=f(x)から x を求める算出アルゴリズムの計算回数の最小値を規定することを目的とし，x から y を求める計算回数の最小値より大きいものを疑似一方向性関数と呼び，その逆関数値を求める算出アルゴリズムの計算回数の最小値をその性能として付記することを推奨する．

$$\mathrm{Min}(\mathrm{Num}(y = f(x))) < \mathrm{Min}(\mathrm{Num}(x = f^{-1}(y))) \quad (3)$$

SVD による電子透かしの埋込み関数を疑似一方向性関数の観点でみると，以下のようになる．埋込みに対し，埋込み後の画像 Gw と W_S を与えた時，整合する特異値展開の組 U,V を求めることは，SVD の展開を W_S により補正すれば求まると考えられる．しかし，Gw は量子化されているため，直接的で機械的な処理だけでなく，反復的な微修正が必要と考えられる．そのため，本来の計算量の数倍の処理がかかると予想される．また，画像のサイズによりこの計算量は増大するため，W_S の要素が多くスパース行列でない時は，O（n^3）の演算量になると予想される．なお，特異値展開はユニーク性が保証されているので，疑似一方向性関数の逆関数を求める場合未知の解法を除き，手間のかかる導出をする必要があると考えられる．

4. SVD 電子透かし方式

4.1 第一方式

SVD 展開に於いて一方向性の電子透かしが構成できるのは，画像データで埋まった２次元行列が SVD 展開により対角成分のみのデータになり，対角成分以外は全て０になっているという性質が意味のあるところである．そして，非対角成分に S S=S+W と配置されることになる透かし行列Wが加えられたことによって，SVD を行う限りにおいては一方向的加算が行なわれたことになり，従って Inversion Attack するためにはこの透かしWを知り，はじめの埋込み者と同一の埋込みを行なったと述べるしか無いことを特徴としている．そこで SS=S+W はそのままはじめの SVD 展開基底U，Vで逆変換して，画像データに透かしを埋込んだ復元を行なえば良い．つまり，

$$G_W = U * SS * V^T$$

なる変換で，透かしを埋込んだ画像データを得れば良い．この G_W に対し，再度 SVD 展開すると，

$$G_W = U_W * S_W * V_W^T$$

となり，一般には，$SS \neq S_W$，$U \neq U_W$，$V \neq V_W$である．SSは非対角成分を有すが，S_Wは対角成分のみで，埋込み画像G_WをSVD展開して得られた対角行列S_Wから透かしデータを求めることはできない．つまり，埋込み画像G_WからSS=S+Wを直接求めることはできない．

一方，はじめの埋込み者は，U，Vを用いて，SSを求めた後，秘密に保存しておいたSを用い，W=SS-Sなる透かしデータを求めることができる．ここにおいて，SVD展開を用いた一方向性を有し，埋込んだデータが正しく算出できる電子透かし方式を定式化することができた．

しかし，この方式にはまだ以下のような問題がある．即ち，G_Wから直接SSやWを求めることはできないが，次のような線形代数の基本演算手法により，SSとは異なり得るが同等の役割を持つU'とV'とWとは異なり得るW'を算出することができ，いわゆるInversion Attackを実現することができる．例えば，

$G_W = U_W * S_W * V_W^T$

を求めた後，適正な正則行列Tにより，

$S_W = U_W^T * G_W * V_W$は，左右からT, T^{-1}を乗じて，

$T * U_W^T * G_W * V_W * T^{-1}$

と変形できる．ここで，$T_U = T$，$T_V = T^{-1}$とおけば，

$$T_U * S_W * T_V = T_U * U_W^T * G_W * V_W * T_V \qquad (3)$$

が得られる．ここで，行列Tの例として，下記を選べば，(3)は

$$T_U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ \varepsilon & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad T_U^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -\varepsilon & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = T_V$$

$$T_U * S_W * T_V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ \varepsilon & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & s_4 \end{bmatrix} * T_V$$

$$= \begin{bmatrix} s_1 & 0 & 0 & 0 \\ \varepsilon s_1 & s_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & s_4 \end{bmatrix} * \begin{bmatrix} 1 & 0 & 0 & 0 \\ -\varepsilon & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} s_1 & 0 & 0 & 0 \\ \varepsilon s_1 - \varepsilon s_2 & s_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & s_4 \end{bmatrix}$$

$$= \begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & s_4 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ \varepsilon s_1 - \varepsilon s_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad (3)$$

式(3)をS_W^*　と置くと，

$S_W^* = S_W^D + W'$ ただし，S_W^Dは対角行列(Diagonal)，W'は非対角行列と分解できることがわかる．

ここで，式(3)を埋込み画像G_W　に関して変形すると，

$$T_U * S_W * T_V = T_U * U_W^T * G_W * V_W * T_V$$

より，

$$(T_U * U_W^T)^{-1} * T_U * S_W * T_V (V_W * T_V)^{-1} = G_W$$

となり，

$$U^* = (T_U * U_W^T)^{-1} * T_U, \quad V^{*T} = T_V (V_W * T_V)^{-1}$$

と再定義すれば，非対角成分を有する透かしW'を得ることができる．

また，

$$\begin{aligned} U^* V^{*T} &= (T_U * U_W^T)^{-1} * T_U * T_V (V_W * T_V)^{-1} \\ &= U_W^{T^{-1}} * T_U^{-1} * T_U * T_V * T_V^{-1} * V_W^{-1} \\ &= U_W^{T^{-1}} * (T_U^{-1} * T_U) * (T_V * T_V^{-1}) * V_W^{-1} \\ &= U_W^{T^{-1}} * I * I * V_W^{-1} \\ &= U_W^{T^{-1}} * V_W^{-1} \\ &= I \end{aligned}$$

である．

このT_Uは画像や埋込んだ透かしに関係なくいつでも使用可能な万能なAttack行列である．

4.2 第二方式

前記した第一方式の問題を解決するため，次に更に改良を行った方式を提案する．これは上記の一方向性が特定な直交変換行列Tにより容易に非対角成分に値を配置するような展開行列を生成できることを防止するために工夫された方式である．第二方式の定式化の前に対角成分のみの行列Sと透かし行列Wの関係を整理しておく．

画像行列Gに対しSVD展開行列U,Vは2つの異なる展開行列で，列展開（U）と行展開（V）をそれぞれ担っている．

次に，非対角成分から成る透かしデータWは行列Tにより対角成分から乗算によって生成することができる．つまり，片側のUだけに変形を施すことにより，

SS=S+W

であるとともに，

$$SS = T_U * S$$

でもあり，行列の乗算により得られた結果は別の加算によって得られた結果と同一の透かしの埋め込まれ

たデータ SS を生成することができる．即ち，

$S+W=T_U * S$

より

$W=S*(T_U-I)$

又は，

$T_U=(S+W)*S^{-1}$

となる．これを観察すれば，前記第一方式の例で用いた透かし行列 W は正則でない形になっている．本論文で提案する方式は，正しい演算ができるので，W は透かしとしての変形量が一定以下ならどのようなものでもよい．そこで，W に充分多くの情報を盛り込んだ形にして，それによって，

変換行列 T が正則にならないような設定を構成すればよい．たとえば対角行列 S の中程で，以下のような部分的コピーを行えば，SS=S+W の数行は，一次従属になり，従って

$T_U=(S+W)*S^{-1}$

より T_U は正則で無くなり，SVD 展開の $U^*=T_U*U_W$ も階数が低下し，正則でなくなる．これにより，透かしの入った画像 G_W を SVD 展開すると，階数の低下した対角行列 S_W が得られるが，この階数の低下した行列から階数を上げ，かつはじめの I_W と整合する SVD 展開行列 U，V を求めることは計算量的に難しい．

画像　1st　SVD

$G \longrightarrow G=U*S*V^T,\ S=U^T*G*V$

W: watermark, a: weight

$G_W \longleftarrow SS=S*a*T_{k,k+1}$:

inv SVD　　adding watermark

Detection: 1st SVD again

$G_W=U*SS*V^T \longrightarrow SS=U^T*G_W*V$

$W=(SS-S)/a$

ここに，

$$T_{k,k+1}=\left[\begin{array}{ccc:cc:cc} 1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&\bullet&0&0&0&0\\ \hdashline 0&0&0&1&1&0&0\\ 0&0&0&1&1&0&0\\ \hdashline 0&0&0&0&0&\bullet&0\\ 0&0&0&0&0&0&1 \end{array}\right] \begin{array}{l} \\ \\ \\ \text{k} \\ \text{k+1} \\ \\ \\ \end{array}$$

図２　提案方式

5.　実験

以下，実画像を用いた例で，具体的に確認をとりながら，提案方式の仕組みを詳細に観察してた．確認をとるため，４ｘ４画素の小ブロックの画像に対して調べた結果は[10]に示されている．

SVD 電子透かしの具体的埋込み方を図３に示す．画像 G に対し，SVD（展開）を行ない，U,V,S を得る．

$G=U*S*V^T$

埋込み後の画像の S/N 低下の目標値に対応した大きさの特異値の場所 k を選ぶ．階数低下の透かしWを作る．

$w_{k,k+1}=s_{k+1,k+1}$，　$w_{k+1,k}=s_{k,k}$

透かしの埋込み，$S_W=S+W$ を行ない，画像に戻す．

$G_W=U*S_W*V^T$

攻撃としては，今回 JPEG 圧縮，$Jpeg(G_W)$ を行い，圧縮率として，1/5,1/10,1/15，1/20，1/30 を試みた．これを復号，$G_W{}^J=Jpeg\_Dec(Jpeg(G_W))$ により復号し，これに対し，はじめの特異値展開を再度行い，$S_W{}^J=U^T*G_W{}^J*V$ を得る．この $S_W{}^J$ の成分を調べ，はじめの特異値，埋込んだ透かし成分が存在することと，他の０値の成分が非ゼロの値（ε）に変化したものが特異値や透かし成分に比べて，十分小さいことを検証する．特異値は正の実数であることから，それらの値の 1/2 を判定値として使用することができる．

$G=U*S*V^T$

$$S=\begin{bmatrix} s_{k-1,k-1}&0&0&0\\ 0&s_{k,k}&0&0\\ 0&0&s_{k+1,k+1}&0\\ 0&0&0&s_{k+2,k+2} \end{bmatrix}$$

$$S_W=\begin{bmatrix} s_{k-1,k-1}&0&0&0\\ 0&s_{k,k}&s_{k+1,k+1}&0\\ 0&s_{k,k}&s_{k+1,k+1}&0\\ 0&0&0&s_{k+2,k+2} \end{bmatrix}$$

$$S_W{}^J=\begin{bmatrix} s_{k-1,k-1}&\varepsilon&\varepsilon&\varepsilon\\ \varepsilon&s_{k,k}&s_{k+1,k+1}&\varepsilon\\ \varepsilon&s_{k,k}&s_{k+1,k+1}&\varepsilon\\ \varepsilon&\varepsilon&\varepsilon&s_{k+2,k+2} \end{bmatrix}$$

図３　埋込みの具体的手法

画像データベース，SIDBA の画像を用いて，SVD 展開と埋込み，JPEG 圧縮，検出の実験を行なった．図４に埋込みによる劣化を表す S/N と埋込んだ画像を JPEG 圧縮した時の S/N を示す．埋込んだ段階での S/N は 47.2dB である．1/20 の圧縮では劣化が大きくなってくる．図５に検出率のデータを示す．表２に電子透かしの埋込み位置と埋込んだ特異値の値を示す．この特異値の値が保たれ，所定の値以上になっている時，検出できたと判定する．今回は，検出の判定基準として，はじめの特異値の値の 1/2 を使用した．図５の検出率は，抽出された特異値の値は，はじめの値を基準として正規化され，表示されている．50%の破線が検出可能か不可能かの判別線である．JPEG 圧縮しない時は，演算誤差のみであり，演算誤差は無視できる小ささであるため，100%の検出が可能である．ＪＰＥＧ圧縮率で 11-13 が検出可能な範囲で，それ以降は検出可能とは言えない状態になっている．SVD_min は SVD 値そのものの変化であり，S(k,k)と S(k+1,k+1)の２個の値のうち小さい方が選ばれている．２画像とも圧縮率 30 まで，判定レベル以上になっている．WM_min は埋込んだ透かしの S(k,k+1)と S(k+1,k)のうち同じく小さい方が選ばれている．少なくとも１個の透かしが 50%のレベルを下回るのは JPEG 圧縮率が 11-13 の時である．Ripple_Max は，S(k,k)，S(k+1,k+1)，S(k,k+1)，S(k+1,k)以外の値は全て０であるが，JPEG 圧縮により非０の値に変化しているが，周辺での変動の絶対値の最大になる値を選んだ値である．このリップル値についても，特異値に比較した割合であり，50%以上になった場合には，異なる透かしが抽出されたと見なし，検出不能と判定する．リップル値は全般に小さく，girl で圧縮率 30 の時でも，15%程度で小さく，検出に影響はなかった．

図６に埋込みサイスを約２倍にした場合の検出率の違いを示す．画像サイズ 506×506 の埋込み劣化は，46.9dB と 256×256 の場合と同程度に設定してある．圧縮率 30 でも耐性は十分高い結果が得られている．

表１　埋込み位置と埋込み特異値の値

Image	Embedded Position(1) S(k,k)	SVD Value	Embedded Position(2) S(k+1,k+1)	SVD Value
girl	50	205.06	50	195.68
couple	51	197.62	51	189.70

6. まとめ

SVD を用いた電子透かし方式を整理し，埋め込んだ透かしが正しく検出でき，かつ SVD の一方向性を実現するため，次数の低下により，簡易な線形直交変換行列の挿入では求まらない，電子透かし方式を提案した．一方向性により，いわゆる Inversion Attack を行うことができない．認証性に関しては，文献[11]等に

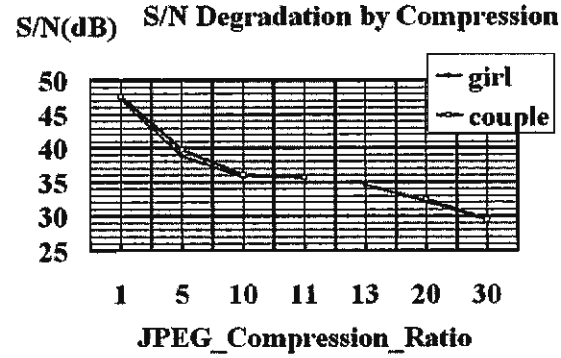


図４　JPEG 圧縮と S/N

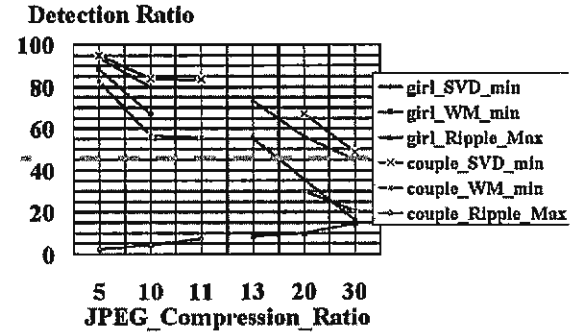


図５　JPEG 圧縮と検出率

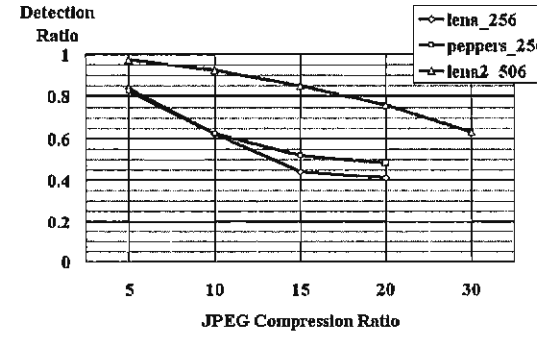


図６　画像サイズと検出率の違い

示されている，検出器公開型の埋め込み方式があり，本方式は，これと組み合わせることにより，電子透かしの新しい存在を示している．本発表の実験では，検出において，透かしやSVDの中で最も小さい値が50%以上であるかの判定をしているが，平均値や多数決などの統合判定を適用すれば，更に性能は向上することが期待できる．また，透かしやSVD以外の周辺の0値の領域の変動であるリップル値は全般に小さく，まだかなりの余裕度があり，この部分の活用も期待できる．

文　献

[1] Scott Craver, Nasir Memon, Boon-Lock Yeo, Minerva M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications", IEEE Journal on Selected Areas in Communications Volume: 16, Issue: 4 pp. 573-586 , May 1998

[2] Kazuo Ohzeki and Masaru Sakurai, "SVD-Based Watermark with Quasi-One-Way Operation by Reducing a Singular Value Matrix Rank", Proc. of The First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-forensics 2008), Technical session B4. Watermarking, 1. Jan 21-23, 2008, Adelaide.

[3]Qiming Li and Ee-Chien Chang. Zero-Knowledge Watermark Detection Resistant to Ambiguity Attacks. In *ACM Multimedia Workshop*, Geneva, Switzerland, September 2006.

[4]Zhang Fan et al, "Capacity and Reliability of Digital Watermarking", Proc of IEEE Inter. Conf. on the Buisness of Electronic Product Reliability and Liability, 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]K. Ohzeki et al., "One-Bit Open Watermarking System", Proc. PCS. S8-14, Dec. 2004.

[7]Alessandra Piva ed., "Deliverable 2.1.pdf", State of the art report and accompanying public presentation(s) http://www.speedproject.eu/, July 2007.

[8]相田慎，築地立家，「一方向性関数の平均時間計算量解析」信学技法 COMP99-28, pp.47-54, Jul. 1999.

[9] Diffie, W. and Hellman, M., "New directions in cryptography", IEEE Transactions on Information Theory, Vol.22, No.6, pp. 644- 654,1976.

[10]大関和夫，「認証性と耐性の精度保証を有す電子透かし方式」研究調査報告書，2008年

[11]Kazuo Ohzeki, Cong Li, "Consideration on Variable Embedding Framework for Image Watermark against Collusion Attacks", Wavilla Challenge (WaCha) 2005, Proceedings of the WAVILA Workshop on Watermarking Fundaentals D.WVL.2-1.0.pdf, pp.54-62., June 8-9, 2005.