白鷗大学論集　第14巻　第2号

論文

電子透かしシステムの構築とその評価

黒　澤　和　人

Implementation of a Digital Watermarking System on PC and Its Evaluation.

Kazuto Kurosawa

目　　次

1．はじめに

情報化社会の進展に伴って、ディジタルコンテンツの流通が活発に行われるようになってきている〔1〕〔2〕。しかし、その反面、たとえばインターネット上のWWWや、ＣＤ－ＲＯＭなどの媒体を通して配信されるテキスト、画像、音声などのディジタルデータに対して、不正コピー、改竄、無断使用などの、いわゆる著作権の侵害に当たると考えられる行為が、多方面で発生するようになってきている〔3〕〔4〕〔5〕〔6〕。これらは、品質の劣化を伴わずに、複製を簡単に作れるというディジタルデータ特有の性質を悪用するものである。このような状況に対して、著作権を保護するための対策の1つとして、**電子透かし技術**の有効性が注目されるようになってきている〔7〕〔8〕〔9〕。

電子透かし技術とは、保護の対象となるオリジナルデータに対して、その冗長性を利用して著作権者を特定するためのデータ（簡単に**透かしデータ**と呼ぶ）を密かに埋め込み、また必要に応じてそれを取り出す技術のことである。この電子透かし技術を利用すれば、たとえば、コンテンツの不正コピーや改竄などの行為を発見した場合には、著作者しか知り得ない透かしデータをコンテンツから実際に取り出して見せることによって、当該コンテンツが確かにコピーされたものであることを立証することが可能となる。あるいはまた、透かしデータを、はじめから判読できる形で埋め込んでおくことによって、犯罪の抑止に役立てたり、または見本品としてインターネット上のWWWサーバに展示しておき、料金と引き換えに透かしデータが除去され、ダウンロード可能となるなどの仕組みを導入するといった方法も考えられる。

電子透かしの技術は、テキスト、画像、音声データなどの著作権保護を目的として、最近利用が活発化し始めた比較的新しい技術である。したがって、実際には、透かしデータがコピーを繰り返すうちに失われたり、通信の途中の激しいノイズに打ち消されたりすることもあり、乗り越えなけれ

ばならないさまざまな技術的問題が残されている。また、既に市販品となった電子透かしシステムもあるが、外部からのあらゆる不正な攻撃にも耐え得る、十分安全と言える透かし技術は未だ開発されていないといってよい〔7〕〔11〕。そのため、データ埋め込みの理論的研究と並行しながら、活用場面ごとにプロトタイプを組み立てつつ、電子透かしシステムの標準案の設計を試行しているというのが現状である。

今回、筆者は、パーソナルコンピュータ上に、ウェーブレット変換を応用した「濃淡画像に対する電子透かしの埋め込みシステム」をインプリメントするとともに、追跡不能性を有する認証システム（いわゆるブラインド署名）の機能を付加した「電子透かしおよび認証のための統合システム」（仮称ＤＷＳ－ＵＵＥＡ：The Digital Watermarking System with Untraceability, Unreusability, and Emergency Accessibility）を構築したので報告する。本システムでは、インターネットやＣＤ－ＲＯＭなどの電子媒体を利用して画像の交換を行う際に、オリジナル画像に著作者を特定する画像を埋め込み、不正な利用に対する対抗手段となることを目的とするものである。また、埋め込みデータの所有者の認証を行う際に、所有者情報を署名者から追跡不可能にするためのブラインド署名のアルゴリズム、および緊急時にオリジナル画像へのアクセスを許す緊急アクセスのためのアルゴリズムを組み込んだものである。

本システムの構築に当たっての理論的基礎は、画像データの圧縮技術として中心的役割を果たしているウェーブレット変換、および電子現金システムの実現の基礎となっている追跡不能性を実現するためのディジタル署名の理論である。

今後の課題としては、今回作成したプロトタイプを元に、カラー画像への対応、透かし情報への攻撃に対する耐性の強化を図ることである。また、将来、経営分野や教育分野などにおいても、実際に利用可能なシステムとなるよう改善を図りたいと考えている。

なお、本システムの開発に当たっては、統合開発環境としての Delphi、言

語処理系としてのObject Pascal、およびリレーショナルデータベース開発環境としてのInterBaseを利用した。

2．問題の背景

2.1 情報化社会の進展とディジタルコンテンツの流通

情報化社会の進展に伴って、ディジタルコンテンツの流通が活発化してきている〔1〕〔2〕。ディジタルコンテンツの具体的な姿は、ディジタルデータとしてのテキスト、図形、音声、静止画、動画像などであるが、さらに次の2点に注意しておく必要がある。

まず第1に、ディジタルデータは、アナログデータと異なり、画質や音質の劣化を伴わずに、何度も繰り返しコピーを取ることが可能である。したがって、オリジナルデータを一度コピーしさえすれば、同じ品質の商品を半永久的に保持し続けることが可能となる。その結果、オリジナルデータと区別のつかない多数のコピーが出回ることになる。

そして第2に、ディジタルコンテンツのノン・パッケージ流通の傾向が、最近特に強まってきている〔13〕。これまでは、書籍、CD、ビデオなどのパッケージに収められて店頭に並べられてきたものが（パッケージ流通）、インターネットなどを媒介とすることによって、ディジタルデータの形そのままに、好きなときに、好きな回数、供給源から直接配信を受けることが可能になっている。

その結果、配信されるディジタルコンテンツに対して、不正コピー、改竄、無断使用などの、いわゆる著作権の侵害に当たると考えられる行為が、多方面で発生するようになってきている〔3〕〔4〕〔5〕〔6〕。また、この傾向は、パソコンやAV機器等の性能が向上し、またネットワーク環境の整備が進むのに伴って、ますます深刻な問題となってきており、法律分野においても多くの検討が行われつつある〔3〕〔4〕〔14〕〔15〕〔16〕〔17〕〔18〕。

図１は、ここでの問題を模式図で表したものである。電子美術館のホームページに展示してある図画を、契約者Ａがダウンロードし、未登録者Ｂがそれを不正コピーした例を示している。

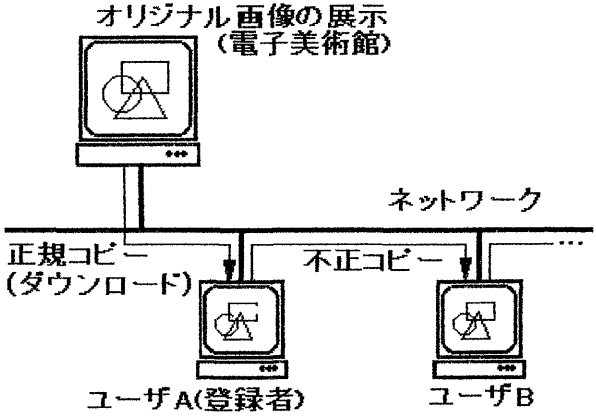

図１：不正コピーの例

この他、ディジタルコンテンツの流通に関する不正な行為として、たとえば次のようなものが考えられる。

・ホームページに展示してある有料画像を、所有者に無断でダウンロードし、自分のホームページの壁紙として使用する。
・ＣＤから録音した楽曲をパソコンで圧縮ファイル化し、インターネット上で不特定多数の人に頒布する。
・新刊の書籍や雑誌のページを文字認識装置で読み取り、パソコンでテキストファイル化し、形式を整えて配布する。

一方、この問題を技術的な面から捉えると、このような不正アクセスからディジタルコンテンツを守る方法として、１つには、パッケージを封印したり、データ全体を暗号化してしまう方法が考えられる。しかしその場合、利用者は購入前に中身を見ることができないため、旧来のパッケージ流通と本質的に変わるところがなく、商品の自由な流通が妨げられる恐れ

がある。また、封印が解かれあるいは暗号が復号された後は、コピーや再配布に対する防御策は意味をなさなくなってしまう。

そこで第２の策として、著作者自身が自分の著作物の利用状況を把握でき、使用者が中身を見てから購入するかどうかを決められ、復号後も効力を持ち得るガードシステムが必要となる。その１つの候補として、**電子透かし技術**が位置付けられている〔7〕〔8〕〔9〕。

電子透かし技術とは、保護の対象となるオリジナルデータに対して、その冗長性を利用して著作者を特定するためのデータを、**透かしデータ**として密かに埋め込み、また必要に応じてそれを取り出す技術のことである。この電子透かし技術を利用すれば、たとえば、コンテンツの不正コピーや改竄などの行為を発見した場合には、著作者しか知り得ない透かしデータをコンテンツから実際に取り出して見せることによって、当該コンテンツが確かにコピーされたものであることを立証することが可能となる。

図２は、著作権を保護するための電子透かしシステムの利用法を、模式図で表したものである。電子美術館のホームページに展示してある図画を、契約者Ａがダウンロードし、未登録者Ｂがそれを不正コピーして Ｂのコン

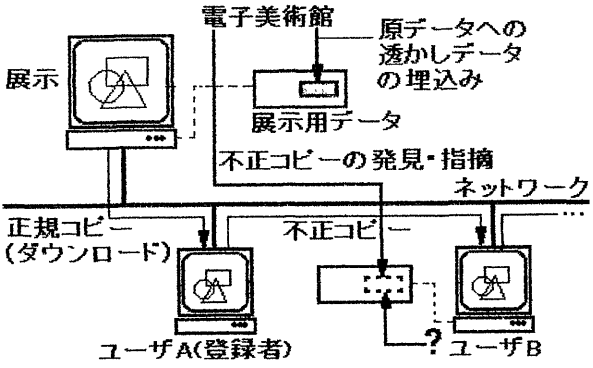

図２：電子透かしの利用例

ピュータ上で展示してあるところを美術館側が発見し、指摘する例を示している。

この他、透かしデータの利用法として、はじめから可視的な状態で埋め込んでおくことによって、犯罪の抑止に役立てたり、または見本品としてインターネット上のWWWサーバに展示しておき、料金と引き換えに透かしデータが除去され、ダウンロード可能になるといった仕組みも考えられる。

2.2 透かしデータの種類

情報化社会の要請と、そこで流通するディジタルコンテンツの特性から、電子透かしシステムの基本的な仕組みを、ここでは次のように捉える。

――コンテンツの製作者ないし配布者は、著作権の保護に役立てるために、しかるべき情報をコンテンツ自体に透かしデータとして密かに埋め込み、配布し、利用者にそれを意識させずに利用してもらう。しかし、利用者が法律に定める範囲を超えた場合は、透かし情報を復元し、著作権侵害であることをアピールする。(図3～5参照)。――

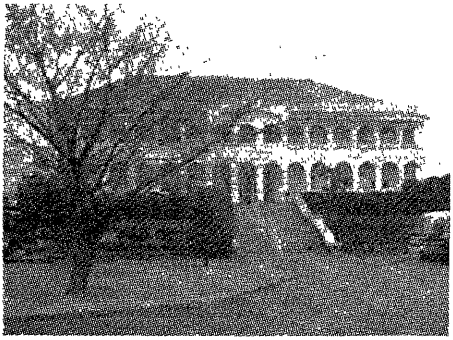

図3：原画像

図4：透かしデータ

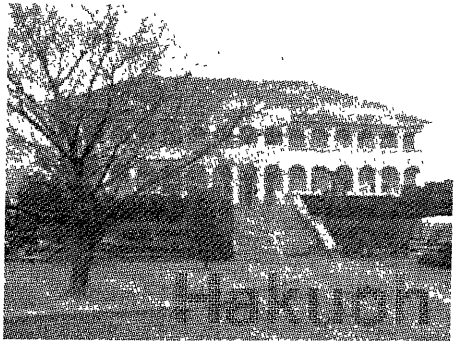

図５：可視的に埋め込んだ例

さて、現在までに提案されている電子透かしシステムでは、各提案の中で必ずしも明確に述べられているわけではないが、透かしデータの利用法としてたとえば次のようなものを想定していると考えられる〔7〕〔13〕。

(1) 著作者情報の記録

著作権侵害に抵触する利用がなされた場合に、透かしデータを復号して、問題の処理に当たるために、コンテンツの製作者あるいは版権者に関する情報を透かしデータとして埋め込む。この場合、透かしデータの情報量は少なくてよいが、利用者には完全に隠蔽されていることが望ましい。

(2) 購入者情報の記録

コンテンツの一部に可視的にマークのようなものを付し、正規の方法で入手した者のみがマークを除去できるようにする。しかし、実は、透かしデータには、購入者情報も埋め込まれており、その者が第三者にそのマーク除去済みコンテンツを再配布すると、再配布コンテンツには、除去したはずのマークとともに、購入者番号が浮き上るように仕組んでおく。これによって違法コピーの抑止を目指す。

配布コンテンツは、マーク入りのため鑑賞には適さないが、サンプルと

して使用することはできる。

(3) 利用者情報の追跡

コンテンツの利用者が変わるたびに、利用者情報を透かしデータとして記録する。利用者情報としては、契約上のＩＤ番号やＩＰアドレスなどが考えられ、コンテンツの違法コピーの流通経路を追跡することができる。しかし一方では、個人情報の取り扱い上問題とされることも有り得る。

(4) 制御信号の埋め込み

コピープロテクトの破壊や大量コピーを企てる悪質な利用者に対しては、コピープロテクトの制御信号を、直接、透かしデータとして埋め込むことも１つの対策となる。

(5) 極秘情報の伝送

透かしデータを通信秘匿に利用するもの。暗号に似ているが、電子透かしでは信号そのものを隠す。一般に、アナログ／ディジタル変換の過程で、少なからず変換誤差が混入する。この誤差部分を、透かしデータの埋め込み領域として利用することが可能である〔37〕。

2.3 電子透かし技術の要件

電子透かしは、コンテンツそれ自体の中に、オリジナルデータとは異なる別のデータを新たに埋め込むために、それが一種の雑音の役割を果たし、コンテンツの商品価値を著しく低下させてしまう可能性がある。この品質の劣化の程度が、コンテンツの流通の鍵ともなる。

また、流通するディジタルコンテンツから透かしデータを復号し、埋め込まれた著作権情報を不正に取り出し、虚偽の著作権情報に改竄するという行為も予想される。このような悪意による透かしデータの変更に対する耐性も持たせる必要がある。

一般に、技術的には、透かしの秘匿の強度を強くすれば、その分コンテンツの品質が劣化し、かといってコンテンツの品質を一定に保とうとすれば、秘匿効果は低下する傾向があり、コンテンツの質と耐性強度は互いに

トレードオフの関係にあるといってよい。

そこで、電子透かし技術に求められる要件を、以下に整理しておくことにする〔7〕〔8〕〔10〕。

(1) 透かしデータは、ヘッダ部などのような特定領域ではなく、コンテンツ自身に埋め込まれること。できれば、コンテンツ全体に渡って埋め込まれるのが望ましい。

(2) 透かしデータは、不可避的に行われるコンテンツの処理（編集、圧縮、伝送等）に対して変化しないこと。特に、画像の一部が切り取られたり、圧縮されても正しく透かしデータを復号できること。また、伝送路のノイズにも撹乱されないこと。

(3) 透かしデータの改竄や削除など、悪意による攻撃に対して耐性をもつこと。

(4) 透かしデータをコンテンツ全体に、繰り返しかつランダムに配置できるアルゴリズムを有すること。

(5) 透かしデータの埋め込みの手間が軽減されること。特に、リアルタイムで通信が行われるインターネットなどでは、手軽に透かしデータの埋め込みと復号ができることが重要である。

(6) 結託攻撃（透かし入りのコンテンツを正規に入手した複数の人あるいはコンピュータが、データを持ち寄って透かしの仕組みを不正に解読すること）を排除できることが望ましい。

(7) 画像フォーマットなどのコンテンツの仕様に制約を受けない透かし方式であること。

(8) コンテンツが本来有している品質を、ある程度に保持できること。たとえば、透かしデータを改竄しようとすると、その痕跡が残るような構造にすること。

(9) 改竄の痕跡を残さないための修復費用が、正規のコンテンツの購入費用を上回ること。

(10) 電子透かしのアルゴリズムに暗号化の概念を導入すること。たとえば、

(4) $\forall t \in \mathbb{R}: f(t) \in V_j \leftrightarrow f(2^m t) \in V_{j+m}$.

(5) 且つ $\varphi(t) \in V_0$; $\{\varphi(t-k)\}_{k\in\mathbb{Z}}$ は V_0 の正規直交基底である。

注意4.12 $\varphi(t)$ はスケーリング関数であり、2進表現した

$$\varphi_{j,k}(t) = 2^{\frac{j}{2}}\varphi(2^j t - k)$$

は、V_j の正規直交基底となる。このとき、スケーリング関数 $\varphi(t)$ は、$L^2(\mathbb{R})$ の多重解像度解析 $\{V_j\}_{j\in\mathbb{Z}}$ を生成するという。

記号4.13

- ヒルベルト空間 $\mathcal{H}$ の点列 $\{e_j\}_{j\in J}$ に対して、

$$Span\{e_j\} = \{\sum_{j\in J} a_j e_j \mid a_j \in \mathbb{C} \text{ のうち有限個の } a_j \text{ を除き } 0\}$$

のとき、集合 $Span\{e_j\}_{j\in J}$ の $\mathcal{H}$ における閉包を $\overline{Span\{e_j\}_{j\in J}}$ と書く。

- $\langle \varphi_{j,k}, \psi_{j,l} \rangle = 0 \ (j,k,l \in \mathbb{Z}, \varphi_{j,k} \in V_j, \psi_{j,l} \in W_j)$ が成り立つことを、$V_j \perp W_j$ と書く。

- $V_j \oplus W_j$ を、V_j と W_j の直交和と呼び、互いに直交する成分の和集合で一意的に表現されることを意味する。

注意4.14 レベル j の近似関数 f_j は f_{j-1} から情報が欠落しているので、この不足分 $g_j(t)$ を $f_j(t)$ に補って、

$$f_{j-1}(t) = f_j(t) + g_j(t)$$

と書ける。また、このとき、f_j はスケーリング関数 $\varphi(t)$ の、g_j はウェーブレット $\psi(t)$ の、それぞれ一次結合で表される。これを整理したのが、次の定理である [22]。

定理4.15 $\{V_j\}_{j\in\mathbb{Z}}$ は $L^2(\mathbb{R})$ の多重解像度解析であるとする。また、

- $V_j \perp W_j$,
- $V_j \oplus W_j = V_{j-1}$,

によって、$L^2(\mathbb{R})$ の閉部分空間の列 $\{W_j\}$ を作るとき、$\{\psi(t-k)\}$ が W_0 の正規直交基底ならば、

$$\begin{cases} \varphi_{j,k}(t) = 2^{-\frac{j}{2}}\varphi(2^{-j}t-k) & : スケーリング関数 \\ \psi_{j,k}(t) = 2^{-\frac{j}{2}}\psi(2^{-j}t-k) & : ウェーブレット関数 \end{cases}$$

は、それぞれ V_jおよび W_jの正規直交基底となり、φ と ψで $L^2(R)$ 空間を張ることができる。すなわち、任意の $f_j \in V_j, g_j \in W_j$は、$\varphi_{j,k}(t)$ をスケーリング関数、$\psi_{j,k}(t)$ をウェーブレット関数として、

$$\begin{cases} f_j(t) = \sum_k s_k^{(j)}\varphi_{j,k}(t) \\ g_j(t) = \sum_k w_k^{(j)}\psi_{j,k}(t) \end{cases}$$

のように、一意的な級数で表される。

4.2 高速ウェーブレット変換アルゴリズム

4.2.1 離散ウェーブレット変換

注意4.16 レベル jのスケーリング係数 $s_k^{(j)}$から、1 レベル精度の低いウェーブレット展開係数 $w_k^{(j+k)}$およびスケーリング係数 $s_k^{(j+1)}$を導出する手順を次に述べる〔20〕〔21〕。

アルゴリズム4.17（離散ウェーブレット展開）

(1) 連続信号 $f(t)$ のレベル0の近似関数 f_0は、レベル0のスケーリング関数 $\varphi(t-k)$ によって

$$f(t) \simeq f_0(t) = \sum_{k\in Z} s_k^{(0)}\varphi(t-k) \in V_0$$

と展開される。ここで、

$$s_k^0 = \int_{-\infty}^{\infty} f(t)\overline{\varphi_{0,k}(t)}dt$$

であるが、具体的には、マラーの方法にしたがい、信号をサンプリングして得られる数列 $f(n)$を、最初に与えられる離散データ $s_k^{(0)}$とみなす〔20〕。

(2) 次に、$s_k^{(0)}$をもとに、0以外のレベルのスケーリング係数 $s_k^{(j)}$を求める。ここで、p_nは展開係数である。

は、抽出に失敗することが多く、また、埋め込み手法や透かし情報の漏洩しやすい傾向がある。

このタイプの透かし方式としては、たとえば〔29〕〔32〕〔33〕〔34〕〔35〕〔36〕などがある。

3.3 電子透かしの安全性

電子透かしへの攻撃には、透かしデータの解読、改竄、撹乱、削除などがあるが、たとえ故意でなくとも、簡単な画像処理によっても大きな被害を被ることは十分有り得る〔10〕。また、埋め込みシステムそれ自体の不正や、透かしデータを第３者が管理する場合などに生じるプライバシーの侵害の問題も考慮する必要がある。

静止画像への透かしデータに対する攻撃手段としては、たとえば次のようなものが考えられる〔７〕〔10〕〔11〕。

・アフィン変換　いわゆる画像の拡大、縮小、回転等の座標変換。
・加工処理　画像の一部切り出し、サンプリング等。
・フィルタリング　エッジの強調、スムージング、高周波成分のカット等。
・非可逆データ圧縮　ＪＰＥＧ圧縮等。
・ＤＡ－ＡＤ変換　プリンタ出力をスキャナで読み込む等。

電子透かしに対するさまざまな攻撃法を集約した評価ツールとしてStirMarkがある〔10〕〔11〕〔38〕〔39〕。既に実用化されている電子透かしシステムについても、その多くが破壊可能であることが示されている〔38〕〔39〕。そのため、透かし技術は、未だ発展途上の技術と言わざるを得ないというのが現状である。

次に示すシステムは、いずれも市販されている電子透かしシステムの例である。しかし、実際のところ上記のベンチマークテストにおいて、破壊可能と診断されたものも含まれている。

・Digimarc社のPicture Marcは、静止画用電子透かしのためのAdobePhotoshopのプラグインソフトである。固定鍵を使い、MarcCenterと呼ばれるセン

トラル管理サイト経由で変換が必要となる公共透かしを提供している。ランダムパターンブロック符号化を適用している。

・Signum Technologies 社の SureSign は、コンピュータに取り付けたドングルの情報が比較処理で利用される。これは、Signum 社のセントラルデータベースで管理される。透かしの埋め込み手法は、ランダムパターンブロック符号化法を使用している。

・Signafy 社（ＮＥＣによって設立）の InvisibleInk は、静止画にメッセージを埋め込むことを目的に、離散コサイン変換を利用したスペクトル拡散符号化法を適用している。特徴は、埋め込みデータの復号時に、埋め込み画像とオリジナル画像との比較を行う点である。オリジナル画像はサーバで管理される。

・Blue Spike 社の Giovanni は、透かしを抽出するために、オリジナルデータを必要としない。周波数に基づくフレームベースのため、部分的にカットされた断片からの透かしの復元を容易にしている。ユーザは個別の鍵を作成して利用できる。また、別々の鍵を使って、別の透かしを同時に埋め込めるなどの利点を持っている。

・ＩＢＭ社の DataHiding は、Adobe Photoshop およびWWWブラウザ用のプラグインソフトである。信頼性が比較的高いことが指摘されているが、埋め込み手法の内容は不明である。

4．アルゴリズムの導出

高速フーリエ変換（ＦＦＴ）や離散コサイン変換（ＤＣＴ）は、計算量の低減とともに、画像の冗長度を圧縮する目的で、画像の時系列信号を空間周波数に直交変換する方法として知られる。しかし、これらの直交変換は、ブロック単位で実行されるために、量子化が粗い場合には、ブロックの境界部分に出る不連続な歪み（ブロック歪み）やエッジ部の雑音やにじみ（モスキート雑音）が発生しやすいなどの欠点をもっている〔7〕〔19〕。

この弱点を克服する手段として、本システムでは、ウェーブレット変換による画像のサブバンド符号化法を導入することにした〔7〕〔8〕〔20〕〔21〕〔22〕〔29〕。

4.1 ウェーブレット変換の定式化

まず、本節では、ハールウェーブレット(Haar Wavelet)を用いた画像データの直交ウェーブレット変換について整理しておく〔20〕〔21〕〔22〕。

注意4.1 実数 R 上で定義された関数 f のうち、

$$\int_{-\infty}^{\infty} |f(t)|^2 dt < \infty$$

を満たすものを2**乗可積分関数**と呼び、その集合を $f \in L^2(R)$ で表す。また、

$$< f, g >= \int_{-\infty}^{\infty} f(t)\overline{g(t)}dt \qquad (f, g \in L^2(R), \bar{g}\text{は}\ g\ \text{の複素共役})$$

によって内積を定義し、さらにこの内積を使って $f \in L^2(R)$ のノルム $||f|| = \sqrt{< f, f >}$ を定義する。これによって、$L^2(R)$ を、有限次元ユークリッド空間 R^n の無限次元への拡張であるヒルベルト空間 $\mathcal{H}$ として考えることができる。

記号4.2 関数 $\psi(t)$ に対して、$C_\psi = \int_{-\infty}^{\infty} |\hat{\psi}(\omega)|^2/|\omega| d\omega$ とおく。

定義4.3(ウェーブレット) 関数 $\psi(t) \in L^2(R)$ を考え、$\hat{\psi}(t)$ を $\psi(t)$ のフーリエ変換とするとき、$\psi(t)$ が

$$\int_0^{\infty} \frac{|\hat{\psi}(\omega)|^2}{\omega} d\omega = \int_0^{\infty} \frac{|\hat{\psi}(-\omega)|^2}{\omega} d\omega = \frac{1}{2} C_\psi < \infty \qquad (1)$$

を満たすとき、$\psi(t)$ を**アナライジングウェーブレット**あるいは、単に**ウェーブレット**と呼ぶ。

定義4.4(ウェーブレット変換) ウェーブレット $\psi(t)$ を任意に選び、t 軸方向にシフトあるいは拡大縮小(ダイレーション)して

$$\psi_{a,b}(t)=\frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right)\qquad(a,b\in R,a>0)\tag{2}$$

を生成する。ここで、bはシフト、aはダイレーションの度合いを表し、$1/\sqrt{a}$ は正規化のための係数である。このとき、$\psi_{a,b}(t)$ と $f(t)$ との内積

$$(W_\psi f)(b,a)=\frac{1}{\sqrt{a}}\int_R f(t)\overline{\psi\left(\frac{t-b}{a}\right)}dt$$

を信号 $f(t)$ の**ウェーブレット変換**という。また、式(1)が成り立つとき、関数 $f(t)\in L^2(R)$ が連続となる点 $t\in R$ において、次の逆変換が成り立ち〔22〕、これを**ウェーブレット逆変換**という。

$$f(t)=\frac{2}{C_\psi}\int_0^\infty\left[\int_{-\infty}^{\infty}(W_\psi f)(b,a)\psi_{a,b}(t)db\right]\frac{da}{a^2}$$

定義4.5（2進ウェーブレット）式(2)において、a,bをそれぞれ2進分割して、$a=2^j,b=2^jk$とすると、ウェーブレット$\psi(t)$は次のように離散化できる。

$$\psi_{j,k}(t)=2^{-\frac{j}{2}}\psi(2^{-j}t-k)\tag{3}$$

注意4.6（正規直交性）式（3）の形の$\psi(t)$をうまく選ぶと（つまり適当なj,kを選ぶと）、$\{\psi_{j,k}\}$を正規直交系にすることができる〔20〕。なお、シフトに関する$\{\psi_{j,k}\}$の正規直交性とは、

$$<\psi(t-k),\psi(t-n)>=\begin{cases}1 & (n=k)\\ 0 & (n\neq k)\end{cases}$$

が成り立つことである。また、ダイレーションに関する正規直交性とは、

$$<2^{-\frac{j}{2}}\psi(2^{-j}t),2^{-\frac{n}{2}}\psi(2^{-n}t)>=\begin{cases}1 & (n=j)\\ 0 & (n\neq j)\end{cases}$$

が成り立つことである。このとき、次が証明される〔20〕〔21〕。

定理4.7（ハール ウェーブレット）式(4)および図6に示す**ハールウェーブレット**は、シフトとダイレーションに関する正規直交条件を同時に満たす。

$$\psi(t) = \begin{cases} 1 & (0 \leq t < \frac{1}{2}) \\ -1 & (\frac{1}{2} \leq t < 1) \\ 0 & (\text{その他}) \end{cases} \tag{4}$$

また、任意の信号 $f(t)$ は、このハールウェーブレットを基底として、

$$f(t) = \sum_j \sum_k w_k^{(j)} \psi_{j,k}(t) \tag{5}$$

の形に級数展開できる。このとき、$w_k^{(j)}$は、シフト k、ダイレーション j の**ウェーブレット展開係数**と呼ばれ、次式で与えられる。

$$w_k^{(j)} = \int_{-\infty}^{\infty} f(t)\overline{\psi_{j,k}(t)}dt = < f, \psi_{j,k} >$$

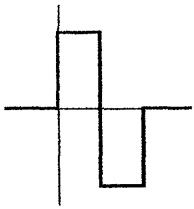

図６：ハールのウェーブレット

定義4.8（スケーリング関数） 信号 $f(t)$ の近似関数 $f_0(t)$ を、ある関数 $\varphi(t)$ の１次結合として

$$f_0(t) = \sum_k s_k \varphi(t-k)$$

と表せるとき、$\varphi(t)$ を**スケーリング関数**、s_kを**スケーリング係数**と呼ぶ。

注意4.9

- 近似関数 $f_0(t)$ の添え字0は、近似のレベルを表し、レベル0の場合が最も近似の精度が高いものとする。
- 式(6)および図７に示す**ハールのスケーリング関数**は、信号を観測するための尺度として一般的によく利用される。

$$\varphi(t)=\begin{cases}1 & (0\leq t\leq 1)\\ 0 & (\text{その他})\end{cases} \tag{6}$$

・ハールのスケーリング関数は、整数シフトが正規直交系をなす〔20〕。

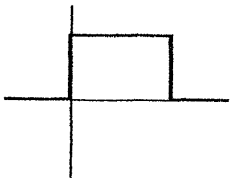

図7：ハールのスケーリング関数

定義4.10 ウェーブレットと同様に、スケーリング関数 $\varphi(t)$ についても、整数シフトと整数ダイレーションを考え、２進表現を用いて、

$$\varphi_{j,k}(t)=2^{-\frac{j}{2}}\varphi(2^{-j}t-k) \tag{7}$$

と定義する。また、この $\varphi_{j,k}$ を用いて、レベル j の近似関数 $f_j(t)$ を

$$f_j(t)=\sum_k s_k^{(j)}\varphi_{j,k}(t)$$

と定義する。ここで、$\varphi_{j,k}(t)$ が、シフトについて正規直交であるなら、スケーリング係数 $s_k^{(j)}$ は、次式で与えられる〔20〕。

$$s_k^{(j)}=\int_{-\infty}^{\infty} f(t)\overline{\psi_{j,k}(t)}dt$$

定義4.11（多重解像度解析） $L^2(R)$ の閉部分空間の列 $\{V_j\}_{j\in z}$ が次の条件を満たすとき、$\{V_j\}_{j\in z}$ を**多重解像度解析**と呼ぶ〔21〕。

(1)$\cdots\supset V_{j-1}\supset V_j\supset V_{j+1}\supset\cdots$（$\{V_j\}_{j\in z}$ は減少列であるという。）

(2)$\bigcup_{j\in k} V_j=L^2(R)$

(3)$\bigcap_{j\in k} V_j=\{0\}$

(4)$\forall\ t \in R\ ;\ f(t)\ \in\ V_j \Leftrightarrow f(2^{-n}t) \in\ V_{j+n}$

(5)$\exists \varphi\ (t) \in\ V_0\ ;\ \{\varphi\ (t-\ k)\}_{k\in z}$は V_0の正規直交基底である。

注意4.12　$\varphi(t)$ はスケーリング関数であり、２進表現した

$$\varphi_{j,k}(t) = 2^{-\frac{j}{2}}\varphi(2^{-j}t - k)$$

は、V_jの正規直交基底となる。このとき、スケーリング関数 $\varphi(t)$ は、$L^2(R)$ の多重解像度解析$\{V_j\}_{j\in z}$を生成するという。

記号4.13

・ヒルベルト空間$\mathcal{H}$の点列$\{e_j\}_{j\in J}$に対して、

$$Span\{\ e_j\}=\{\sum_{j\in J} a_j e_j \mid\ a_j \in\ C\text{のうち有限個の } a_j\text{を除き}0\}$$

のとき、集合 $Span\{e_j\}_{j\in J}$の$\mathcal{H}$における閉包を $\overline{Span}\{e_j\}_{j\in J}$と書く。

・$<\varphi_{j,k}, \psi_{j,l}>=0$ $(j,k,l \in Z, \varphi_{j,k} \in\ V_j,\ \psi_{j,l} \in\ W_j)$ が成り立つことを、$V_j \perp\ W_j$と書く。

・$V_j \oplus\ W_j$を、V_jと W_jの直交和と呼び、互いに直交する成分の和集合で一意的に表現されることを意味する。

注意4.14　レベル jの近似関数 f_jは f_{j-1}から情報が欠落しているので、この不足分 $g_j(t)$ を $f_j(t)$ に補って、

$$f_{j-1}(t)\ = f_j(t)\ + g_j(t)$$

と書ける。また、このとき、f_jはスケーリング関数 $\varphi(t)$ の、g_j はウェーブレット $\psi(t)$ の、それぞれ一次結合で表される。これを整理したのが、次の定理である［22］。

定理4.15$\{V_j\}_{j\in z}$は $L^2(R)$ の多重解像度解析であるとする。また、

・$V_j \perp W_j$

・$V_j \oplus W_j = V_{j-1}$

によって、$L^2(R)$ の閉部分空間の列$\{W_j\}$を作るとき、$\{\psi(t-\ k)\}$が W_0の正規直交基底ならば、

$$\begin{cases} \varphi_{j,k}(t) = 2^{-\frac{j}{2}}\varphi(2^{-j}t-k) & : スケーリング関数 \\ \psi_{j,k}(t) = 2^{-\frac{j}{2}}\psi(2^{-j}t-k) & : ウェーブレット関数 \end{cases}$$

は、それぞれ V_jおよび W_jの正規直交基底となり、φ と ψ で $L^2(R)$ 空間を張ることができる。すなわち、任意の $f_j \in V_j, g_j \in W_j$は、$\varphi_{j,k}(t)$ をスケーリング関数、$\psi_{j,k}(t)$ をウェーブレット関数として、

$$\begin{cases} f_j(t) = \sum_k s_k^{(j)}\varphi_{j,k}(t) \\ g_j(t) = \sum_k w_k^{(j)}\psi_{j,k}(t) \end{cases}$$

のように、一意的な級数で表される。

4.2 高速ウェーブレット変換アルゴリズム

4.2.1 離散ウェーブレット変換

注意4.16 レベル jのスケーリング係数 $s_k^{(j)}$から、1レベル精度の低いウェーブレット展開係数 $w_k^{(j+k)}$およびスケーリング係数 $s_k^{(j+1)}$を導出する手順を次に述べる〔20〕〔21〕。

アルゴリズム4.17（離散ウェーブレット展開）

(1) 連続信号 $f(t)$ のレベル0の近似関数 f_0は、レベル0のスケーリング関数 $\varphi(t-k)$ によって

$$f(t) \simeq f_0(t) = \sum_{k\in Z} s_k^{(0)}\varphi(t-k) \in V_0$$

と展開される。ここで、

$$s_k^0 = \int_{-\infty}^{\infty} f(t)\overline{\varphi_{0,k}(t)}dt$$

であるが、具体的には、マラーの方法にしたがい、信号をサンプリングして得られる数列 $f(n)$を、最初に与えられる離散データ $s_k^{(0)}$とみなす〔20〕。

(2) 次に、$s_k^{(0)}$をもとに、0以外のレベルのスケーリング係数 $s_k^{(j)}$を求める。ここで、p_nは展開係数である。

$$\begin{aligned} s_k^{(j)} &= \int_{-\infty}^{\infty} f(t)\overline{\varphi_{j,k}(t)}dt \\ &= \int_{-\infty}^{\infty} f(t)\sum_n \overline{p_{n-2k}\varphi_{j-1,n}(t)}dt \\ &= \sum_n \overline{p_{n-2k}}\int_{-\infty}^{\infty} f(t)\overline{\varphi_{j-1,n}(t)}dt \\ &= \sum_n \overline{p_{n-2k}}s_n^{(j-1)} \end{aligned}$$

(3) 一方 $s_k^{(j-1)}$から、ウェーブレット展開係数 $w_k^{(j)}$を求める。ここで、q_nは展開係数である。

$$\begin{aligned} w_k^{(j)} &= \int_{-\infty}^{\infty} f(t)\overline{\psi_{j,k}(t)}dt \\ &= \int_{-\infty}^{\infty} f(t)\sum \overline{q_{n-2k}\varphi_{j-1,n}(t)}dt \\ &= \sum_n \overline{q_{n-2k}}\int_{-\infty}^{\infty} f(t)\overline{\varphi_{j-1,n}(t)}dt \\ &= \sum_n \overline{q_{n-2k}}s_n^{(j-1)} \end{aligned}$$

注意4.18 あるレベルのスケーリング係数が、次に精度の低いスケーリング係数とウェーブレット展開係数に分割される様子を模式的に表すと、次のようになる。

$$\begin{array}{ccccccccc} s_k^{(0)} & \longrightarrow & s_k^{(1)} & \longrightarrow & s_k^{(2)} & \cdots & s_k^{(l-1)} & \longrightarrow & s_k^{(l)} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ w_k^{(1)} & & w_k^{(2)} & & w_k^{(3)} & & w_k^{(l)} & & \end{array}$$

アルゴリズム4.19(ウェーブレット再構成) レベルjのウェーブレット展開係数およびスケーリング係数から、逆に、元の与えられた離散データ $s_k^{(0)}$を再構成できる。再構成公式は、

$$s_n^{(j-1)} = \sum_k (p_{n-2k}s_k^{(j)} + q_{n-2k}w_k^{(j)})$$

で与えられる〔20〕。これを模式的に表すと次のようになる。

$$\begin{array}{ccccccccc} s_k^{(l)} & \longrightarrow & s_k^{(l-1)} & \longrightarrow & s_k^{(l-2)} & \cdots & s_k^{(1)} & \longrightarrow & s_k^{(0)} \\ & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\ & & w_k^{(l)} & & w_k^{(l-1)} & & w_k^{(2)} & & w_k^{(1)} \end{array}$$

アルゴリズム4.20（２次元離散ウェーブレット変換） 画像データは、２次元の離散データ $f(m,n)$ で表す。

(1) 画像データ $f(m,n)$ をレベル０のスケーリング係数 $s_{m,n}^{(0)}$ とみなす。

(2) まず横方向に、次いで縦方向に離散ウェーブレット変換を施す。これをまとめると次式で表される。

$$\begin{cases} s_{m,n}^{(j+1)} = \sum_l \sum_k \overline{p_{k-2m} p_{l-2n}} s_{k,l}^{(j)} \\ w_{m,n}^{(j+1,h)} = \sum_l \sum_k \overline{p_{k-2m} q_{l-2n}} s_{k,l}^{(j)} \\ w_{m,n}^{(j+1,v)} = \sum_l \sum_k \overline{q_{k-2m} p_{l-2n}} s_{k,l}^{(j)} \\ w_{m,n}^{(j+1,d)} = \sum_l \sum_k \overline{q_{k-2m} q_{l-2n}} s_{k,l}^{(j)} \end{cases}$$

ここで、$w_{m,n}^{(j+1,h)}$ は横軸方向にスケーリング関数を作用させ、縦軸方向にウェーブレット関数を作用させた係数、$w_{m,n}^{(j+1,v)}$ は横軸方向にウェーブレット関数を作用させ、縦軸方向にスケーリング関数を作用させた係数、また、$w_{m,n}^{(j+1,v)}$ は縦横ともにウェーブレット関数を作用させた係数を表す。

(3) さらに、このうち $s_{m,n}^{(j+1)}$ を次のレベルの４つの係数に分解する計算を繰り返す。

注意4.21 ２次元画像データのウェーブレット変換を模式的に表したものを図８に示す。

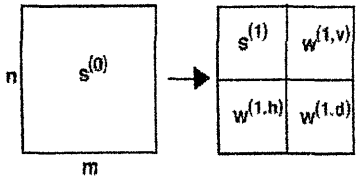

図８：$s^{(0)}_{m,n}$の分解

一般に、図８に示したウェーブレットの階層表現を図９のように表す。このとき、LL,LH,HH,HLを、LLと（LH,HH,HL）の２部に分け、LLを多重解像度分解の近似部、（LH,HH,HL）を多重解像度分解の表現部と呼ぶことにする〔７〕〔８〕。このうち、近似部の分解をさらに続けて、LL部が１×１要素になるまで繰り返すことができる。

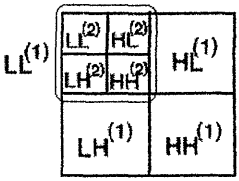

図９：ウェーブレット係数の階層表現

定義4.22（２次元離散ウェーブレット逆変換）多重解像度解析の逆変換は、次式で行われる。

$$s^{(j)}_{m,n} = \sum_k \sum_l \{ p_{m-2k} p_{n-2l} s^{(j+1)}_{k,l} + p_{m-2k} q_{n-2l} w^{(j+1,h)}_{k,l} + q_{m-2k} p_{n-2l} w^{(j+1,v)}_{k,l} + q_{m-2k} q_{n-2l} w^{(j+1,d)}_{k,l} \}$$

4.3 電子透かしの埋め込みアルゴリズム

多重解像度表現部の非零要素から、原画像の高周波成分を推定できる。つまり、表現部は原画像のエッジ部分やノイズ成分を表していると考えら

れるので、実はこれまでの変換手順から、近似部は原画像の解像度を1/2にした画像を表し、一方表現部は、原画像の横、斜め、縦方向の差分情報を表すようにできる。そこで、前節で述べたダイレーションおよび展開係数の部分を含めて、ウェーブレット変換式を次式で表すこととする。

$$\begin{pmatrix} s_{m,n}^{(j+1)} \\ w_{m,n}^{(j+1,h)} \\ w_{m,n}^{(j+1,v)} \\ w_{m,n}^{(j+1,d)} \end{pmatrix} = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \begin{pmatrix} s_{2m,2n}^{(j)} \\ w_{2m+1,2n}^{(j)} \\ w_{2m,2n+1}^{(j)} \\ w_{2m+1,2n+1}^{(j)} \end{pmatrix}$$

$$(m,n = 0, 1, 2, \cdots)$$

これは、ウェーブレット基底として、ハール基底を採用する場合、次と同等である。

$$\varphi(i) = \begin{cases} 0.5 & (i=0,1) \\ 0.0 & (i \neq 0,1) \end{cases} \tag{8}$$

$$\psi(i) = \begin{cases} 0.5 & (i=0) \\ -0.5 & (i=1) \\ 0.5 & (i \neq 0,1) \end{cases} \tag{9}$$

さて、表現部の輝度パターンは表1に掲げる8通りに分けられる。ただし、表中の1は非零であることを示す。このうち、非零の輝度を持つパターンを選んでビット単位で情報を埋め込んでいく〔7〕。

表１：表現部の輝光度パターン

クラス	LH	HH	HL
0	0	0	0
1	0	0	1
2	0	1	0
3	0	1	1
4	1	0	0
5	1	0	1
6	1	1	0
7	1	1	1

アルゴリズム4.23（透かしデータの埋め込み処理）

(1) 使用する輝度クラスを１つ選ぶ。

(2) 表現部ベクトル（LH, HH, HL）の非零成分の指定ビットに透かし情報を１ビット埋め込む。

(3) その要素の値が0かチェックする。もし0となるときは、k+１ビット目に１を挿入する。（クラス変移の回避）

(4) ウェーブレット変換出力に戻す。

この方法は、ウェーブレット多重解像度解析表現の局所的特性を利用したものである。本システム（DWS-UUEA）では、画像への透かしデータの埋め込みモジュールに、基本機能として、この方法を適用している。なお、要素当たりの埋め込みビット数 k は、画質劣化を抑えるために $k \leq 2$ とすることとした〔7〕。

アルゴリズム4.24（データの抽出処理） ハールウェーブレット基底は、完全正規系であるから、埋め込んだ画像にウェーブレット変換を施すことにより、同様に表現部ベクトル（LL, HH, HL）が得られる。埋め込み時に使用した輝度クラス番号を鍵として、表現ベクトルの指定ビットから透かしデータを１ビット取り出す。

５．システムへの攻撃と安全性の確保

5.1 差分法としきい値法

画像の周波数領域に透かしデータを隠蔽する方式は安全性が高い。しかし、安全性と画質とのトレードオフが問題となる。そのためには、データを特定の周波数帯域に正確に埋め込むことが必要となる。そこで、前章で述べた埋め込み手法を「ビット置き換え法」と呼び、それに加えて、次に述べる２つの手法を本システムに組み込むこととした。

5.1.1 差分法

透かしビットを、多重解像度表現部ベクトルの要素間の最大値と最小値の差の絶対値の法２の結果として埋め込むことを考える〔7〕。

アルゴリズム5.1（差分法）

(1) 表現部の要素から最大値と最小値を、それぞれ

$$w_m(k,l)=\max_{i\neq 0}\{w_i(k,l)\},\ w_n(k,l)=\min_{j\neq 0}\{w_j(k,l)\}$$

とおく。

(2) さらに、その差分を$\delta(k,l)$とおく。すなわち、

$$\delta(k,l)=|\max_{i\neq 0}\{w_i(k,l)\}-\min_{j\neq 0}\{w_j(k,l)\}|\bmod 2$$

(3) $s(k,l)=0$かつ$\delta(k,l)=1$のとき

$$\textit{if } w_m(k,l)>0 \textit{ then } w_m(k,l)\leftarrow w_m(k,l)+1$$
$$\textit{else } w_n(k,l)\leftarrow w_n(k,l)-1$$

(4) $s(k,l)=1$かつ$\delta(k,l)=0$のとき

$$\textit{if } w_m(k,l)>0 \textit{ then } w_m(k,l)\leftarrow w_m(k,l)+1$$
$$\textit{else } w_n(k,l)\leftarrow w_n(k,l)-1$$

これによって、表現部ベクトルに含まれる3つの要素の差分情報をうまく利用して、透かしデータを埋め込むことができる。透かしデータが2値であるときに有効である。

5.1.2 しきい値法

データを特定の周波数帯域により正確に埋め込むために、サブバンドフィルタバンクを利用した電子透かし法を考える〔8〕〔33〕。本システムでは、フィルタバンクのシミュレータを作成し、データをウェーブレット変換フィルタに複数回通すことによって耐性を高めるとともに、最終的な埋め込み周波数の選択において、しきい値を設定する方法を採用することとした。以下に、その手順を示す。

(1) サブバンドフィルタバンク

原画像 V_0の２次元ウェーブレット変換にサブバンドフィルタバンクを用いる。サブバンドフィルタバンクによる画像変換の原理を図10に示す。

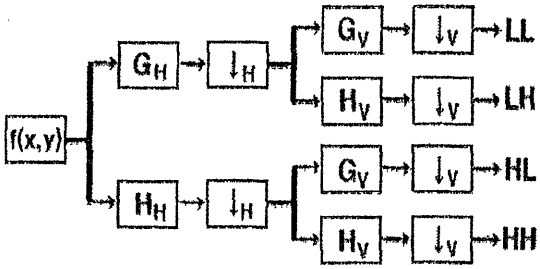

図10：サブバンドを用いた画像の変換

Z_2上の２変数関数 $f(x,y)$ を入力値として、図10の各記号は次の意味を持つ。ただし、$V=\{(x,y) \mid x,y \in Z, x \in [0,m\rceil\ , y \in [0,m\rceil\}$とする。

G_H, G_V, H_H, H_Vは、それぞれ、すべての $(x_0,y_0) \in V$について次式の値を求めることを意味する。

$$\begin{cases} G_H & : \sum_{x=-\infty}^{\infty} \varphi(x) f(x_0+x, y_0) \\ G_V & : \sum_{y=-\infty}^{\infty} \varphi(x) f(x_0, y_0+y) \\ H_H & : \sum_{x=-\infty}^{\infty} \psi(x) f(x_0+x, y_0) \\ H_V & : \sum_{y=-\infty}^{\infty} \psi(x) f(x_0, y_0+y) \end{cases}$$

また、 $\boxed{\downarrow_H}$、$\boxed{\downarrow_V}$、$\boxed{\uparrow_H}$、$\boxed{\uparrow_V}$ はそれぞれ次式の値を求めることを意味する。

$$\begin{cases} \boxed{\downarrow_H} : f(x_0,y)=f(2x_0,y);\ x_0\in[0,m/2] \\ \boxed{\downarrow_V} : f(x,y_0)=f(x,2y_0);\ y_0\in[0,m/2] \\ \boxed{\uparrow_H} : f(x_0,y)=\begin{cases} f(\frac{x_0}{2},y) & (x_0\text{が奇数}) \\ 0 & (x_0\text{が偶数}) \end{cases};\ x_0\in[0,2m] \\ \boxed{\uparrow_V} : f(x,y_0)=\begin{cases} f(x,\frac{y_0}{2}) & (y_0\text{が奇数}) \\ 0 & (y_0\text{が偶数}) \end{cases};\ y_0\in[0,2m] \end{cases}$$

原画像 V_0を図10のサブバンドフィルタバンクに通すことによって、4つの成分 $LL^{(1)},LH^{(1)},HL^{(1)},HH^{(1)}$に分解される。さらに、$LL^{(1)}$について同様の処理を施して、$LL^{(2)},LH^{(2)},HL^{(2)},HH^{(2)}$を得ることができる。すなわち、2次元実数値関数 $f(x,y)$ としての原画像 V_0に j 回この処理を施すことで、

$LH^{(1)},HL^{(1)},HH^{(1)},LH^{(2)},HL^{(2)},HH^{(2)},\cdots$

$$\cdots LH^{(j-1)},HL^{(j-1)},HH^{(j-1)},LL^{(j)},LH^{(j)},HL^{(j)},HH^{(j)}$$

を要素とする2次元画像が得られる。

(2) 処理の流れ

アルゴリズム5.2（埋め込み処理）

(1) 埋め込みビット列を求める。$(s_0,s_1,s_2,\cdots,s_i,\cdots)$

(2) しきい値を d とする。

(3) 原画像をサブバンドフィルタバンクに通し、ベクトル

$$V_j=(LL^{(j)},LH^{(j)},HH^{(j)},HL^{(j)})$$

を得る。jは、サブバンドフィルタバンクを通した回数を表す。

(4) 表現部ベクトル $(LH^{(j)}(x,y)\ ,HH^{(j)}(x,y)\ ,HL^{(j)}(x,y))$ $(0\leq x,y\leq m)$ のうち、少なくとも1つの要素が非零であって、そのいずれも d 以上であるとき、対応する近似部 $LL^{(j)}(x,y)$ を透かしビットの処理対象と

して選択する。

(5) 次の手順で、$LL^{(j)}(x,y)$ に透かしデータの埋め込みを行う。

・$LL^{(j)}(x_0,y_0)$ の値の整数部を取り出し、３進表現に直し、

$$LL^{(j)}(x_0,y_0) = (\cdots, d_3, d_2, d_1)_{(3)}$$

とする（$d_j = 0,1,2$）。

・第１位 d_1に透かしビット s_iを埋め込む（$d_1 \leftarrow d_1 + s_i \bmod 2$）

(6) 埋め込み後の新しい $LL^{(j)}$を含むベクトル$(LL^{(j)}, LH^{(j)}, HH^{(j)}, HL^{(j)})$に、２次元ウェーブレット逆変換を施し、埋め込み画像データ V'とする。

一方、データの抽出処理も、同様に、LH, HH, HL がしきい値より大きくなる (x,y) を見つければよい。

5.2 アクセス制御と緊急アクセス

本システムでは、画像データをデータベースに保存して一括管理するが、データを外部からのさまざまな攻撃から護るために、アクセス制御方式を採用することとした。

そもそも画像データを不正に閲覧したり、改竄を防止するためには、ユーザ認証などによるアクセス制御が必要となる。これまで一般には、電子透かしシステムとアクセス制御は切り離して議論されることが多かったが、今回、この２つを組み合わせることによって、より安全な透かしデータおよび復号鍵の管理が行えるものと考える。特に、原画像の所有者が不在であっても、画像データに緊急にアクセスする必要が生じた場合を想定して、次に示す緊急アクセス方式を利用することとした。

5.2.1 埋め込み画像への緊急アクセス

ここでは、埋め込み画像への緊急アクセス方式として、**(k,n)しきい値符号方式**を応用することとした〔40〕。本来の (k,n)しきい値符号方式は、暗号化ファイルの緊急アクセスを実現する方式であるが、画像データも１つ

のファイルと考え、適用を試みることとした。

(k,n)しきい値方式は、基本的には、離散対数問題に基づく公開鍵暗号方式を用いて、鍵の所有者をグループ化し、メンバーが協力しなければ復号できない仕組みを実現している。以下に、(k,n)しきい値符号方式の、透かし画像への適用手順を整理しておく。

(1) システムパラメータの初期化

・素数 p,q（ただし、$p=2q+1$）と、巡回群 Z_p^*上の原始根 g を生成する。
ここで、p,q,gをシステムパラメータと呼ぶ。

・Z_{p-1}の中から、任意の偶数 x を選び、緊急アクセス用秘密鍵とする。

・$y=g^x \pmod p$ により公開鍵 y を求める。

(2) 秘密鍵の分割

$m={}_nC_k$個の $n+1$ 変数1次式を生成する〔40〕。

$$\begin{cases} a_{00}x_0+a_{01}x_1+\cdots+a_{0j}x_j+\cdots+a_{0n-1}x_{n-1} &= x/2 \pmod q \\ a_{10}x_0+a_{11}x_1+\cdots+a_{1j}x_j+\cdots+a_{1n-1}x_{n-1} &= x/2 \pmod q \\ \cdots\cdots \\ a_{i0}x_0+a_{i1}x_1+\cdots+a_{ij}x_j+\cdots+a_{in-1}x_{n-1} &= x/2 \pmod q \\ \cdots\cdots \\ a_{m0}x_0+a_{m1}x_1+\cdots+a_{mj}x_j+\cdots+a_{mn-1}x_{n-1} &= x/2 \pmod q \end{cases}$$

ここで、各 iに対して、$a_{i0},a_{i1},\cdots,a_{in-1}$のうち $n-1$ 個は0、残る k 個は非零とする。ただし、各 iに対して、a_{ij}が非零である x_jの組合せは、互いに異なるものとする。このとき、$x_0,x_1,\cdots,x_{k-2}$をランダムに選べば、残りの $x_{k-1},x_k,\cdots,x_{n-1}$が決まるので、これらの x_jを分割鍵保有者に配布する。なお、配布する分割鍵は、暗号化して分割鍵保有者のパスワードでしかアクセスできないようにしておかなければならない。

(3) 1次のパラメータ a_{ij}への署名

パラメータ a_{ij}は緊急アクセスで再度必要になるため、改竄の予防措置として署名を施しておく。

(4) システムパラメータ p,q,g の配布および緊急アクセス用公開鍵 y の配布を行う。

5.2.2 緊急アクセス手順

(1) ユーザ側の処理手順

・Z_{p-1}から乱数 r を選ぶ。

・画像ファイル鍵 m をランダムに生成する。

・$c_1 = g^r \pmod{p}$ を生成し、緊急アクセス用データとして保存する。

・$c_2 = my^r \pmod{p}$ を生成し、緊急アクセス用データとして保存する。

(2) 管理者側の処理手順

・c_1, c_2の提出を受ける。

・$d_j = c^{2aij \bmod q}$を各 x_jに対して求める。

・画像ファイル鍵

$$m = c_2 / \prod d_j = c_2 / c^{2\sum a_{ij} x_j \bmod q} = c_2 / c_1^{x}$$

を求める。

・m によって緊急アクセスを行う。

5.3 追跡不能な署名法

原画像への著作権データの埋め込みを行った後、照合のためそのユーザ情報はサーバに付属のデータベースで一括管理される。しかし、このユーザ情報に対する不正アクセスが心配される。また、このユーザ情報が、他の著作物への埋め込みデータとして活用された場合に、データベース管理者によって追跡され、ユーザのプライバシーが侵害される恐れもある。一方、透かしデータに信頼性を持たせるために、第３者機関、あるいは簡易的に埋め込みサーバの管理者側等が署名を行うことが必要となる。このとき、次の処理が可能である。すなわち、原画像の提供者にとっては、署名者に提供者の個人情報を秘密にしたままで、署名を付けてもらう追跡不能

な署名法、いわゆるブラインド署名が可能である〔41〕〔42〕。

本システムでは、原画像と透かしデータのデータベース管理部において、*Chaum*の提案した、ＲＳＡ法に基づくブラインド署名法を組み込み、著作者の個人データの追跡不能性を付加することとした。

以下は、透かしデータの現所有者が、管理者に署名を施してもらい、データの譲渡先がその署名の正当性を検査・確認するための一連の流れを示している。このとき、署名者は現所有者の個人情報（この場合、透かしデータの中身）を知ることはできない。

アルゴリズム5.3（ブラインド署名）

(1) 透かしデータの持ち主（署名の要求者）は、ブラインド署名前処理によって画像 Mを乱数 Uで撹乱してブラインドメッセージ Xを生成する。具体的には、$UU'=1 \bmod n$となる乱数 U, U'を選び、署名者の公開鍵 d, nを使って、

$$X = MU^d \bmod n$$

を求める。

(2) 管理者（署名者）は、秘密鍵を用いて Xに対応する仮りの署名 Yを計算する。このとき、Mは Uによって撹乱されているので、署名者は文書 Mを知ることはできない。すなわち、署名者は、自分の秘密鍵 eを用いて、

$$Y = x^e \bmod n$$

を求める。

(3) 署名要求者は、ブラインド署名後処理によって Yから乱数 Uの影響を除去して、本来の文書 Mに対する真の署名 Y'を求める。すなわち、

$$YU' \bmod n = M^e U \times U' \bmod n = M^e \bmod n$$

の結果を Y'とおく。

(4) 署名の要求者は、Mと Y'の組を透かしデータの譲渡者（検査者）に送信する。

(5) 検査者は、署名者の公開鍵を用いて、Y'がMの署名であることを確認する。すなわち、$Y'^{d} \bmod n$がMと一致すればよい。なおここで、検査者は、YとY'の関係を知ることはできない。

6．DWS－UUEAシステムの概要

パーソナルコンピュータ上に構築した、電子透かしシステム（仮称DWS－UUEA：The Digital Watermarking System with Untraceability, Unreusability, and Emergency Accessibility）の概要を以下に述べる。基本OSはMicrosoft社のWindows95/98、開発環境はInprise社のDelphiである。

6.1 システムの特徴

本システムの主な特徴を以下に列挙しておく。

(1) 本システムの実体は、Object Pascal言語で記述されたサブルーチン・サブプログラム・ライブラリ、およびユーザインタフェースとしての各種フォームモジュール群である。ユーザは、利用したい埋め込み手法や埋め込みデータの種類等に応じて、準備されたモジュールのなかから、必要なものを選択し、自ら組み立てて、実行する。

(2) 本システムは、GUIの利点を活かしたマンマシンインタフェースも有している。システムが組み上がった時点からは、たとえば、入出力画像の画面表示と印刷、処理手続きのガイダンスのためのグラフィックス表示などが実現されている。

(3) 本システムの中核は、電子透かし処理システムモジュールである。また、この他に、各種ユーティリティが付属している。たとえば、統計分析モジュール、モニタリングおよびデバッギングモジュールなど。

(4) 本システムでは、さまざまな種類の乱数と確率分布関数、およびいくつかのウェーブレットとスケーリング関数を生成することができる。また、必要に応じて、本体に付属の統計分析システムSTATPCを起動して、入力データの生成や出力データの解析が可能である。

(5) 本システムは、多くの入出力用データファイルを利用する。

6.2 システム構成

図11は、ＤＷＳ－ＵＵＥＡのシステム構成図である。現在までのところ、主要モジュールとして、ユーザインタフェース部（ＵＩＮＦ）、電子透かし部（DWMK）、電子認証部（ＥＡＵＨ）、データベース管理部（ＤＢＭＳ）、統計パッケージ（ＳＴＡＴＰＣ）の5つを含んでいる。以下に、各部の概要を述べる。

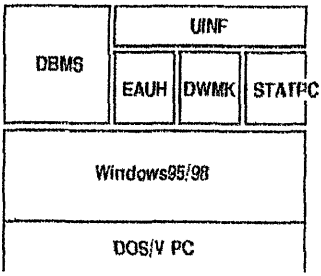

図11：ＤＷＳ－ＵＵＥＡシステムのシステム構成

6.2.1 電子透かし部（DWMK部）

電子透かし部は、本システムの中核をなすモジュール群である。これまでに組み込みに成功した透かしデータの埋め込み手法は、

・ビット置き換え法
・差分法
・しきい値法

の３通りである。これらの各手法に対して、透かしデータの埋め込みと再構成の両方を担当する。ここに属するプログラム・ライブラリの主なものとして次がある。

・画像処理ライブラリ……基本プログラム、アプリケーションプログラム、

ユーティリティプログラムから成り立っている。ユーザは、これらを利用して、画像ファイルへのアクセスが行える。

・電子透かし埋め込みライブラリ……本システムの中核となる部分である。各種埋め込み手法がコード化されている部分である。データの抽出もここで行う。ここには、埋め込みモジュール、復号モジュールなどが含まれる。

6.2.2 ユーザインタフェース部（ＵＩＮＦ部）

ＯＳとＤＷＳシステムのインタフェースの役割を果たすと同時に、ユーザとＤＷＳシステムとの間のＧＵＩの役割も同時に果たす。ＤＢＭＳとＤＷＳ、あるいはＤＢＭＳとユーザのインタフェースは、InterBase のインタフェースが受け持つ。

6.2.3 電子認証システム部（ＥＡＵＨ部）

電子透かしシステムを補完するための著作権管理システムモジュールである。原画像やユーザ情報記録用データベースへの不正アクセスに対応することを目的とする。具体的には、電子透かし部自体の不正の回避と、ユーザの匿名性を実現するための各種モジュールから構成されている。主な、モジュールを列挙すると、次の2つである。

・ブラインド署名処理ライブラリ……透かしデータに書き込まれたユーザ情報が、追跡不可能性を有するための一連の処理を担当する。

・緊急アクセス処理ライブラリ……データベース管理者が緊急にデータへのアクセスが必要になった場合の処理を担当する。

6.2.4 データベース管理部（ＤＢＭＳ部）

画像情報やユーザ情報を管理するためのデータベース管理システムである。リレーショナルデータベース管理システムの InterBase を利用して構築されている。DBMS 部が管轄するデータファイルの全体像を図12に示す。

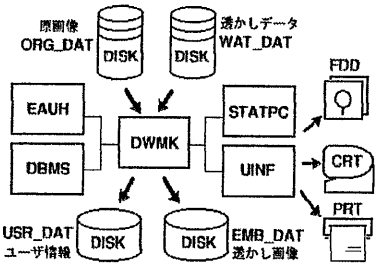

図12：DWSシステムと各種ファイル群

6.2.5 その他

統計的な性質を有する特別な画像データを生成したり、入出力画像の品質のチェックなどを行うためのモジュールとして、統計パッケージ（ＳＴＡＴＰＣ）が準備されている。利用に当たっては、ＤＷＭＫ本体の外部関数として組み込む。

6.3 実行事例

以下では、静止画への電子透かしの埋め込みの流れを概観する。ただし、説明のために、組み込みモジュール構成は最小の場合（ＤＷＭＫ部の埋め込みモジュールとＵＩＮＦ部の組み合わせ）を例にとる。

6.3.1 原画像

原画像として受け付けるのは、現在のところ256×256ピクセルのビットマップファイル（bmp）である。たとえば、図３の画像は横長タイプであるため、事前に正方形に整形しておかなければならない。

6.3.2 透かし情報

原画像と同様である。なお、現在のＤＷＳシステムでは、透かしデータ

はすべて目に見えない（不可視）状態で埋め込まれる。

6.3.3 実行動作

・必要最小限のモジュールを指定して、システムをビルドする。ここでは、埋め込みモジュールを組み込む。
・作成された実行可能プログラムを起動すると、図13のような画面が表示される。
・適切な透かしデータの埋め込み手法を選択する。
・原画像と透かしデータの各ファイル名を指定し、〔OK〕をクリックする。
・図14のような画像ウィンドウが開き、原画像と透かしデータが、左側に上下並んで表示される。
・透かしの埋め込み手法によっては、〔鍵の入力〕ダイアログボックスが開くので適当な値を入力する。なお、鍵を設定するために入力する値は、鍵そのものではなく（実質的な鍵の選択はシステムが行う）、ユーザは乱数発生のための初期値を与える。
・透かし画像の出力ファイル名を指定し、〔実行〕ボタンをクリックすると、原画像の右隣りに、出力画像が得られる。

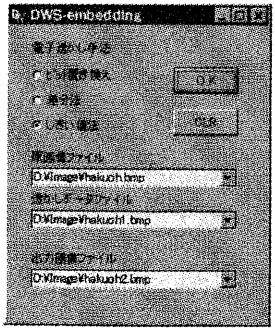

図13：パラメータの指定画面

図14：実行結果の画面表示例

6.4 システムの性能評価

画像処理関係の実験では、ＳＩＤＢＡなどから入手した画像を用いるのが一般的であるが、今回は、身近な３つの風景画像を基に評価を行った。原画像は、256×256ピクセル、透かし画像は、文字のレタリング画像で、２値画像、128×128ピクセルである。

また、画質を客観的に評価するために、次式で定義されるＳ／Ｎ比（ＳＮＲ）を利用することとした〔7〕〔29〕。

$$SNR = 20 \times \log_{10}\left(255/\sqrt{\{\sum_{i=1}^{n^2}(org_i - emb_i)^2\}/n^2}\right)$$

ここで、255は画像のピークピーク値（輝度の最大、最小の差）、平方根内は原画像と合成画像との差の2乗の平均値（平均2乗誤差）である。なお、org_iは原画像の画素 i の輝度値、emb_iは透かし済み画像の画素 i の輝度値、n は画像のサイズである。

これによる今回の3種のプログラムによる画像のＳ／Ｎ比を表２に示す。

表2：透かし画像の画質

画像＼手法	ビット	差分	しきい値
A	37.51	36.18	42.25
B	38.82	40.27	43.62
C	42.36	44.32	43.55

・ビット置き換え法

ベクトルの要素当たりの埋め込みビット数 k を2以下と決めて、画質劣化を抑えることに成功した。周波数領域における透かし情報のビット置き換えであるから、復号手順も簡単で、システムの構築もしやすい手法である。

・差分法

多重解像度解析の3つの要素の大小関係を利用している。画像の位相成分に透かしビットを埋め込みことと解釈できる。

・しきい値法

高周波成分にビットを埋め込んではいるが、ウェーブレット変換に複数回通しているので、画像の劣化は比較的高い。また、高周波をカットするなどの攻撃に弱いと考えられるので、今後は、エッジ部分への埋め込みなどのアルゴリズムを付加するなどの工夫が必要である。

一方、認証システム部については、安全性は、秘密鍵の管理のレベルによっては、あらゆるコンテンツの利用が可能になってしまう。

運用性については、鍵をデータベースで管理するため、定期的なバックアップが必要となり、その分手間がかかる。

速度性能については、計算量が多く、しかもファイル入出力の部分でのオーバーヘッドがかかることがわかった。また、ネットワークを介しての端末からサーバへの問い合わせでは、データアクセスと認証が繰り返され、ターンアラウンドタイムがかかり、受け渡し処理の改善が必要である。

7．おわりに

以上、電子透かしおよび認証のための統合システム（仮称ＤＷＳ－ＵＵＥＡ）の概要を述べた。最後に、本システムをプロトタイプとして、今後の改善点等について述べる。

まず、電子透かし部については、多くの画像フォーマットに対応すること、任意の大きさの画像に対応すること、可視モードと不可視モードの両モードを揃えること、外部からの攻撃に耐性のある埋め込み手法を組み込むこと、StirMark のベンチマークテストにかけること、等が今後の課題である。特に、第4点目については、高速フーリエ変換、あるいは画像認識に使われるフーリエ・メリン変換の利用も検討したいと考えている。

また、これまでの電子透かしシステムでは、埋め込みアルゴリズムを秘密にするのが当然とされてきたが、現実の暗号システムでは、アルゴリズムを公開した上で、暗号鍵によって秘密情報の安全性を確保しようとしている。したがって、電子透かしシステムにおいても、アルゴリズムを公開するという方向でシステムの安全を守ろうとする流れが強まるものと考えられる。したがって、埋め込みアルゴリズムを公開した場合の安全性の確保も今後の課題となろう。

次に、電子認証システム部については、追跡不能な署名法のアルゴリズムの安全性をより高めるために、多重ブラインド署名法が有効である。しかし、さらに安全なものとして、ゼロ知識証明に基づいたブラインド署名方式も今後主流になると予想されており〔41〕、新たなアルゴリズムの組み変えが必要になると考えられる。

データベース管理部については、電子認証システム部と同様に、扱うデータ量が多い。したがって、ファイルアクセスのためのオーバーヘッドの部分の負荷をいかに減らすかが、今後の重要な課題として残されている。また、データベースとネットワークとの連携を深めるために、ＳＱＬＩＮＫの利用、抽象データセットの拡張、ＣＯＲＢＡアプリケーションの組込みなども必要と考えている。

参考文献

〔1〕郵政省："平成11年度通信白書"，郵政省（1999）．

〔2〕日本インターネット協会編："インターネット白書'99"，インプレス（1999）．

〔3〕著作権審議会マルチメディア小委員会："著作権審議会マルチメディア小委員会ワーキンググループ（技術的・管理関係）報告書（平成10年12月10日）"，文化庁（1998）．

〔4〕著作権審議会マルチメディア小委員会："著作権審議会マルチメディア小委員会ワーキンググループ（技術的・管理関係）中間まとめ（コピープロテクション等技術的保護手段の回避について）（平成10年2月20日）"，文化庁（1998）．

〔5〕名和小太郎："ネットワークをめぐる法的課題"，情報処理，Vol.37，No.2，pp.135－142（1996）．

〔6〕姫野桂一："インターネットの抱える諸問題と今後の展望－特に知的財産権保護に関してー"，郵政研究所月報，No.112，pp.43-65（1998）．

〔7〕松井甲子雄："電子透かしの基礎－マルチメディアのニュープロテクト技術－"，森北出版（1998）．

〔8〕井上彰："電子透かしーマルチメディア時代の暗号システムー"，丸山学芸図書（1998）．

〔9〕高橋史忠："電子透かしがマルチメディア時代を守る"，日経エレクトロニクス，No.683，pp.99-124（1997）．

〔10〕松井甲子雄："電子透かし技術の最新動向"，情報処理，Vol.40，No.2，pp.178-183（1998）．

〔11〕渡辺創："電子透かしについて"，Computer Today，No.91，サイエンス社（1999）．

〔12〕チャックリット・リムバーンイエン，外山高裕，山口和彦："JAVAを用いた電子透かしの評価ツール"，情報処理学会研究報告，99-CSEC-

4, pp.13-18 (1999).

〔13〕井上彰, 斎藤直哉 : “デジタルコンテンツのノン・パッケージ流通と著作権の保護”, 情報処理学会研究報告, Vol.98, No.85, pp.89-95 (1998).

〔14〕中山信弘 : “マルチメディアと著作権”, 岩波書店 (1996).

〔15〕苗村憲司, 小宮山弘之 : “マルチメディア社会の著作権”, Keio-up 選書 (1997).

〔16〕三山雄三 : “著作権法詳説 (第2版) 判例で読む14章”, 東京布井出版 (1997).

〔17〕則近憲佑, 服部裕子 : “マルチメディアと知的財産権”, 情報処理, Vol.37, No.2, pp.117-121 (1996).

〔18〕三次衛, 小田久司 : “ソフトウェアをめぐる法律問題”, 情報処理, Vol.37, No.2, pp.122-127 (1996).

〔19〕小野定康, 鈴木純司 : “JPEG／MPEG2の実現法”, オーム社 (1995).

〔20〕中野宏毅, 山本鎮男, 吉田靖夫 : “ウェーブレットによる信号処理と画像処理”, 共立出版 (1999).

〔21〕芦野隆一, 山本鎮男 : “ウェーブレット解析”, 共立出版 (1997).

〔22〕チャールズ K.チュイ, (訳) 桜井明, 新井勉 : “ウェーブレット入門”, 東京電機大学出版局 (1993).

〔23〕清水周一, 沼尾雅之, 森本典繁 : “ピクセルブロックによる静止画像データハイディング”, 情報処理学会第53回全国大会, Vol.2, pp.257-258, IN-11 (1996).

〔24〕岡一博, 松井甲子雄 : “埋込み関数を用いた濃淡画像への署名法”, 電子情報通信学会論文誌, Vol.J80-D-II, No.5, pp.1186-1191 (1997).

〔25〕向川公宏, 田辺英彦, 阪口文則, 梅田博之 : “データハイディングによる濃淡画像へのディジタル署名”, 電子情報通信学会技術研究報告, Vol.97, No.254, IT97-42, pp.7-12 (1997).

〔26〕中村康弘, 松井甲子雄 : “離散的直交変換を用いた濃淡画像とテキス

トデータの合成符号化法”，電子情報通信学会論文誌，Vol.J72-D-II，No.3，pp.363-368（1989）．

〔27〕松井甲子雄，大西淳児，中村康弘：“ウェーブレット変換における画像への署名データの埋込み”，電子情報通信学会論文誌，Vol.J79-D-II，No.6，pp.1017-1024（1996）．

〔28〕大西淳児，松井甲子雄：“ウェーブレットを利用した著作権保護のための画像符号化”，情報処理学会論文誌，Vol.33，No.3，pp.534-539（1997）．

〔29〕酒井康行，石塚裕一，櫻井幸一：“著作権保護のためのウェーブレット変換を用いた電子透かし方式の安全性評価”，情報処理学会論文誌，Vol.38，No.12，pp.2640-2647（1997）．

〔30〕W.Bender，D.Gruhl，森本典繁，A.Lu:“電子透かしを支えるデータ・ハイディング技術（上）”，日経エレクトロニクス，No.683（2月24日号），pp.149-162（1997）．

〔31〕I. Pitas: “A method for signature casting on digital images”，Proceedings of 1996 International Conference on Image Processing, Vol. III，pp.215-218（1996）．

〔32〕山田隆行，松井甲子雄：“パッチワークによる署名画像に対する秘密鍵の探索攻撃”，情報処理学会研究報告，Vol.99，No.54，pp.1-6(1999)．

〔33〕安田咲子，岡本栄司，阿部亨：“QMF を用いた電子透かしの提案”，情報処理学会研究報告，Vol.98，No.54，pp.17-22（1998）．

〔34〕松井甲子雄，中里隆博：“攻撃耐性を強化した離散コサイン変換による電子透かしの一方法”，情報処理学会論文誌，Vol.40，No.12，pp.4258-4265（1999）．

〔35〕江島将高，宮崎明雄：“ウェーブレットを利用した電子透かし方式の検討”，電子情報通信学会技術研究報告，Vol.98，No.512，pp.13-18（1999）．

〔36〕大西淳児，小澤慎治：“多重解像度解析によるクロップ画像から署名

検出可能な電子透かし法”，電子情報通信学会論文誌，Vol.J81-D-II，No.10，pp.2321-2329（1998）．

〔37〕松井甲子雄：“絵に秘める暗号の科学”，コロナ社（1994）．

〔38〕Fabien A.P.Petitcolas，Ross J.Anderson: “Evaluation of Copyright Marking Systems”, Proceedings of IEEE Multimedia Systems'99, Vol.1, pp.574-579（1999）．

〔39〕Fabien A.P.Petitcolas, Ross J.Anderson, Markus G.Kuhn: “Attacks on Copyright Marking Systems”, Lecture Notes in Computer Science Portland, Vol.1525，pp.218-238（1998）．

〔40〕宮崎博，鮫島吉喜，遠田潤一：“セキュアファイルシステムの構築”，情報処理学会研究会報告，Vol.99，No.54，pp.19-24（1999）．

〔41〕情報理論とその応用学会（編）：“暗号と認証”，培風館（1996）．

〔42〕D.Chaum: “Security without Identification:Transaction Systems to Make Big Brother Obsolete”，Communications of the ACM，Vol.28，No.10，pp.1030-1044（1985）．

（本学経営学部助教授）