情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2009-SE-164 No.5
Vol.2009-EMB-13 No.5
Vol.2009-CSEC-45 No.5
2009/5/28

電子透かし用に開発された疑似一方向性写像の程度の数値解析

大関和夫† 瀬尾祐貴† 魏遠玉†

電子透かしの埋め込み機能を疑似的な一方向性写像とみたて，その一方向性の程度を評価することを試みた．埋め込んだ電子透かしの大きさに対する，写像の成分の変化の対応を調べ，一部に不連続性があることがわかった．この不連続点においては，逆写像が求まりにくい一方向性があると考えられる．電子透かしの埋め込みには，特異値展開を用い，埋め込み量と展開行列係数の変化を解析している．

Numerical Analysis of Continuity of Quasi-One-Way Mapping Developed for Watermarking

KAZUO OHZEKI† YUKI SEO† and ENGYOKU GI†

Singular Value Decomposition (SVD) watermark embedding has the possibility of quasi-one-way functionality. An advanced SVD method with rank reduction can protect against inversion attacks. At embedding, the decomposing matrix obtained from the original image differs from the one obtained from the embedded image. In this paper, it is demonstrated that the difference is distinct and is discontinuous in the Euclidean Norm by numerical evaluation. This evidence enhances the probability that SVD embedding is resilient against inversion attacks.

1. はじめに

汎用の電子透かしを認証性まで確保して構成することは難しい．認証性を含めたセキュリティ性に関し，理論と実用化にギャップがあることが指摘されている［1］．電子透かしにおける耐性，埋込み情報量，画質の維持という要求事項は相反するものである．耐性を上げ，埋込み情報量を増大すると，画質の劣化が大きくなる．従って，埋込み情報量を削減し，画質を維持することが必要である．又，誤り訂正符号などで耐性の向上が図れるが，攻撃による劣化が大きい場合に対しては，効果がなくなる［2］．電子透かしの埋込み・検出を伝送路と見做すと，その誤り率は攻撃により 0.1 以上になりうる．汎用的に完成された電子透かしは明らかに構成困難であるが，用途を限定していけば，その存在価値が生じる．例えば，企業内のシステムに限定すれば，埋込み・検出は非公開で独自に行うことができ，通常第三者に対して認証の証明をする必要が無くなる．

筆者らは，個人がホームページに画像を公開する時に埋込む電子透かしの認証性を安価に個人単位で行うための方式を検討してきた．そのために埋込み情報量を最小化し，必要な情報は外部の検出器に移設する．埋込み情報量は埋込んだか，込まなかったかを識別する１ビットの意味情報を作り，実際の埋込みはこの １ビット情報を多数回埋込み，検出では，多数決乃至は誤り訂正演算によって 0.5 ビットより大きい検出がなされた時，情報が存在したと判定する．これにより，埋込み量と劣化が最小で，耐性が最大の構成をとることができる．この方式の問題点は，検出器を認証の為に，公開する必要があることである．公開する検出器は難読化により内部構造を隠蔽できたとしても，別途偽の検出器を生成すれば，著作権の確保が難しくなる．

本研究では，この応用例を改修し，検出器を公開せずに，監視のみ続ける段階と ，不正使用を発見した時に検出器等を公開して，認証する段階を分けることにより，より限定されたシステムにしていく．この段階においても偽の検出器に対する抑止力がないといけない．これには，いわゆる Inversion Attackに対する耐性必要になる． Inversion Attackは簡易だが根本的な問題である． Inversion Attackは埋込みが加算でその逆演算が減算である場合に，他人が別の透かしを宣言する事が可能になる事である．埋込みが単純な加算の規則で定義されている以上， Inversion Attackは可能になる． Inversion Attackを回避するには，単純加算でない，複雑な演算ルールを導入する必要がある．単純加算でない例として， Hash値を画像に埋込む，非線形の量子化（ QIM など）を行う，多数個の異なる透かしを埋込む，一方向性関数の利用などがある．このなかで，一方向性関数は未だ数学的に存在が示されていない．本研究では，埋込み自体は加算だが，強い方向性を有する拘束条件を持つものを考える．

Vol.2009-SE-164 No.5
Vol.2009-EMB-13 No.5
Vol.2009-CSEC-45 No.5
2009/5/28

以上のような検討に基づき，筆者らは特異値展開（SVD）を拘束条件として用いる方式を提案し，その埋込み処理が一方向性を有してないかの検討を行ってきた［3］．画像を特異値展開すると，正の特異値が対角成分に並び，対角成分以外は全て 0 になる．この非対角成分に透かしとしてある成分を加え，展開の逆演算である合成をすると透かし埋込み画像が得られる．これを再度特異値展開すると，非対角成分は全て 0 になり，埋込んだ透かしやはじめの特異値展開行列は得られない．そこで特異値展開して透かしを埋込む処理には，表面的には少なくとも一方向性がある事がわかる．本報告では，この一方向性の手がかりとして，透かし成分値の変化に対し，求まった特異値展開行列の変化を観察し，その連続性を調べる．結果は，ある種の不連続性があることが，実験上確かめられた．

2. Web 用の二段階電子透かしシステム

図 1 に二段階 web 画像認証システムを示す．第一段階は透かし入りの画像を公開する通常の場合で，第二段階は攻撃者がある画像の著作権を主張した場合の処理を扱う．第一段階では，攻撃による変形への耐性と Inversion Attack への耐性があるものと仮定する．著作権所有者 (Ow) は透かし入り画像から秘密検出鍵に相当する情報を用いて，透かしを検出することができる． Inversion Attack への耐性があるためには，この秘密検出鍵のみが検出を行うことができ，他の情報からは検出できないことが必要である．従って埋込み処理が擬似的な一方向性を有していれば良い．埋込みが加算であっても，埋込み規則に拘束条件を追加して，１：１から多：１へ変形できると考えられる．

第一段階で， Ow は，画像

$$G^1, G^2, \ldots, G^i \qquad (2\text{-}1)$$

に対し，透かし w を埋込み，

$$G_w^1, G_w^2, \ldots, G_w^i \qquad (2\text{-}2)$$

を得る． Ow はこの透かし入り画像を Web ページ上に公開する．ここまでは，埋込みの処理に関わる自己の作業以外に公的機関への登録手続きや登録料は発生しないため，これをフリーの公開段階と呼ぶ． Ow は検出鍵を秘密に保持し，公開しない．通常， Ow は画像に埋め込まれた透かしを自己認証でき，著作権を確認できるという状態が続く．

攻撃者 (At) が現れ，ある画像に対して著作権を主張した場合，第二段階に入る．第二段階は，争議段階で， Ow は第三者の公証人に秘密鍵に相当する情報を提出し，透かしの検証を依頼する．検証された画像とその原画像は，

$$G_w^c \text{ and } G^c \qquad (2\text{-}3)$$

である．埋込み透かしは完全であることを仮定しているので， Ow はこの認証を成功させ，訴訟により，著作権料を得て，それをもって，この画像を公的機関に有料登録し，以後は，電子すかしではなく公的な認証によって著作権の維持を図る．

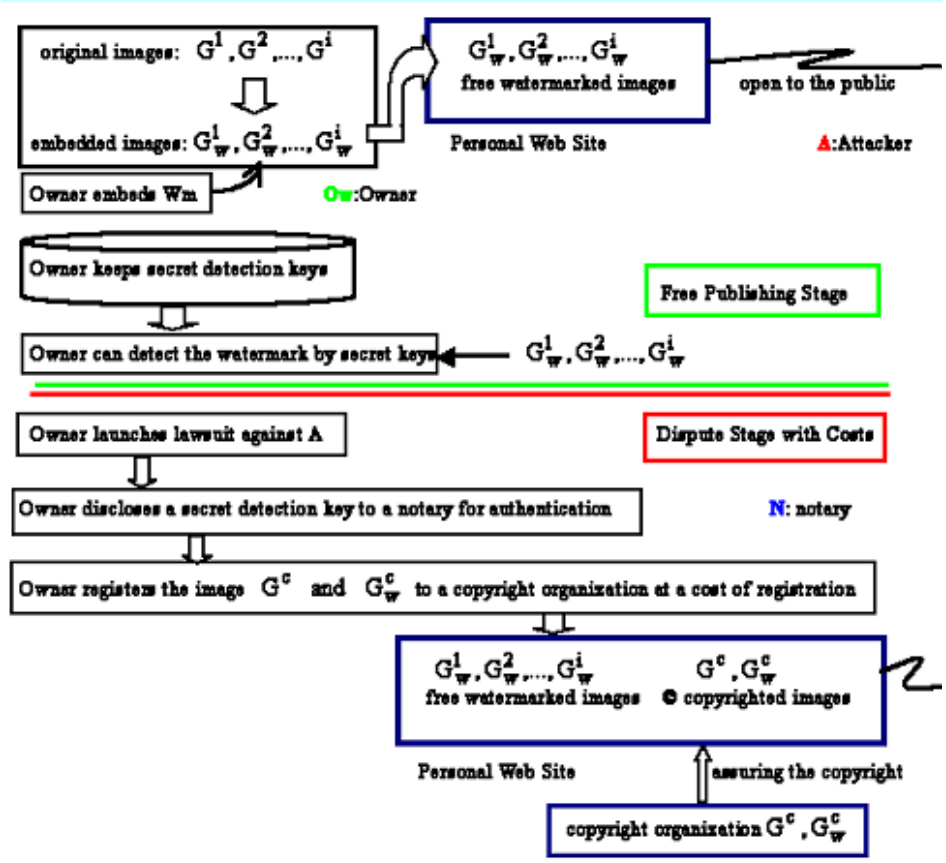

図 1　二段階 web 画像認証システム

Vol.2009-SE-164 No.5
Vol.2009-EMB-13 No.5
Vol.2009-CSEC-45 No.5
2009/5/28

3. SVD 電子透かしシステム

SVD 電子透かしシステムについては，既発表 [4] に述べられているが，一方向性の議論を精密化するために補足を行う．Gを正方の画像行列とする．長方形の場合も通常のSVDと同様の手法が適用できる．通常撮影された画像－これは自然画像と呼ばれる事が多い－は正方行列としたとき，正則行列になっていると考えられる．文献 [4] によると小数例ではあるが，CG などの人工画像を除き，全て正則であった．そこで，もし非正則であっても，画像サイズから１乃至は２程度の減少と予想され，その正則部分を代用すれば良いので，ここではほぼ正則と仮定して置く．G は極分解により，

$$G = |G| \cdot P \qquad (3.1)$$

ただし，$|G|$ は対称な正値行列，P は直交行列，に分解表現できる．$|G|$ は

$$|G| = Q^T \cdot S \cdot Q \qquad (3.2)$$

のように対角化できる．S は $|G|$ の固有値 λ_i を対角成分に持つ対角行列，各

$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N > 0$

は正の実数である．(3.1)と(3.2)から，

$$G = Q^T \cdot S \cdot Q \cdot P \quad , \qquad (3.3)$$

を得る．$U = Q^T$ ， $V = P^T \cdot Q^T$ と置くと，これらは直交行列となり，

$$G = U \cdot S \cdot V^T \qquad (3.4)$$

を得る．これがいわゆる特異値分解で，S は $G \cdot Gt = G \cdot G^T$ の固有値行列の平方根である．

極分解の仕方から，$|G|$ と P はユニークである．従って S もユニークであるが，U と V はユニークとはいえない．

3.1 SVD電子透かしの埋込み

透かしは特異値分解された領域で S に対して埋め込まれ，対角成分以外に 0 でない値を持つ透かし行列 W を加算することにより， SS=S+W となされる． U と V を乗ずることにより，

$$G_W = U * SS * V^T \qquad (3.5)$$

となり，埋込み画像 Gw が得られる．この画像だけを入手した第三者が特異値分解を行うと，

$$G_W = U_W * S_W * V_W^T \qquad (3.6)$$

ここで，一般には $SS \neq S_W$, $U \neq U_W$ ， $V \neq V_W$ となる．

埋込んだ W を推定することは難しいが，別の W’ で非対角成分に要素を持つ様な Uw’，Vw’ を作ることは，線型演算により可能である [3]．そこで，下記のような行列の階数を低下させる行列を乗じて，一方向性を高める工夫がなされている [3]．

$$SS = S * T_{k,k+1}$$

$$T_{k,k+1} = \begin{array}{c|cc|cc|cc|l} & & & k & k+1 & & & \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & 0 & \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & \\ 0 & 0 & \bullet & 0 & 0 & 0 & 0 & \\ \hline 0 & 0 & 0 & 1 & 1 & 0 & 0 & k \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & k+1 \\ \hline 0 & 0 & 0 & 0 & 0 & \bullet & 0 & \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \end{array}$$

3.2 埋込み処理の写像

画像に対してSVD埋込み処理への対応関係を写像 m として定義する．

$$m : G \rightarrow G_w \quad . \qquad (3.8)$$

図２に埋込み処理の関係を示す． Gから Gw を求めることが埋込みだが， Gw か

Vol.2009-SE-164 No.5
Vol.2009-EMB-13 No.5
Vol.2009-CSEC-45 No.5
2009/5/28

らSVDの分解行列UとVを求めることが，攻撃となる．上で見たようにUとVはユニークでは無く，U,Vから Gw を見ると多対１の関係になっており，一方向性の形式になっている．従って， Gw から U,V を求めることは，特に工夫をしない表面的な処理では困難と成る．しかし， U,V とは異なるものなら，非対角成分を生じる分解行列は求めやすい．そこで，階数低下を図ったものを使用すれば，線型演算で，単純な手法では，非対角成分を発生させる分解行列を求める事はできない．

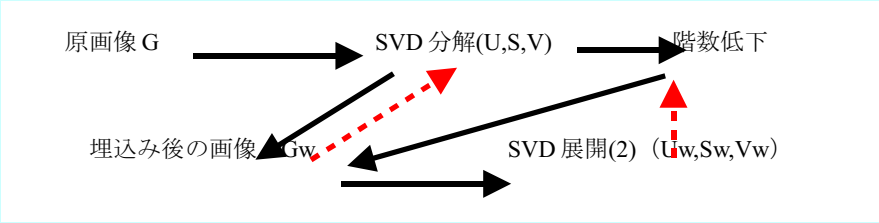

図２　埋込み処理の関係

3.3　疑似一方向性写像の評価

一方向性関数は数学的に厳密な定義があり，またその存在例が証明されていない．電子透かしや暗号に使用する場合，実用的な観点では，計算量が膨大であればよく，その観点で実施されている．具体的には，その画像の情報の価値と計算量が釣り合っていれば，無限の困難性を課する必要はない．つまり，表 3.1 のように，計算量的に，１日，１カ月，１年という複数のクラスを設け，画像の価値により，有限の計算量の疑似一方向性の透かしを埋込むことの意義は存在する．個人がホームページに画像を公開する場合は，現在では著作権も放棄したことになるが，有限であっても，一方向的な耐性があれば，無制限で自由な攻撃ができないだけでも現状より進歩があることになる．例えば表 3.1 のクラス１であっても，そこで埋込み画像から，透かし検出の鍵となる情報を求める特異値分解行列を求めることが多価写像になっている事から，この多価性を調べていく事が重要である．

表　3.1　解読計算量のめやす

クラス	解読計算時間
1	１日
2	１カ月
3	１年
4	１０年

4.0　数値解析

埋込み写像の逆演算の困難性を評価するため，特異値分解行列と埋込み後の画像から求まる特異値分解行列の距離を評価して，疑似一方向性を外部から観察していく．

4.1　ユークリッドノルムによる評価

U と Uw の距離， V と Vw の距離を調べた． SVDは基本比較であるので，式 (3.4) を用い， (3.7)は用いていない．ユークリッドノルムはユニタリ不変ノルムの典型例で，

$$\|X\|_2 = \left(\sum_{j=1}^{n} \sum_{i=1}^{m} |x_{i,j}|^2 \right)^{1/2} = \left(m \quad , \right)^{1/2} \qquad (3.8)$$

ただし， $n \le m$ で， $X = (x_{i,j})$ はユニタリ行列で，その固有値は，

$$\sigma_1 \ge \sigma_2 \ge \cdots \ge \sigma_m \ge 0 \qquad (3.9)$$

である．

透かし行列 Wの成分は振幅の変動と埋込み位置の変動がある．振幅の変動として ，振幅値 1,2,4,8,16,32 を用いて実験した．埋込みの位置としては，図 3(a) に示す 4×4 の小行列に対し，右上領域の 1 から６のどれかの点に１個だけの埋込みをする場合 ，２個４個をある特定の場所に埋込む場合， ８個を非対角の位置の特定の場所に埋込む場合について実験した．結果を図 3(b)-(d) に示す．埋込んだ透かしは Sw から得られる特異値に影響を与えている．図 3(b) によれば， SS の下方の方が特異値が小さいせいか影響が若干大きくなっている．原画と埋込み画像の差異を S/N で表したのが図 3(c) である．単一位置に異なる振幅の透かしを埋込み，計測をしている．これはきれいな比例を示している．図 3(d) は特異値分解行列の片方の U と Uw のユークリッドノルム距離である．埋込みの透かしの振幅値の増加に対し，ユークリッドノルム距離は，比例的でなく，むしろ緩やかな段差が見られる．ユークリッドノルム距離の式 (3.8)は要素の差の 2 乗和の平方根であるので，差に関し連続な関数である．しかるにこのような段差があるのは，不連続な要因を持つ可能性を示している ．ここまでの計測は， 4×4 画素の実画像から切り出した小画像ブロックに対するものである．

次に， 256×256 画素の実画像に対し，ノルム評価を行った．図 4 は透かしを埋込

Vol.2009-SE-164 No.5
Vol.2009-EMB-13 No.5
Vol.2009-CSEC-45 No.5
2009/5/28

むことによる変化に対する U と Uw の差の振る舞いを示すものである．埋込み位置は，特異値行列 S の 100 行の上である．第 100 番目の特異値は，(100,100)にある．これに対し，(100,P)， P=101,102,…,256 の位置に透かしを埋込む．埋込みの振幅値は，0.01,0.1,1.0,10.0,100.0を用いた．図 4 で最下の線はWの振幅 0.01 の場合を示す．そし

$$W = \begin{bmatrix} \bullet & 1 & 2 & 3 \\ \bullet & \bullet & 4 & 5 \\ \bullet & \bullet & \bullet & 6 \\ \bullet & \bullet & \bullet & \bullet \end{bmatrix}$$

Fig. 3(a) Embedding position for theupper-right part of the waterrmark matrix. The singular values are in the diagonal position. The size of the image is 4×4. W is added to S as SS=S+W.

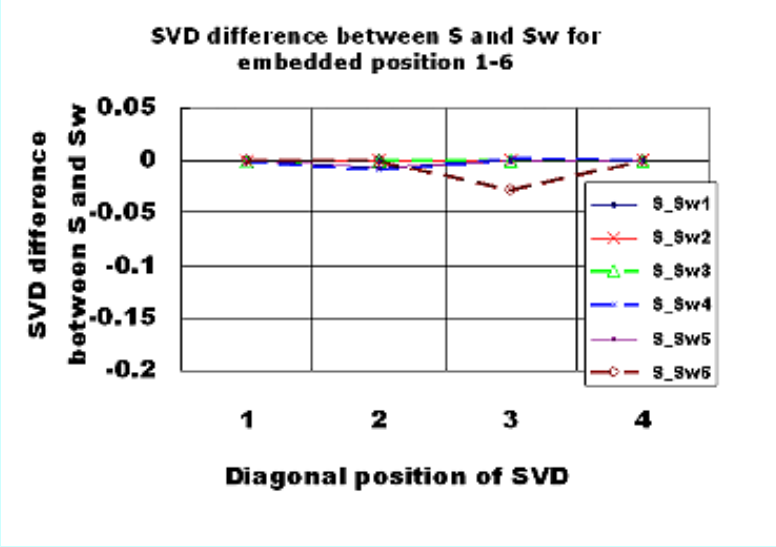

Fig.3 (b) SVD difference between S and Sw vs. SVD values. SVD values are sorted in descending order. Six embedding positions are investigated. The size of the image is 4×4.

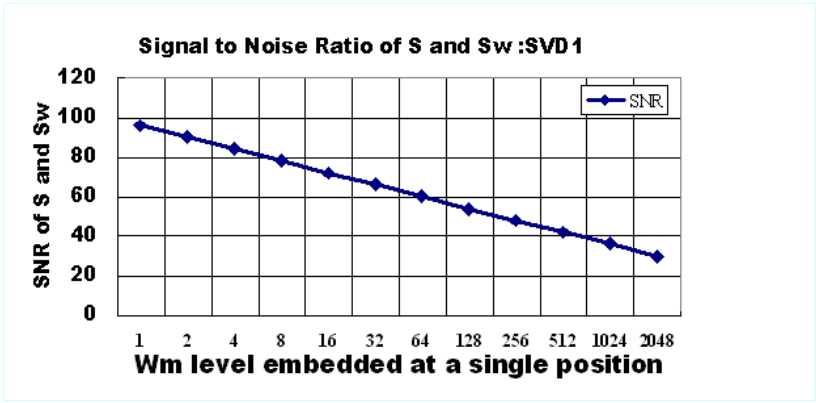

Fig. 3(c) Signal to nise rtio of an embedding error vs. the watermark's magnitude. The SNR is in dB, where the signal level is 255. The size of the image is 4×4.

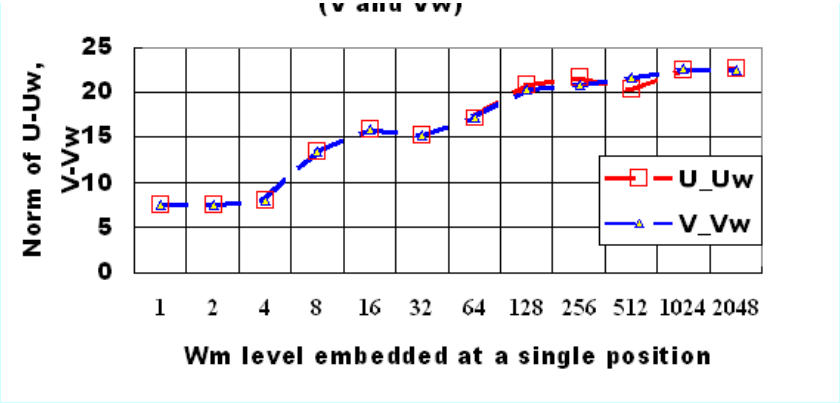

Fig 3(d) Norm difference between U and Uw vs. watermark magnitude. The norm is the Euclidean Norm. The size of the image is 4×4.

Vol.2009-SE-164 No.5
Vol.2009-EMB-13 No.5
Vol.2009-CSEC-45 No.5
2009/5/28

て，振幅が 0.1,1.0,10.0,100.0 の順に下から上に示されている．振幅が 0.1,1.0 の場合，多くの場所で，ノルム値の変動が大きくなっている．この変動は，同一埋込み位置の５本の線を垂直に見て，変動がある線に於いて，不連続になっていると解釈できる．振幅が 10.0,100.0 の部分では，変動が見られないが，縦軸は対数尺になっており，下の変動は実際の大差に埋もれていると考えられる．

次に，SVD電子透かしの埋込みに，式(3.7)も用いて階数の低下をさせた場合についての計測を示す．図５は埋込み位置の変化と誤差のノルム，画像の埋込み誤差を S/N で調べている．画像はSIDBAの標準画像” girl”である．式（ 3.7 ）の k の値が埋込み位置となり，図５の横軸の値に対応している．埋込み位置 k が大きくなるほど，S/N は緩やかに上昇している．また， U-Uw や V-Vw という差のノルムは緩やかに減少している．今回の実験では，埋込み位置が対角成分の隣に固定されている．また，埋込みの振幅も特異値の値に依存する．

次に式(3.7)を用いない場合（方式 1 ）と，用いる場合（方式２）の長所を組み合わせた方式を調べた．埋め込みの位置は方式 1 で定め，振幅は方式 2 で定まる固有値を用いるようにする．埋め込みの振幅値は固有値の値で与えられる．図６の LV は単一の透かしの埋め込みの振幅で劣化を与えた時， Numは複数の透かしで劣化を与えた時で，両者を合わせて劣化として横軸にとっている．縦軸は， U-Uw のノルムと V-Vw のノルムである．埋め込んだ手法の差異に関し，劣化量とノルムに一致性が見られる．

方式１で埋め込まれた後の画像の例を図７に示す．埋め込みによる劣化が観察しやすいよう，比較的大きな振幅値 W=1024 を埋め込んだ場合を示してある．うろこのようなSVDパターンが見られる．

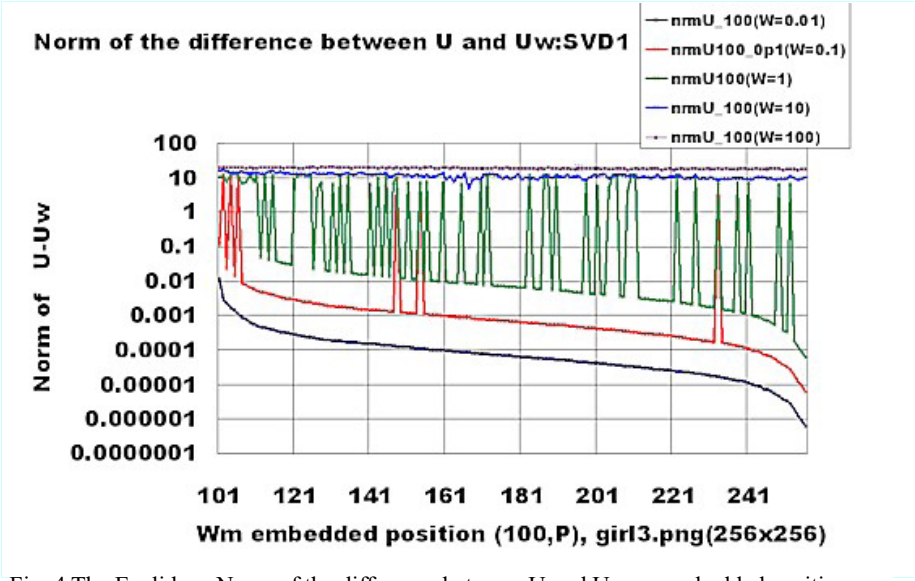

Fig. 4 The Euclidean Norm of the difference between U and Uw vs. embedded position. The magnitudes of the watermarks are 0.01, 0.1, 1, 10, and 100 from the bottom line to the top line respectively. The embedded positions are on the 100th row of the watermark matrix. The size of the image is 256×256.

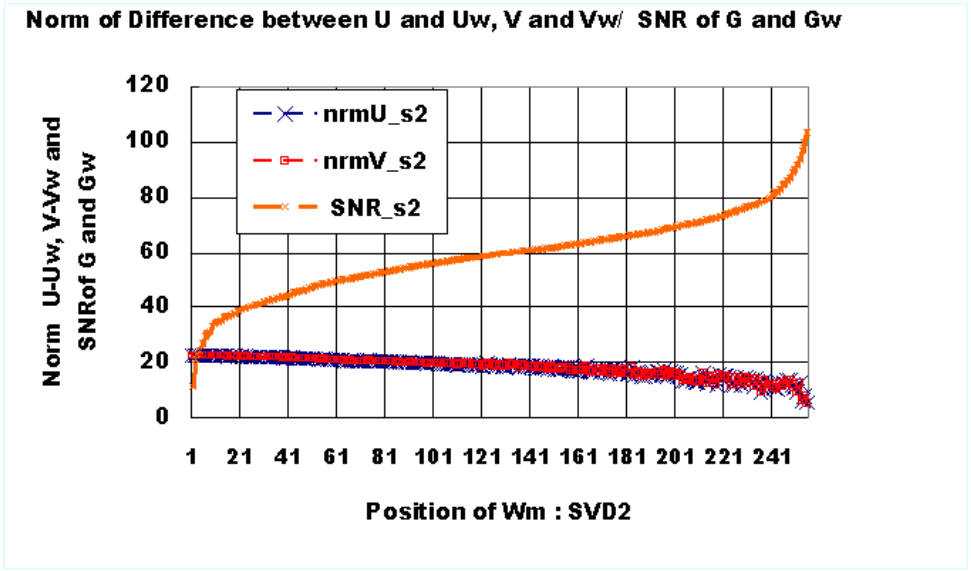

Fig. 5 The SNR of G and Gw vs. the embedding position at the uppermost line in dB. The Euclidean Norm of the difference between U and Uw (V and Vw). Both graphs are for the SVD2. The image “girl3.png”is monochrome. The size of the image is 256×256.

an

Vol.2009-SE-164 No.5
Vol.2009-EMB-13 No.5
Vol.2009-CSEC-45 No.5
2009/5/28

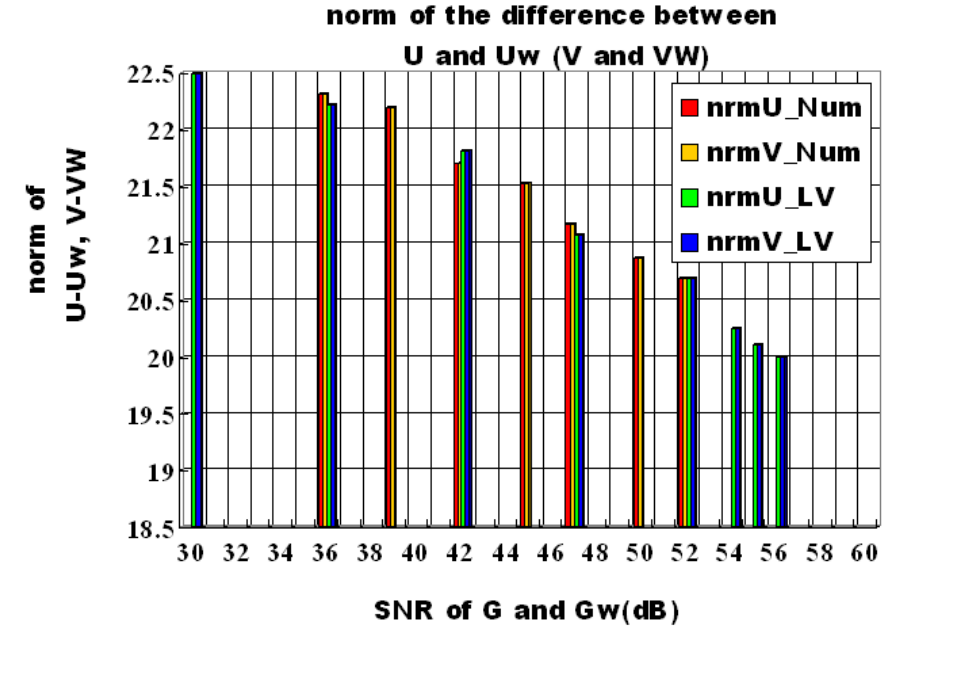

Fig. 6 The Euclidean Norm difference between U and Uw and (V and Vw) vs. the SNR of G and Gw. The image “girl3.png” is monochrome. The size of the image is 256×256.

4. おわりに

SVD電子透かし方式において，定式化を改良し， Inversion Attack を回避する方式２をの特性評価を行った．方式 1 には単純な Inversion Attack が存在するが，方式２は，構成の点で疑似的な一方向性を有しており，単純な Inversion Attack は行えない．

SVD分解行列の変化を数値的に調べる手法を提案した．埋込み透かしの微小な変化に対し，生成行列の差はノルム評価で，一部不連続的な変動が見られる．この不連続生は，埋込み写像が疑似一方向性を有する可能性を示すものである．

今後は，他のノルムでの評価，逆演算に必要な演算回数の評価等を行っていく．

Fig.7. An embedded image example with a large magnitude of watermark. （SVD1, A large magnitude of W=1024 is used to see the SVD noise pattern. The embedded position is (100,110)）.

Vol.2009-SE-164 No.5
Vol.2009-EMB-13 No.5
Vol.2009-CSEC-45 No.5
2009/5/28

参考文献

1) Luis Pérez-Freire, Pedro Comesaña, Juan Ramón Troncoso-Pastoriza, Fernando Pérez-González: : Watermarking Security: A Survey: Trans on Data Hiding and Multimedia Security I, pp. 41--72. (2006)

2) 叢力、大関和夫、「認証性を有する非対称な検出器公開型の電子透かし」電子情報通信学会、技術報告、情報セキュリティ研究会、 ISEC2006-72 、pp. 1-7、 (2006-09)

3) Kazuo Ohzeki, Engyoku Gi, “Quasi-One-Way Function and Its Applications to Image”, First International Symposium on Multimedia—Applications and Processing (MMAP), in International Multiconference on Computer Science and Information Technology (IMCSIT), pp501-508, Oct., 2008.

4) 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..