数理解析研究所講究録
第1684巻 2010年 93-113

多重解像度解析に基づくデータハイディングにおける流通画像中の秘密画像の視認困難性および機密性の向上

Improvement of visibility of the hiding key images in the publicly available hiding images for the data hiding method based on Multi-Resolution Analysis

新井康平
Kohei Arai
佐賀大学
Saga University

1．まえがき

ユビキタス社会の実現に呼応して、情報セキュリティの重要性が増している。ITC技術が情報の流通を促進し、情報活用が快適に行えるようになり、生活の質の向上に繋がっていることを実感するが、これは正の面である。その裏には安心･安全が脅かされる可能性という負の側面がある。個人情報の漏洩、情報改ざん、盗用、著作権侵害、サイバーテロ等日常茶飯に起きる事件は後を絶たない。個人の著作物はデジタル形式のファイル等で表されることが多いが、このデジタルコンテンツの著作物の著作権を主張する方法にも心許ないという現状がある。すなわち、盗用されたとしても著作権を主張する術を知らなければ著作権は守ることができないのである。デジタルフォレッジックスの重要性が叫ばれている。すなわち、証拠性である。著作権を侵害されたとの証拠性は如何に残せばよいのであろうか?この目的のため、また、デジタルコンテンツそのものを隠して送受者間のみにて隠した当該デジタルコンテンツを第三者には見えないように送受する方法がある。データハイディング技術である。データハイディングはステガノグラフィと電子透かし等の総称である。埋め込む情報が重要でありかつその存在が知られないことが重要な場合には，ステガノグラフィ、秘密の情報が埋め込まれたコンテンツ自体が重要な場合は電子透かしと一般に分けて呼んでいる[1]。また、ステガノグラフィではマルチメディアコンテンツの品質と埋め込み可能な情報量がトレードオフの関係にあるが，電子透かしでは更に攻撃に対する耐性と埋め込み可能な情報量がトレードオフの関係にある[2]。電子指紋システムのように、暗号プロトコルを効率良く行うために，計算量や通信量を抑えた方式が優れた方式とされる場合がある。また、埋め込まれた電子指紋を改ざんしたり，消去したりする攻撃に対して耐性のある電子透かし技術が重要である[3]。

本論文で紹介するデータハイディングは、著作権を主張できるように、デジタルコンテンツに著作者の秘密キーを流通コンテンツに忍ばせるものである。当該流通コンテンツが盗用された場合に当該秘密キーを知り得る著作者が当該流通コンテンツから取り出すことによって著作権を主張することを可能にするものである。その際、流通コンテンツに秘密

キーが視認できるようであってはならず、この視認困難性が重要である。また、流通コンテンツに秘密キーを忍ばせる方法に工夫を凝らし、機密性を高くすることも重要である。この方法の一つにウェーブレット多重解像度解析における分解要素に秘密キーを忍ばせる方法があり、特に、高いウェーブレット周波数成分に忍ばせると視認困難性は一般に高い[4],[5],[6],[7]。ウェーブレットに基づくデータハイディング方法にはこの多重解像度解析に基づく方法以外にも整数ウェーブレットに基づくヒストグラムギャップ法による可逆性データハイディングがある[8]。

秘密キーを埋め込む周波数成分を総当り法等によって探索されると秘密キーを盗用、改ざんされる恐れがある。したがって、単純に多重解像度解析を用いてデータハイディングを行うことは甚だ危険である。そのため、本論文では多重解像度解析によるデータハイディングに前処理を施し、それを施すことのできる著作者のみが知り得る前処理のパラメータも埋め込む周波数成分に係る情報と一緒に併せて持たなければ秘密キーを見つけ出すことができないように工夫した。

第 2 章において多重解像度解析に基づくデータハイディングを概説し、第 3 章では前処理に固有値展開を施す方法、斜交座標変換を行う方法、さらに、秘密キーのビット配列にランダム走査による配列順序変換、順列変換処理を行う方法を提案し、併せて典型的な標準画像データベースにある画像データを原画像に選んだデータハイディング処理を例示し、その機密性および流通コンテンツにおける秘密コンテンツの視認困難性を評価する。第 4 章は結論および今後の検討課題を述べる。

2．多重解像度解析に基づくデータハイディング

双直交ウェーブレット分解(たとえば、Daubechies 双直交基底関数[1]に基づく離散ウェーブレット変換(Discrete Wavelet Transformation: DWT)は原データ(一次元スカラーデータ：

---

[1] Daubechies 基底関数はコンパクトサポートなウェーブレット関数によって、以下の三式を満たす数列 $\{\alpha_k\}$ から求められる。この基底関数は不連続ではない。

$$\phi(x)=\sum_k \alpha_k \sqrt{2}\phi(2\pi-k)$$

$$\beta_k=(-1)^k\alpha_{1-k}$$

$$\varphi(x)=\sum_k \beta_k \sqrt{2}\phi(2\pi-k)$$

サポート長とはスケーリング関数 ϕ とウェーブレット関数 ψ からなる基底関数の長さである。上式における採り得る k のことをサポート長と定義している。すなわち、サポート長が 2 の Daubechies 基底関数は Haar 基底関数と同じであり、これが大きくなるにしたがって基底関数は滑らかになる。すなわち、ディジタルフィルタにおけるタップ数が大きい場合に相当する。この数列から求められる基底関数 Cn と対象データ f との線形変換を DWT と呼ぶ。

$f=(x_1,x_2,..,x_n)$に対して正方行列 Cn により、

$$F=Cn\,f \tag{1}$$

と定義できる。ここで、Cn は、

$$CnCn^t=I \tag{2}$$

となる双直交基底関数に基づく変換行列である。この Cn の要素は付録に示すように決定できる[2]。変換後の F は低周波分 L と高周波分 H からなる。すなわち、f は、

$$F=(H_1,L_1) \tag{3}$$

と変換される。ここで、H,L の添え字は変換回数、すなわち、段数(レベル数)を表す。また、この L_1 に Cn をかけることにより H_2,L_2 に、さらに、これを n 段繰り返すことにより、H_n,L_n と変換される。これをウェーブレット変換(分解)という。逆変換は、

$$Cn^{-1}=Cn^t \tag{4}$$

を F にかけることによって行う。逆変換を n 段繰り返すことにより、$f=(x_1,x_2,..,x_n)$が復元されることになる。これを再構成(離散ウェーブレット逆変換 IDWT: Inverse DWT)という。これを二次元データ、たとえば、画像に適用すると、

$$F=(HH_1,HL_1,LH_1,LL_1) \tag{5}$$

に変換される。ここで HH_1 は縦・横次元ともに高周波成分の意味であり、以下同様に LL_1 は縦・横次元ともに低周波成分を意味する。これを二次元ウェーブレット変換と呼ぶ。これを繰り返し、原画像データを各周波数成分に分解することができる。3 段までの二次元ウェーブレット変換を Fig.1 に例示する。

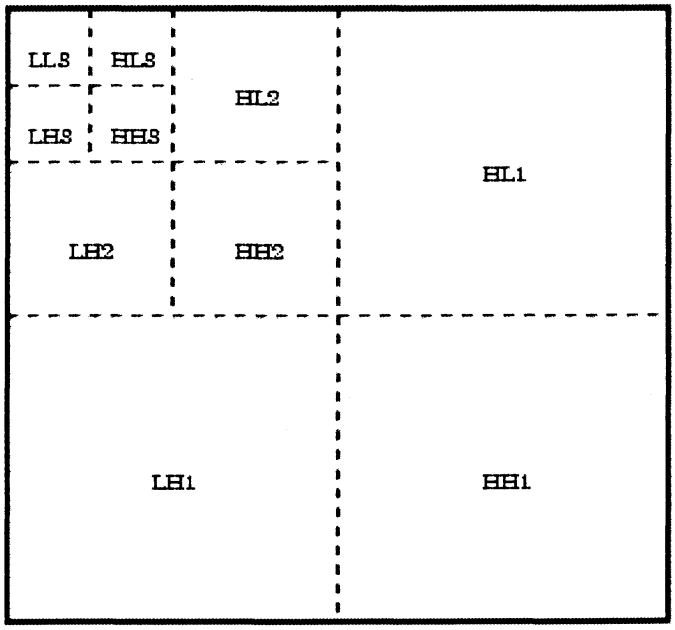


Fig.1 An example of DWT (The third stage of DWT)

[2] この係数方法は基底関数に依存しており、付録の例示は Daubechies 基底関数の場合のものである。

また、一次元データの場合と同様に逆変換を繰り返し、原画像データを安全に復元することができる(再構成)。これを多重解像度解析(Multi Resolution Analysis: MRA)と呼ぶ。また、動画像のように画像の時系列データである三次元データ f_{xyz} に対する三次元 DWT は、

$$F=[C_n[C_m[C_l f_{xyz}]']']' \tag{6}$$

で表される。したがって、DWT を n 個の時系列データに 1 段施すと n/2 個の高周波数成分と n/2 個の低周波数成分とに分解できる。この n/2 個の低周波数成分にさらに 1 段 DWT を施すとさらに、その n/4 個の低周波数成分と n/4 個の高周波数成分とに分解できる。これを繰り返すことにより、データ数は 1,2 個になる。この様子を Fig.2 に示す。これはラプラシアンピラミッドと呼ばれている。

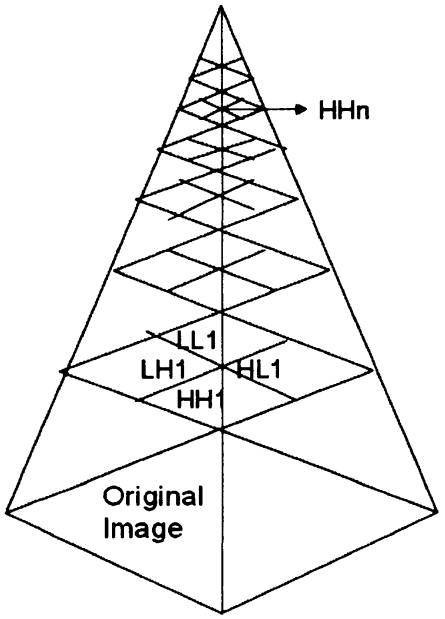


Fig.2 Laplasian pyramid

この場合、各段毎に画像のサイズは DWT により縦横ともに半分になる。これをダウンサイジングしない Dyadic Wavelet も提案されている。また、この場合、ある低周波成分画像は 4 つに分解されるが、これを 16 等に分解する Multi Wavelet も提案されている。それぞれ、ノイズ除去やデータ圧縮等に有効であるとの報告がある。これらの Wavelet およびその他多くの Wavelet について参考文献[9]の可視化情報学会誌特集号に掲載したので参照されたい。

この分解によって生成した各段の高周波数成分と低周波数成分を用いてウェーブレット逆変換(Inverse DWT: IDWT)を変換の段数分施せば完全にもとの時系列データが復元できる。この分解した周波数成分データのうち、「人間の目は高周波数成分の分解能が低い」ことを利用し、高周波数成分のいずれかに秘密データを埋め込み、秘密データを埋め込んだ状態にて再構成し、原画像レベルまで復元を試みると、秘密データは高周波数成分に埋め込まれているために視認困難な状態で原画像に似たデータが再構成される。このようにして生

成したデータを流通データ(コンテンツ)と呼ぶ。当該流通コンテンツは一般に公開するコンテンツであり、誰でもが入手可能である。したがって、盗用の危険性に晒されることになる。この流通コンテンツは元のコンテンツと殆ど同等であるが、高周波数成分に秘密データを埋め込んでいる点で元のコンテンツと異なる。当該流通コンテンツが盗用された場合であっても著作権者は高周波数成分に埋め込まれている秘密コンテンツ(たとえば、コピーライト)を抽出して見せることにより著作権を主張できるようになる。このような著作権を主張するための秘密データを著作コンテンツに埋め込み、流通画像を生成し、当該流通画像から秘密データおよび元のコンテンツを復元するまでの一連の処理フローを Fig.3 に示す。

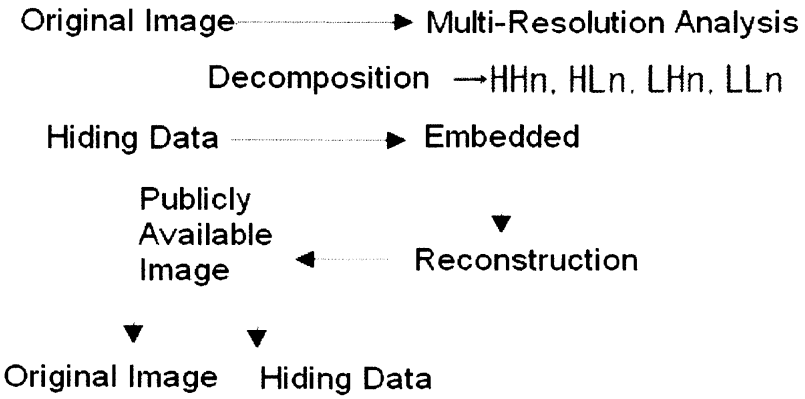


Fig.3 Process flow of data hiding based on Multi Resolution Analysis (MRA)

一例を示せば、以下のようになる。まず、Fig.4 の原画像(コンテンツ)に MRA を施し、Fig.5,6 の画像コンテンツ(1 段および 2 段)を生成し、流通画像中に視認困難なようにいずれかの高周波数成分に秘密データ(コンテンツ)を Fig.7(a)のように埋め込む。この場合、DWT1 段後の LH1 に埋め込んだ場合を想定して処理画像を示している。

Fig.4 Original image ("Lena" in the SIDBA image database)

Fig.5 The first stage of MRA

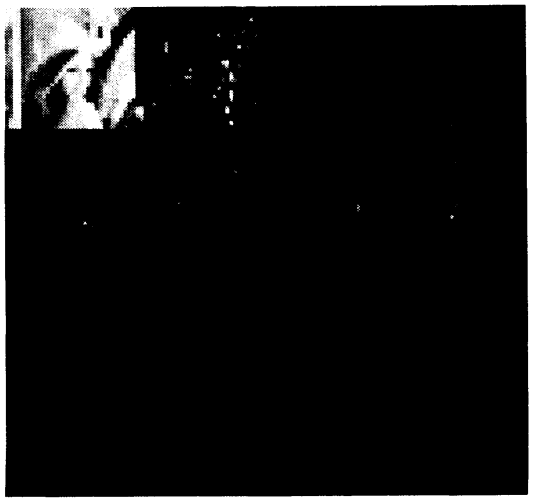
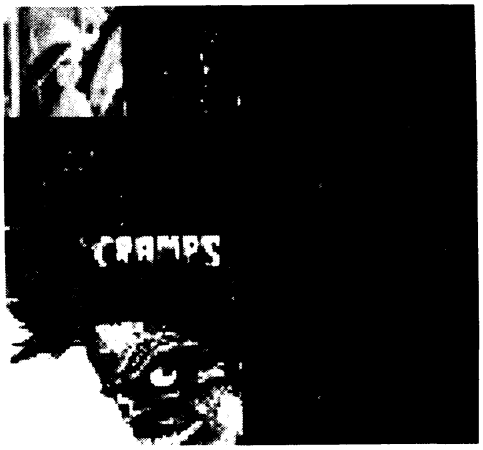


Fig.6 The second stage of MRA



(a) Hiding image with hidden location

(b) Reconstructed image

Fig.7 LH1 of MRA is replaced to the hiding image content of "CRAMPS".

再構成して得られる流通画像(コンテンツ)は同図(b)に示すように秘密データ(CRAMPS)が]視認可能である。したがって、埋め込む秘密データ(コンテンツの周波数成分)、埋め込む場所(周波数成分)によっては秘密コンテンツの流通コンテンツにおける視認困難性が大きく左右されることが分かる。そのため、Fig.8 に示すように秘密コンテンツを埋め込む場所は流通コンテンツにおける秘密コンテンツの視認可能性を考慮するうえできわめて重要な因子であるといえる。

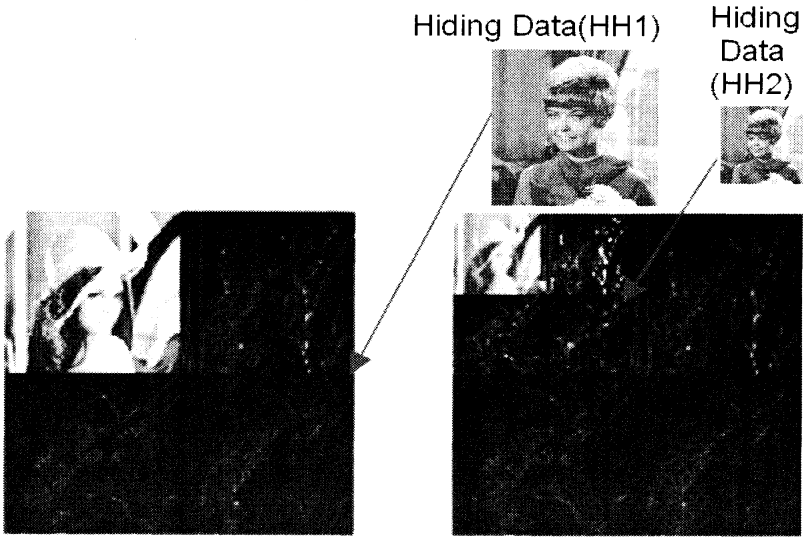


Fig.8 Hiding contents can be embedded in anywhere in the Laplasian pyramid

次に流通データコンテンツにおける秘密データコンテンツの視認困難性を評価する。このとき、視認困難性評価に用いる指標として、流通画像コンテンツと原画像コンテンツとの平均二乗偏差(RMSD: Root Sum Square difference)を用いた。原画像および秘密画像コンテンツをそれぞれ、Fig.9(a)および(b)に示す。また、HH1,HH2,HH3 および HH4 のそれぞれに秘密画像コンテンツを埋め込んだ場合の流通画像コンテンツを Fig.10(a),(b),(c),(d)にそれぞれ示す。さらに、原画像と秘密画像との平均二乗偏差(RMSD)を Table 1 に示す。表により明らかなように秘密画像を埋め込む高周波成分のレベルが高いほど RMSD が大きい。

Table 1 Root Mean Square Difference: RMSD between the original and publicly available image contents when the hidden image content is hided in the different level of high frequency components.

Level	RMSD
1	0.0137
2	0.0144
3	0.0153
4	0.0169

(a) Original image of content

(b) Hidden image of content

Fig.9 An example of original and hidden image contents.

(a) Hidden image content is hided in the level one (HH1)

(b) Hidden image content is hided in the level two (HH2)

(C) Hidden image content is hided in the level 3 (HH3)

(d) Hidden image content is hidden in the level four (HH4) .

Fig.10 Publicly available image contents which contains hidden image content in HH1,HH2, HH3 and HH4.

3．機密性および流通コンテンツにおける秘密コンテンツの視認困難性向上に有効なデータハイディングの前処理

3.1　主成分変換

Fig.10 により明らかなように高レベルの高周波成分に秘密画像データを埋め込んだ場合、流通画像上に秘密画像が視認できてしまう。また、秘密画像データを埋め込んだレベルおよび周波数成分の場所を探索することは容易にできてしまうことになり、秘密画像データを抽出されてしまう危険性がある。この危険性を回避し、かつ、視認困難性を向上するため、本論文ではMRAに基づくデータハイディングに前処理を施すことを提案している。すなわち、秘密画像データおよび原画像データの性質を知らなければ施すことのできない前処理を適用し、その後、MRAを伴うデータハイディングに基づき秘密画像データを埋め込む方法である。本論文ではこの前処理の一つとして主成分変換(固有値展開)を取り上げている。その手順を以下に示す。

(1)原画像(カラー画像を想定)に主成分変換を行う。

(2)第1主成分画像にウェーブレット分解を行う。

(3)ウェーブレット分解後の任意の高周波成分に秘密画像データを埋め込む。

(4)ウェーブレット再構成を行う。

(5)各主成分画像を用い、主成分逆変換を行い、流通用データを生成する。

(6)流通データを主成分変換し、第 1 主成分画像を生成する。
(7)ウェーブレット分解を行い、高周波数成分を抽出して秘密画像データを検出する。
一例として Fig.11 に示す SIDBA 画像データベース内の Mandrill を原画像として用い、埋め込む秘密データとして Fig.12 のグラフを用いる。原画像の RGB3 次元空間におけるヒストグラムは Fig.13 となる。

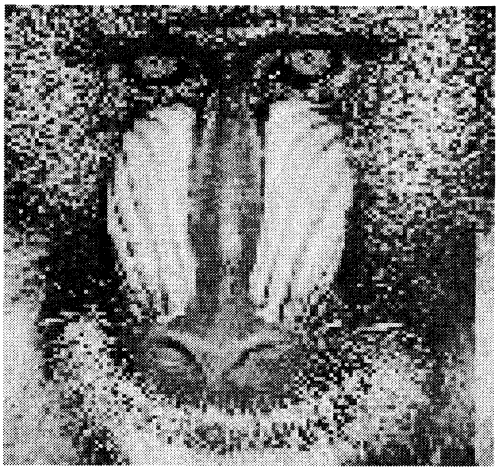


Fig.11 Original image of Mandrill

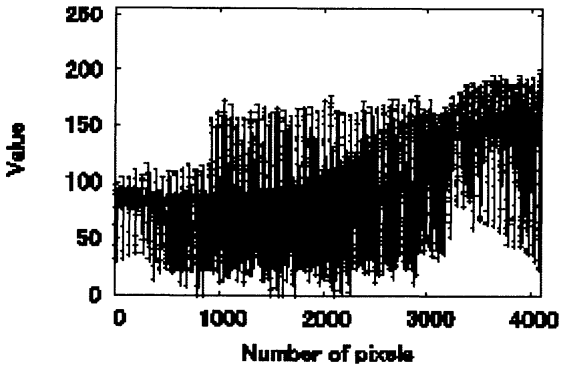


Fig.12 Hiding data

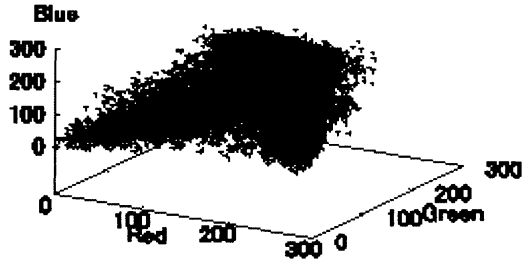


Fig.13 Three dimensional histogram of the original image of Mandrill.

この原画像のRG2次元平面における固有値、固有ベクトルを求めると、

λ =(133.772, 129.297)

V=|0.835　　0.550|

　|− 0.550　　0.835|

となっており、これによって主成分変換(固有値展開)を行うと、Fig.14となる。

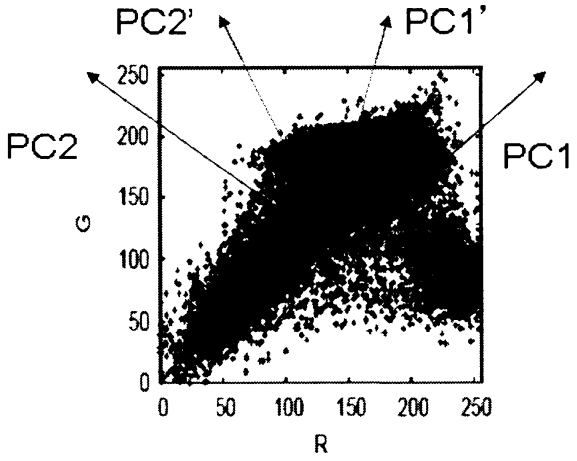


Fig.14 An example of PCA analysis (Principal Component Analysis) and slant coordinate system conversion as a preprocessing for the data hiding based on the MRA analysis.

この固有値および固有ベクトルはこれを知り得る著作者のみである。すなわち、3次元空間における主成分変換の変換行列は、

$$\begin{pmatrix} x_1^T \\ x_2^T \\ x_3^T \end{pmatrix} = \begin{pmatrix} 0.3765 & 0.5732 & 0.7277 \\ -0.9054 & 0.0614 & 0.4199 \\ -0.1959 & 0.8170 & -0.5421 \end{pmatrix}$$

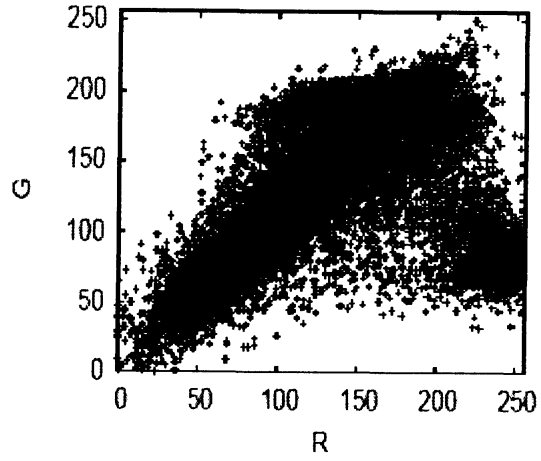
であるが、秘密画像データを埋め込んだ流通画像を用いて固有値、固有ベクトルを求めて固有値展開行列をもとめると、

$$\begin{pmatrix} x_1^T \\ x_2^T \\ x_3^T \end{pmatrix} = \begin{pmatrix} 0.3668 & 0.5800 & 0.7272 \\ 0.9095 & -0.0595 & -0.4113 \\ -0.1953 & 0.8124 & -0.5494 \end{pmatrix}$$

となる。したがって、当該流通画像からは秘密データを復元するに足る固有値展開行列は抽出不可能であり、よって、これを改ざんすることもできない。しかし、情報ハイディング後のデータを整数に変換しない場合の当事者による秘密データ抽出結果のRMS誤差は零であるが、情報ハイディング後のデータを整数に変換した場合の当事者による秘密データ抽出結果のRMS誤差は零ではないので当事者は差分情報を確保する必要がある。

3.2　斜交座標変換

さらに、この秘匿性を向上させるため、前処理に斜交座標変換を施すことも可能である。直交カーテシアン座標を斜交座標に変換するとこの斜交座標の角度も著作者のみが知り得る鍵となり、より秘匿性が向上する。たとえば、前出の Fig.14 に斜交座標変換の施し、Fig.15 のように、まず、元の RG2 次元散布図を主成分変換し、その後、Fig.16 のように斜交座標に変換することが可能である。これにより、データの定義領域を狭小化することによるデータ圧縮との親和性が図られ、かつ秘匿性が飛躍的に向上することが可能である。



RGB カラー原データの R 成分と G 成分の散布

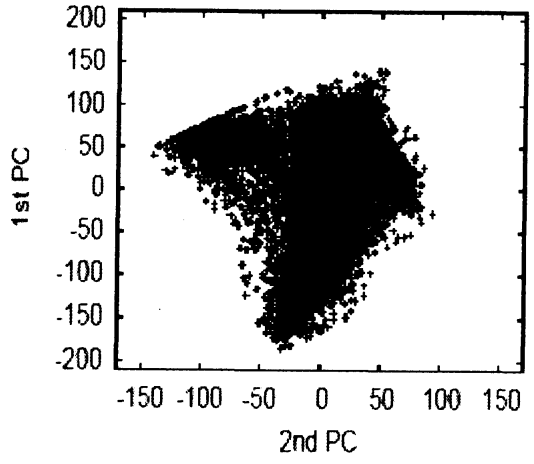
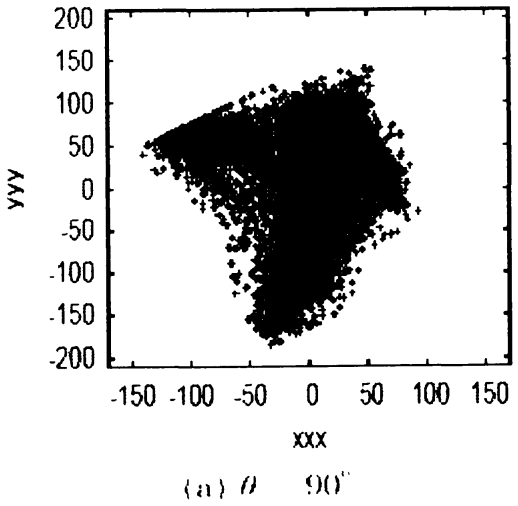
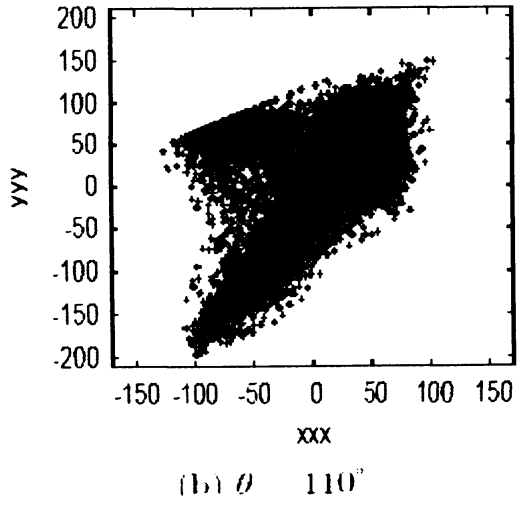


Fig.15 2D scatter diagram for both original and PCA applied images.



(a) θ 90°



(b) θ 110°

Fig.16 Examples of scatter diagrams after oblique coordinate transformation.

このとき、斜交座標変換軸角度によって秘匿性の効果およびデータ圧縮率との親和性および圧縮率そのものも変化する。Fig.17 に斜交座標変換した画像に基づき復元した画像と原画像との平均二乗誤差を評価した結果を示す。

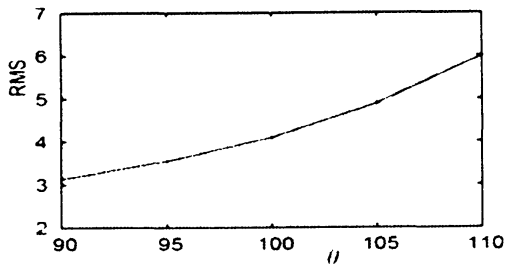


Fig.17 Root mean square error between the original and reconstructed image with the image after the oblique slant coordinate system conversion.

また、斜交座標変換し、データ圧縮して画素値の定義領域を変更後復元して原画像との平均二乗偏差を評価した結果を Fig.18 に示す。

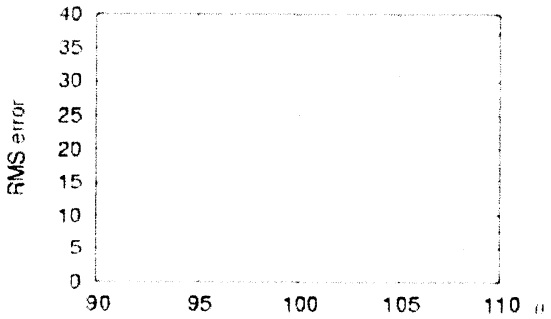


Fig.18 Root Mean Square error between reconstructed and decompressed image and the original image

さらに、原画像に故意に重畳させた平均値 0 で標準偏差 sigma の正規乱数をパラメータとした場合の RMSE を Fig.19 に示す。

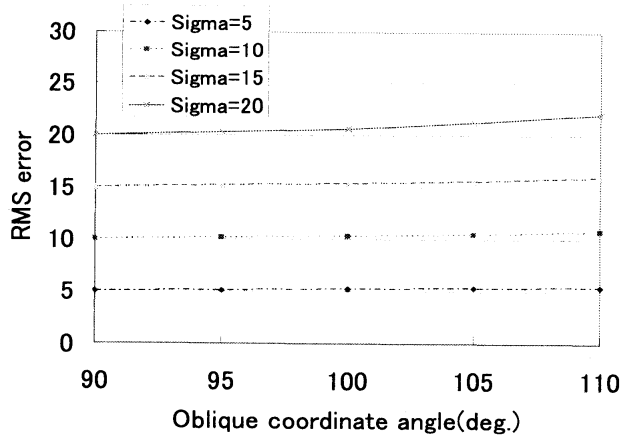


Fig.19 RMSE between oblique coordinate conversion and decompressed image and the original image when the normally distributed random noise is added.

この提案方法の処理フローを Fig.20 に示す。

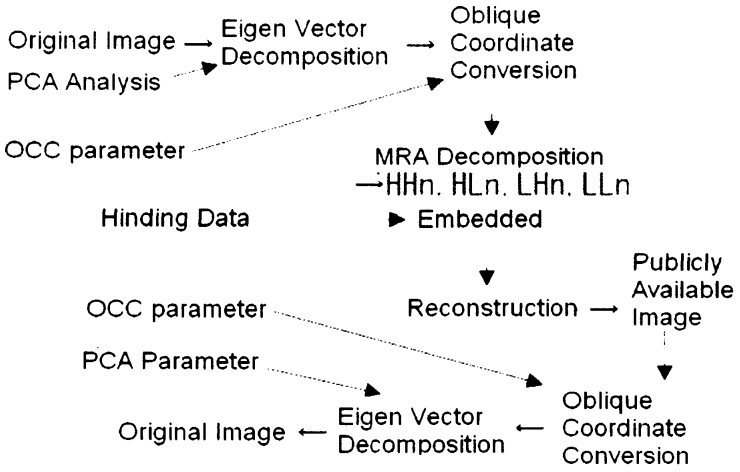


Fig.20 Process flow of data hiding based on MRA with PCA conversion and oblique coordinate system conversion.

また、画像例を含む理解しやすい形式による、MRA に基づき PCA,OCC を伴う提案データハイディング方法を Fig.21 に示す。

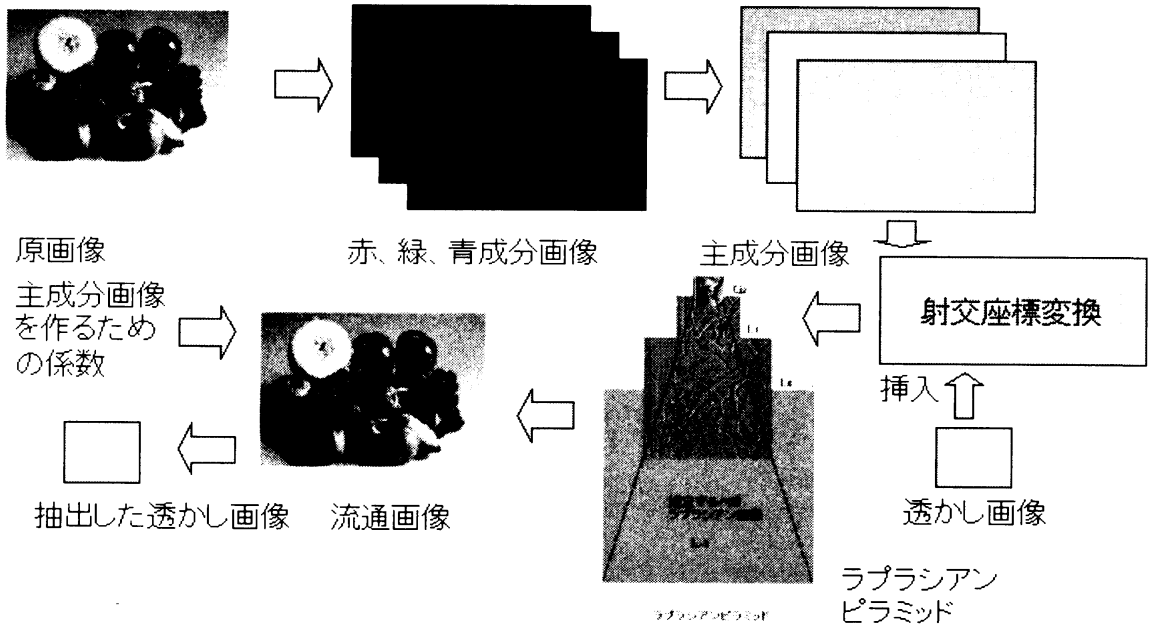


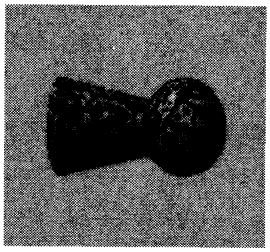
Fig.21 Process flow of the proposed data hiding with preprocessing of Principal Component Analysis and oblique coordinate system conversions

この提案方法の特徴として、(1)複合分布の着目分布のみの主成分による座標変換、データ圧縮が可能、すなわち、次元縮退が可能であり、情報損失もともなう、(2)座標変換を斜交

座標への変換を導入し、より分布を偏らせた座標返還が実現し、高効率圧縮が可能であり、これは定義領域縮退することによる効果であるが、S/N は劣化する。また、これを電子透かしの前処理に用いることにより、より機密性が向上すると期待できる。さらに、前処理を電子透かしに施すことにより機密性向上することが確認でき、100%確実に原本証明が可能であることを立証することができた。したがって、著作権保護が可能であり、電子透かし情報に時刻コードや処理パラメータ等を挿入することが可能であることが分かった。提案方法はコピー管理や編集に利用が可能であることが分かった。

3.3　走査方式を考慮したデータハイディングにおける秘密画像データの視認困難性の向上

秘密画像データの走査方式を通常の線逐次走査からランダム走査に変更して流通画像における秘密画像の視認困難性を向上することができる。一例を Fig.22 に示す。Fig.22(a)は秘密画像の一例である。これを前出の原画像(Lena)の HH1、HL1、LH1 のそれぞれに挿入した場合の流通画像を Fig.22(b),(c),(d)にそれぞれ示す。



(a)Hidden image

(b) Publicly available reconstructed image through embedding the hiding image at HH1 component.

(c) Publicly available reconstructed image through embedding the hiding image at HL1 component.

(d) Publicly available reconstructed image through embedding the hiding image at LH1 component.

Fig.22 Hidden image and publicly available reconstructed images through embedding the hiding image at HH1, HL1 and LH1 components.

Fig.22 から明らかなように秘密画像データは流通画像上に視認することができる。この秘密画像データを Fig.23 に示すように線逐次走査からランダム走査に変更し視認性を向上する。

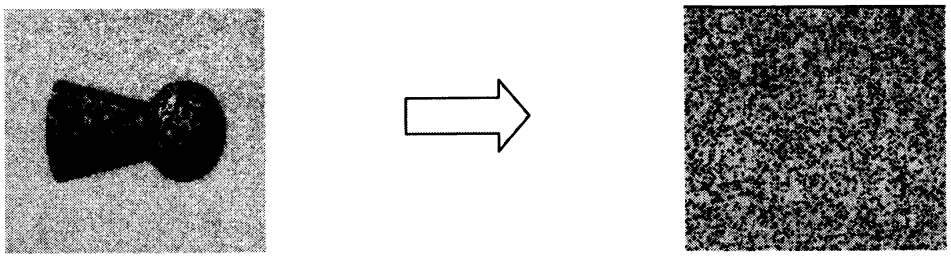


Fig.23 Scanning scheme conversion from the line-by-line to random.

Fig.24(a),(b),(c)にこの走査方式の変更に伴う流通画像上の秘密画像データの視認困難性の向上結果を示す。Fig.24(a),(b),(c)は前出の原画像(Lena)の HH1、HL1、LH1 のそれぞれに挿入した場合の流通画像をそれぞれ示す。

(a)HH1

(b)HL1

(c) LH1

Fig.23 Hidden image and publicly available reconstructed images through embedding the hiding image at HH1, HL1 and LH1 components after the scanning scheme conversion for hidden image from line-by-line to random.

MRAに用いたDaubechies基底関数のサポート長(dbn)およびランダム走査に用いる一様乱数の初期値(rand50/5000)をパラメータとして線逐次走査(Normal)およびランダム走査(rand)における流通画像と原画像との平均二乗偏差RMSDを比較してみるとTable 2のようになっており、この結果から、ランダム走査は線逐次走査よりも良好であること、サポート長が長い方が短いよりも良好であること、乱数の初期値にはさほど影響されないこと等が分かる。

Table 2 Comparisons of Root Mean Square Difference (RMSD) between the original and the publicly available reconstructed images through data hiding based on MRA with embedding the hiding image to HL1, HH1 and LH1 and with scanning scheme conversion from line-by-line to random.

	HL1	HH1	LH1
Nomal(db2)	69.594	69.137	69.183
Nomal(db4)	69.397	69.089	69.058
Nomal(db8)	69.518	69.069	69.056
rand50(db2)	68.790	68.297	68.340
rand50(db4)	68.609	68.215	68.247
rand50(db8)	68.568	68.135	68.123
rand5000(db2)	68.856	68.357	68.427
rand5000(db4)	68.665	68.291	68.316
rand5000(db8)	68.633	68.182	68.202

流通画像上の秘密画像データの視認性は用いる乱数の初期値に依存しないため、送受当事者間でこの初期値をステガノグラフィにより隠蔽しておけば、この初期値を知っている当事者間のみが当該秘密画像データを復元することができるようになる。

4．あとがき

ウェーブレットとして Daubechies(双直交基底を採用したが、双直交ウェーブレットであれば鍵画像(または、秘密画像データ)情報を復元できることを実証した。また、双直交ウェーブレットとして何を採用するかの情報を隠蔽することによっても鍵画像情報を保護することができること、画像の横方向の双直交ウェーブレットと縦方向の双直交ウェーブレットとが同じものである必要はないこと、秘密データの挿入位置も自由に選択できること、秘密データのビット列を分割して任意の高周波成分に挿入することも可能であること、秘密データのビット列数（情報量）によって情報隠蔽能力が変化すること、流通データにおける秘密データの視認困難性向上に固有値展開、斜交座標変換、ランダム走査は有効であること、走査方式種類選択、乱数初期値を当事者間のみで共有することは秘匿性向上に有用であることを示した。また、ノイズに対する耐性、データ圧縮に対する耐性、データの改ざんに対する耐性を示した。さらに、秘匿性を向上するためのアルゴリズムはあえて公開するべきであると考えている。

参考文献

[1] Tirkel, A., et al., "Electronic Water Mark" Proceedings DICTA 1993, 666-672, 1993.[2] Fabien A. P. Peticolas, Ross J. Anderson, Markus G. Kuhn : "Attacks on copyright marking systems", David Aucsmith(ed), Information Hiding, Proceedings, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp.219-239. 1998.[3] H. Keith Melton : "The Ultimate Spybook", Dorling Kindersley Limited, London, (画像の構成要素の一部を変更する方式), 1996.[4] 新井康平、瀬戸要、ウェーブレット多重解像度解析に基づくデータハイディング、可視化情報学会誌、Vol.22, Suppl.No.1, 229-232, 2002

[5] 新井康平，瀬戸要，固有値展開による情報の偏りを利用した多重解像度解析に基づくデータハイディング，可視化情報学会論文誌，Vol.23, No.8, pp.72-79,2003.

[6] 新井康平、特許出願番号：2004一29933、電子透かし挿入・抽出装置及び方法

[7] 新井康平、PCT 出願番号：PCT/JP2005/13512、座標変換方法、それを用いたデータ圧縮及びデータハイディング方法及びそれらの装置, 2005.

[8] Yao Qiuming, Xuan Guorong, Yang Chengyun, Shi Yunquin,