認証性と耐性の精度保証を有す電子透かし方式

大　関　和　夫　　芝浦工業大学工学部教授

1 はじめに

電子透かしに認証性と高い耐性を与え、個人がコストをかけずに電子透かしの埋込みと第三者への著作権の主張という認証機能を果たせるシステムを開発することを目的とする。

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に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開発することを目標とする。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、これまで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方式を提案して来た。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。

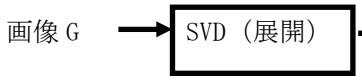
電子透かしの認証に対して、「Inversion Attack」といわれる攻撃手法がある。これは、一旦電子透かしを埋込んだ後にその電子透かしの存在を無効にする手法であるが、電子透かしの埋込みが加算演算であり、逆演算である減算が存在すれば、Inversion Attack は可能とされている。そこで、加算は可能だが、減算は困難性が高くなる一方向性関数の性質を有する埋込みを行なえば、Inversion Attack は防止できる。本研究では、この一方向性関数を作り出すため、まず疑似一方向性関数を定義し、その埋込み後の劣化と耐性について検証してきた。特異値展開(Singular Value Decomposition)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。以下、主に疑似一方向性関数とＳＶＤを用いた電子透かしについて述べる。

2 特異値展開(Singular Value Decomposition: SVD) を用いた電子透かし

2-1　疑似一方向性関数の導入

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。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、その透かしがある一方向的な演算の後に見える物になるものであれば、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[1]。図 1 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。また、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。



$G = U * S * V^T$　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

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

図１　SVD 領域における電子透かし埋込み

・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実情から、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(1)に示すような形式でなされている。一方向関数の存在は証明はされていないが、経験上、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補助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[2]：式(1)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、(1)が成立する。ここで、確率は Un は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[2]。

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

・疑似一方向性関数の定義：

疑似一方向性という用語は、Whitfield Diffie らにより、quasi one-way-function として、述べられている。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のかかるものを疑似一方向性関数と拡張し、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。

$$\mathrm{Min}(\mathrm{Num}(y = f(x))) < \mathrm{Min}(\mathrm{Num}(x = f^{-1}(y))) \qquad (2)$$

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、整合性のある導出をする必要がある。

2-2 ＳＶＤ電子透かしの従来方式

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、非対角化の成分が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、有効なものはほとんどなかった。

SVD を用いた電子透かしは、Gorodetski[3]により 2001 年に発表された[3]。しかし、方式自体に問題があったり、耐性が低い方式であったり、DCT や Wavelet 変換との組合せに特徴を置いたりしたものが多く、正式に一方向性を保持した Inversion　Attack への耐性のある方式は提案されていない。本論文では SVD 展開を数学的に見直し、今まで議論されてきた問題点を再度明確化し、その結果新たに一方向性を有し、Inversion Attack が難しい電子透かし方式を提案し、その有効性を論じている。また、実データで、SVD 計算の様子を示し、直感的にも事態を理解し易いようにして、SVD 展開を用いた電子透かし方式の研究に供する用意した。

（１）Liu　Tan　の方式と問題点

Liu,Tan らは 2002 年 SVD を用いた電子透かし方式を発表[4]したが、その後 Xiao,Zhang らに指摘された[5]ように、一旦埋込んだ透かし入り画像の検出において、異なる透かしを埋込んだ時に生成される行列を用いると、はじめの透かしの有無に関わらず、常に乗じた行列に含まれている透かしが優勢となり検出されるという問題があることが示されている。この誤った検出は一種の Inversion　Attack とも見做すこともできるが、SVD 演算の不備により SVD で情報が不足しているため、埋込みにおいて情報を正しく埋込んでいないことが分かる。実際この方式は以下のように構成されるが、透かしを埋込んだ後に SVD の対角化を再度行なっているところが問題であり、これにより、系全体が透かしデータに関し、検出可能である、つまり攻撃の無い状態では、透かしデータは可逆に復元できるという条件が満たされていない。

文献[4]の方式について、再考してみる。Ａを画像を表す実数又は複素数のＮ×Ｎの正方行列とし、その特異値展開は、

$A = USV^H$、

となる。ただし、Ｕ，ＶはＡを対角化する直交行列、Ｓは対角行列で、Ｈは複素共役転置を行なう。

次に透かし情報を表す行列Ｗに重み付け係数ａを適用し、

Ｓ＋ａＷなる透かしの埋込みを行なった後、これを SVD 展開により再度対角化し、

$S + aW = U_W S_W V_W^H$　としたS_W　を透かしを埋込んだ後の固有値とみなし、U_W, V_W^Hを透かしの検出行列として使用している。Ｗを無視し、はじめのＵ，Ｖを用いて逆特異値変換することにより、

$A_W = US_W V^H$

を得て、透かしを埋込んだ画像とする方式である。

しかし、この手法ははじめのＵ，Ｖを用いて、U_W, V_W^Hにより変形されたS_Wを逆特異値変換するという、数学的に不整合な数式変形を行っており、電子透かし情報は正しく復元できない。これについては、その後[5]により、埋込んだ透かしが正しく復元できず、別の透かしと混合することのあるという不具合が、実例によって示されている。即ち、埋込んだ透かしは他の透かしと混合され区別が付かないことが実験画像によって示されている。

しかし、この後者の文献[5]は、実験的に不具合があることを基に、透かしＷの機能を解説しているものの、数学的に透かしの埋込みと検出が可逆な対称性を有していないことを明確には示していない。また、以後の SVD を用いた電子透かし方式も文献[4]に基づいた方式や、その不完全性を部分的に補正するような方式[5]などがあるのみで、明確な埋込みと検出のアルゴリズムが示されていない。文献[4]では画像を表す行列Ａは任意の実数又は複素数と仮定しているが、一般に任意の行列はＳＶＤ展開される保証はあるが、任意の画像の行列Ｇを対角化しようとした時は、ある直交行列Ｕ，Ｖにより、

$U\ GV^T = S$　　（ただしＳは対角行列）、

と変形できる。これをＳＶＤ分解といい、任意の画像の行列Ｇはその転置行列との積

$GG^T = G^T G$

を求めて、その固有ベクトルからなる実数の直交行列Ｕ、Ｖを求めることにより、前記の様な対角化が可能となる。これは、前記転置行列との積、$GG^T = G^T G$が実数の対称行列であることから、一次独立の次数（rank（GG^T））の範囲まで、実数の直交行列Ｕ、Ｖが求まることが保証されている。従って、複素数までの

範囲で検討する必要はなく、実数の範囲で検討すればよいことがわかる。すなわち、文献[4]ではＧをＳに対角化した後、透かし情報の行列Ｗを用意し重み付け係数ａを用い

Ｓ＋aW

なる行列を再度ＳＶＤ展開により対角化し、

$S+aW=U_W S_W V_W^T$

とし、それをはじめの正規直交行列Ｕ、Ｖで逆変換し、

$G_W=U^T S_W V$

が透かしの埋め込まれた、画像となる。従って透かしの情報は、近似的にはじめの行列Ｇとその転置行列との積、GG^T の固有値の平方根からなる対角行列Ｓと埋込み後のS_W との差のパターンからその有無を判定しようとしている。具体的には、透かしの埋め込まれた画像、G_W　には劣化が加わり、G_W^* となったとして、その特異値展開を行い、

$G_W^*=U^* S_W^* V^{*T}$

を得る。Ｗの埋込みによって固有値が変化しないほどＷの要素が少なく、かつ小さければ、また攻撃による劣化が無ければ、$G_W^*=G_W$、その他であることから、固有値の一意性から$S_W^*=S_W$　になる。得られたS_W^*　に対し埋込みの時の逆変換を施すと、

$D^*=U_W S_W V_W^T$

を得る。これと、はじめの対角行列Ｓとの差のａ分の１倍

$$W^*=\frac{1}{a}(D^*-S)$$

が埋込んだ透かし情報として検出される。

しかし、文献[3],[4]のようにＷの要素として多くの乱数などのパターンを入れた実験では、$S_W^* \neq S_W$ となり、埋込みと、検出が対称に処理されず、攻撃が無くても、正しい透かしが検出できない。そして、上記の演算では、Ｕ，Ｖの優位性が働き、埋込んだはずの透かしよりもＵ，Ｖの作用が大きくなり、埋込みデータに関係なく、Ｕ，Ｖの値に依存した透かしデータが出力されることになっている。

また、文献[6]では対角線状に埋込んで、透かし行列の階数を上昇させているが、基本的な方式が文献[3]の方式であるため、整合が不完全である。階数の上昇に関しては、後章で述べる。

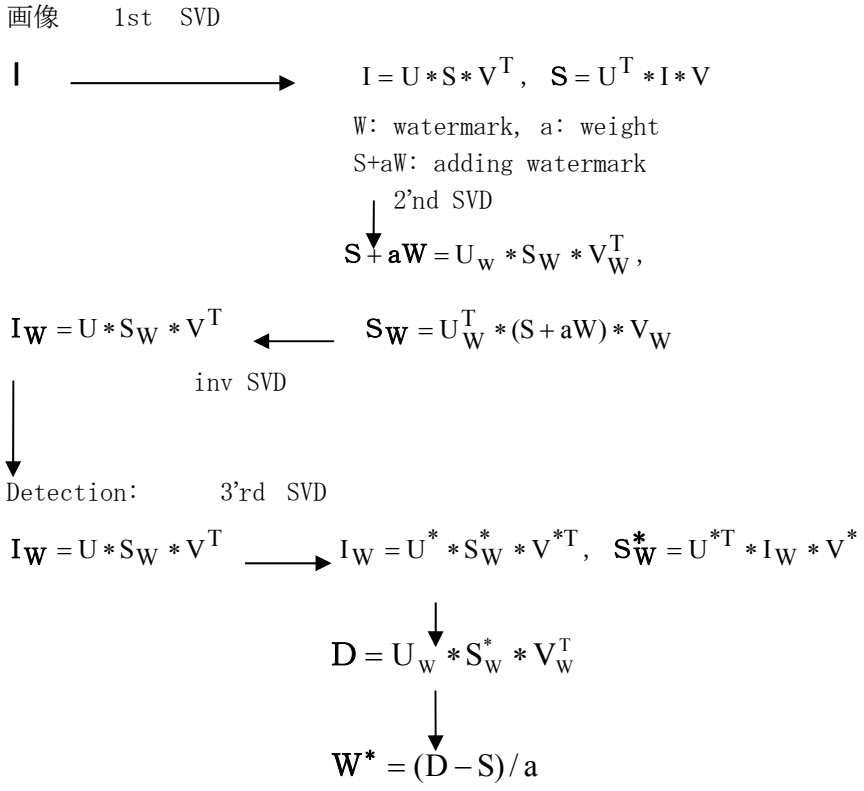


図１　Liu　Tan 方式

3.1 第一方式

SVD 展開に於いて、前章で示したように透かしWを重畳した後に再度 SVD 展開を行なう必要はない。そもそも SVD 展開で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ＳS=S+W と配置された透かし行列Wが加えられたことによって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 SVD 展開で対角化することなく、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、

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

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I_Wに対し、再度 SVD 展開すると、

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

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I_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I_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、I_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、

$I_W = U_W * S_W * V_W^T$

を求めた後、適正な正則行列Ｔにより、

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

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

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

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

が得られる。ここで、行列Ｔの例として、下記を選べば、(3)は

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

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

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

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

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

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(3.1.1)を埋込み画像I_W　に関して変形すると、

$T_U * S_W * T_V = T_U * U_W^T * I_W * V_W * T_V$　より、

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

となり、$U^* = (T_U * U_W^T)^{-1} * T_U$, $V^{*T} = T_V (V_W * T_V)^{-1}$

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。

3.2　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

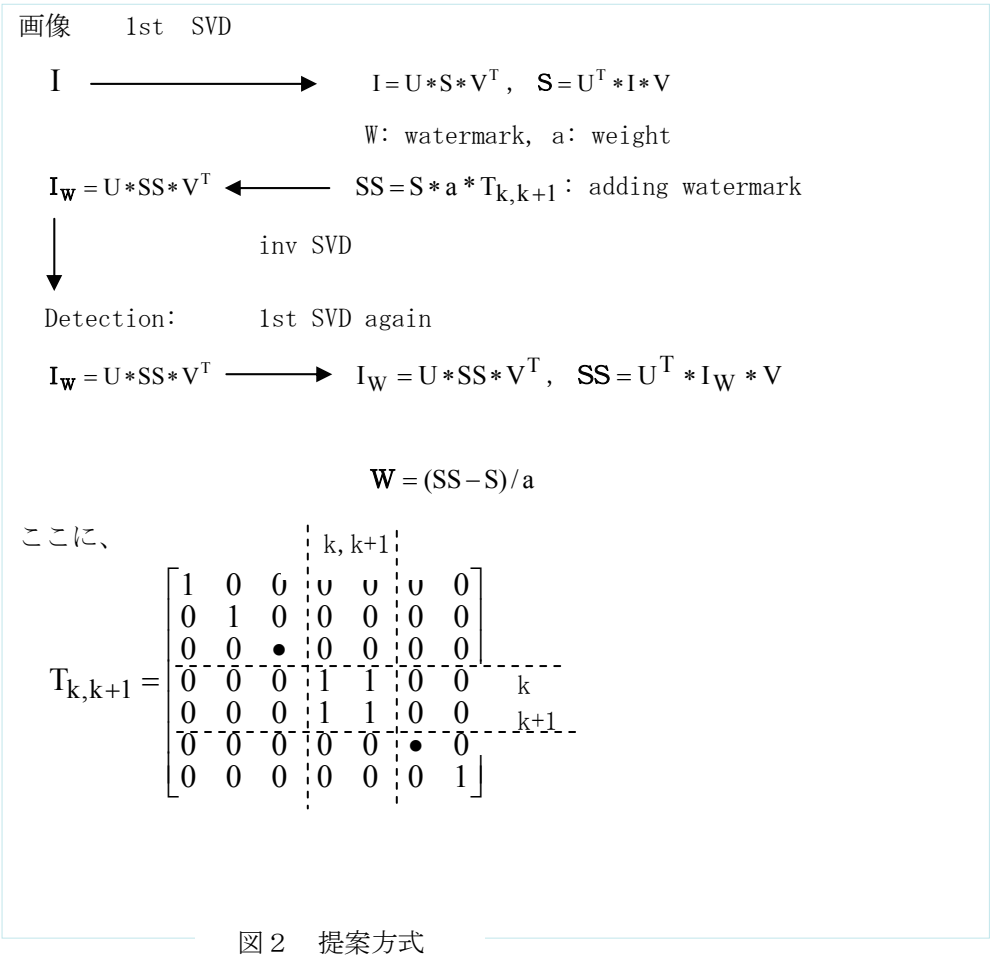


図２　提案方式

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 I_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。

４．　実験例

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いく。確認をとりやすくするため、はじめに４ｘ４画素の小ブロックの画像に対して調べる。まず、入力画像をＩとし、その SVD 展開を[U,S,V]とする。

I ＝

236	227	204	183
203	177	164	158
169	162	174	190
177	199	213	222

S=

767.579556694097	0	0	0
0	63.1804907392307	0	0
0	0	17.9384827561283	0
0	0	0	0.246113086952545

U=

-0.554448070072689	-0.533095031464902	0.481720107910591	-0.419931854774931
-0.457973187745198	-0.434336858003431	-0.469697061247156	0.617249320568273
-0.45235804411934	0.353912751629588	-0.607402533968744	-0.548798802734525
-0.527465730469476	0.63396131225897	0.422365446052046	0.376138787843588

V=

-0.512817520953815	-0.664103773399817	-0.532648295046837	0.110770763934372
-0.501796388777014	-0.227887262937507	0.661460507986631	-0.508662733031689
-0.494118825917294	0.263244982251759	0.307516702652383	0.769403757973141
-0.490983869681322	0.661615940607726	-0.429172771442423	-0.37014850951873

次に透かしWとして、Sの第２列と第３列を同一にするものとして、
W(2,3)=S(2,2), W(3,2)=S(3,3)
を用いる。これから SS=S+W も算出できる。

W=

0	0	0	0
0	0	63.1804907392307	0
0	17.9384827561283	0	0
0	0	0	0

SS=

767.579556694097	0	0	0
0	63.1804907392307	63.1804907392307	0
0	17.9384827561283	17.9384827561283	0
0	0	0	0.246113086952545

次に SS をU，Ｖを用い $I_W = U*SS*V^T$ と画像に変換する。

I_W =

248.201498358751	202.751964017341	195.917252878461	203.172296648128
223.212237595186	160.76855376712	153.343234004991	164.20264822814
164.325775953567	179.273541434739	178.00790502962	173.194645358824
150.633666702599	223.767520909017	227.311770642005	209.822715676598

この I_W を再度 SVD 展開すると、$I_W = U_W * S_W * V_W^T$ から、

U_W =

-0.554448070072689	-0.381253732728727	-0.419931854774919	-09007525584356
-0.457973187745198	-0.546110091614014	0.617249320568266	0.333208048224904
-0.45235804411934	0.174556920609469	-0.548798802734539	0.680971332366497
-0.527465730469476	0.72521668526385	0.376138787843593	-0.233152900206643

V_W =

-0.512817520953815	-0.846231502997657	0.110770763934378	0.0929530601675069
-0.501796388777014	0.306582581715293	-0.50866273303165	0.62886383965363
-0.494118825917294	0.403589457837179	0.769403757973143	0.031304833710029
-0.490983869681322	0.164362141157277	-0.370148509518777	-0.771304095132379

S_W =

767.579556694097	0	0	0
0	92.8823295750267	0	0
0	0	0.246113086952552	0
0	0	0	9.82487009997665e-15

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３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。1/20 の圧縮では劣化が大きくなってくる。図４に検出率のデータを示す。表１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４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。

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

５．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。４ｘ４画素の小ブロックでデータの動きを確認し、所定の動作が達成されていることが示された。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[7]等に示されている、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。

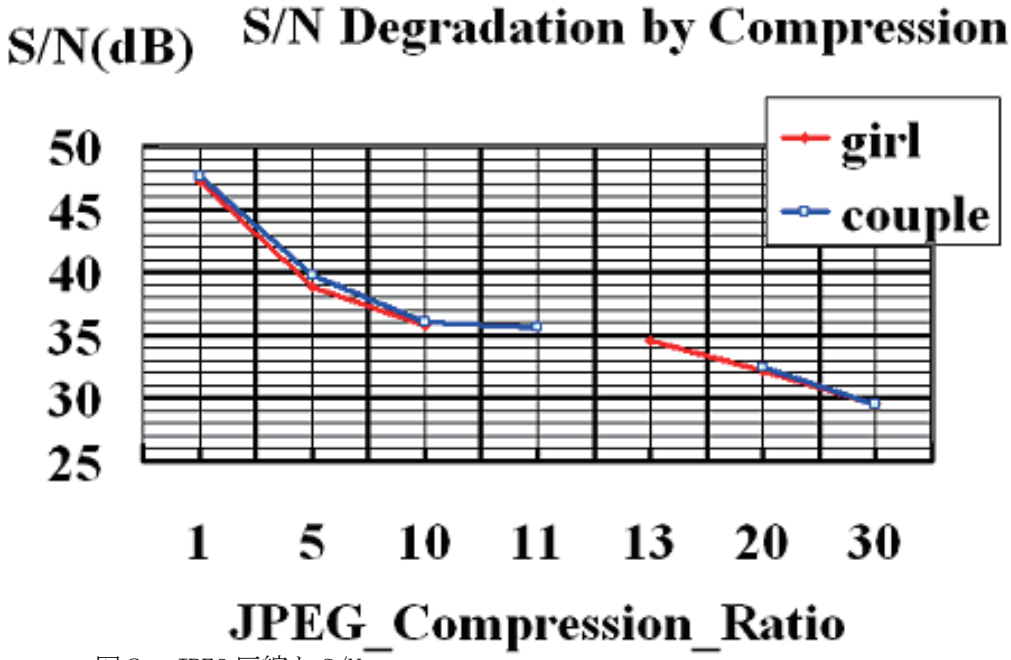


図３　JPEG 圧縮と S/N

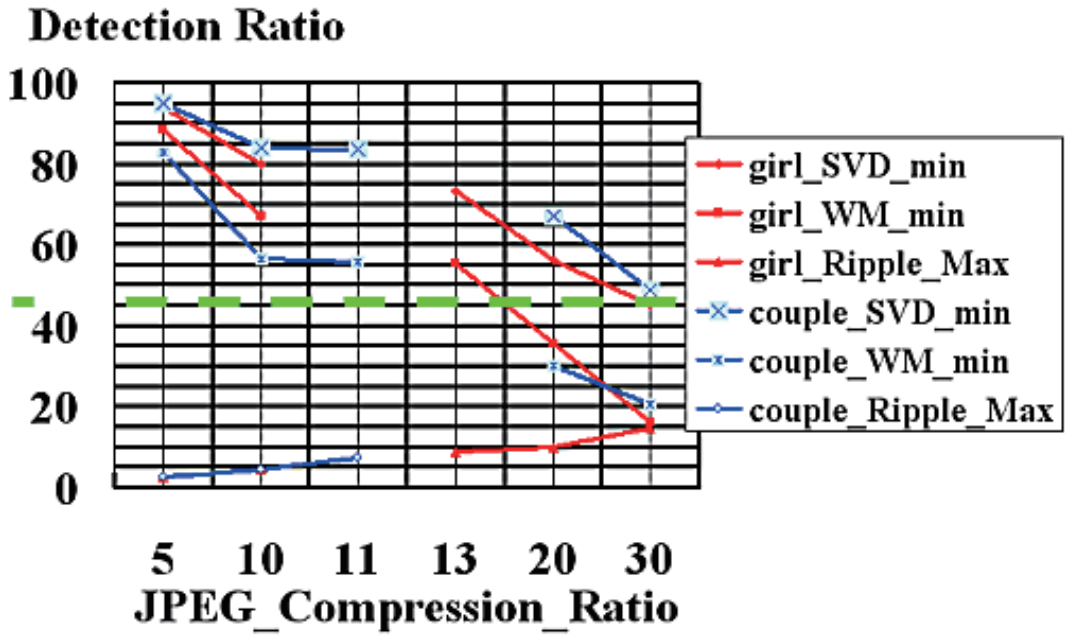


図４　JPEG 圧縮と検出率

参考文献

[1]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.

[2]S. Aida and T. Tsukiji, “Average-Time Analysis of One-Way Functions”, IEICE Tech. Report COMP99-28, pp. 47-54,　1999.

[3] V. Gorodetski, L. J. Popyack, V. Samoilov, and V. A. Skormin, “SVD-based Approach to Transparent Embedding Data into Digital Images,” Proceedings of the International Workshop on Information Assurance in Computer Networks: Methods, Models, and Architectures for Network Security (MMM-ACNS 2001),Pages: 263 - 274, May 21-23, 2001.

[4] Ruizhen Liu and Tieniu Tan, “An SVD-Based Watermarking Scheme for Protecting Rightful ownership”, IEEE Transactions on Multimedia, Vol. 4 No.1 pp.121-128, Mar. 2002.

[5]Xiao-Ping Zhang and Kan Li ‘Comments on “SVD-Based Watermarking Scheme for Protecting Rightful ownership” ‘, IEEE Transactions on Multimedia, Correspondence, Vol. 7 No.2 pp.593-594, April 2005.

[6]Wu, Yongdong, ″ On the Security of an SVD-based Ownership Watermarking″, IEEE Trans. on Multimedia, vol.7, no.4, pp. 624-627, Aug. 2005.

[7]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.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
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)**	2008 年 1 月 22 日