Kobe University Repository : Kernel

PDF issue: 2025-01-01

電子透かし技術とその応用に関する研究

栗林, 稔

(Degree)
博士（工学）

(Date of Degree)
2004-09-17

(Date of Publication)
2007-08-09

(Resource Type)
doctoral thesis

(Report Number)
乙2773

(URL)
https://hdl.handle.net/20.500.14094/D2002773

※ 当コンテンツは神戸大学の学術成果です。無断複製・不正使用等を禁じます。著作権法で認められている範囲内で、適切にご利用ください。

神 戸 大 学 博 士 論 文

電子透かし技術とその応用に関する研究

平成 16年 8月

栗 林　稔

内容梗概

ディジタル情報の著作権保護方式として，電子透かし技術に注目が集まっている．電子透かしとは，人間の知覚特性を利用してディジタル情報に著作権情報などの副情報を埋め込む技術である．本論文では，ディジタル画像や動画などのコンテンツの著作権保護を目的として，電子透かし技術及びその応用技術に関する研究を行う．電子透かし技術において，埋め込みによる視覚的な劣化を防ぐことと各種攻撃に対する耐性向上の間にはトレードオフの関係がある．本研究では，ディジタルコンテンツが有する特徴を最大限に活用することで視覚劣化を抑え，攻撃に対する耐性向上を同時に満足させる手法を考案する．また，リアルタイム処理が求められるアプリケーションに適用可能な手法及び，ネットワーク上での売買を安全に効率的に行うことのできる手法を提案する．

まず，人間の視覚特性に基づいて，ディジタル画像の低周波成分に透かし情報を埋め込む手法を提案する．画像の低周波成分への埋め込みを行った場合，各種攻撃に対して耐性は高いが，ブロック歪みが生じやすいため，改善が必要である．DCT 係数の低周波成分を解析した結果，特定の 4 個の DCT 係数に与えた透かし信号エネルギーは，ブロック内の中央領域付近に緩やかな曲線を描いた模様として現れ，ブロックの端ではその振幅がほとんど変化しないことを発見した．そこで，この DCT 係数間の加法特性を利用することで，ブロック歪みを抑える手法を提案する．DCT 係数間の加法特性による埋め込みを行えば透かし信号は，ブロックの中心付近のサブブロックからも検出できる．そのため，検出に要する計算量を抑えることが可能である．また，微小な回転，拡大縮小，平行移動などの幾何学的な改変が施された場合でも透かし情報を検出できるように，同期を回復するための処理手法を提案する．計算機シミュレーションにより，幾何学的な改変により生じる同期位置の変化量を調べ，その結果を用いて以降に提案する方式のパラメータを設定する．

次に，画像の有する局所的な情報に基づいて，適応的に透かし情報を埋め込む手法を提案する．画像の変化が激しい領域は人間の視覚特性上，雑音による影響が知覚されにくい．そこで，局所的に選出するブロックにおいて縦横及び斜め方向の輝度値の分散を調べることで，画像の平坦な領域と複雑な模様の領域を分類し，埋め込みに適した領域に透かしを埋め込む．また，透かし信号を複雑な模様に変調させてその領域に適した信号とすることで，局所的に適応的な埋め込みを行う．その際，信号処理により変質しやすい高周波成分を避けて，特定の周波数成分にランダムな振舞いをする信号を埋め込むために，ウェーブレット変換を用いて周波数成分を分割し，PN 系列を用いたスペクトル拡散法を利用する．

データ量が多くリアルタイム性が求められる動画像を扱うためには，透かし情報の検出に要する計算量が問題となる．幾何学的な改変を考慮して同期信号を埋め込む従来手法では，幾何

学的な改変を受けた場合，その歪みを補正した後に透かし情報を埋め込むため，計算量が莫大であった．そこで，従来手法に改良を加えて，同期信号の位置関係を変化させて埋め込みを行う．微小な回転，拡大縮小，平行移動による同期点を検出できれば，提案手法では補正を行わずに検出した同期信号の隣接する信号間の距離を計算することで透かし情報を検出することができる．また，同期信号の誤り検出を補正することで，透かし信号の検出率を向上させる手法を提案する．従来の電子透かし技術では，透かし信号は画像の成分値の大きさを変化させて埋め込みを行っており，信号処理の観点からパルス振幅変調とみなすことができる．しかし，ディジタル信号の伝送には他にも変調方式が存在するにも関わらず，これまでは使用されていなかった．提案手法は，パルス位置変調の概念を電子透かしの分野に適用させた手法であり，新しい埋め込み領域を示すことで，今後の発展が期待できる手法である．

電子透かし技術を応用させた電子指紋技術では，販売者が購入者にディジタルコンテンツを販売する際に，購入者を示す情報を埋め込んでいる．この技術を用いれば，不正コピーが配布された場合，埋め込まれた情報からその購入者を特定することができる．売買の取引終了後，購入者だけが電子指紋の埋め込まれたコンテンツを得られるならば，不正コピーを配布できるのは購入者に限られるため，販売者は不正を検挙できれば購入者を訴えることができる．従来法では，このような電子指紋のプロトコルを理論上構成できるが，効率が極めて悪い．提案手法では岡本–内山暗号の加法性準同型写像の性質を利用して電子指紋プロトコルを構成する．この手法を用いれば，暗号化された透かし情報を暗号化されたコンテンツに埋め込むことが可能となり，プロトコルの正当性も検証できる．また，多くの電子透かし技術で採用されている量子化法による埋め込みが可能であることを実例を挙げて示す．従来法では，ネットワーク上での取引を行うためには通信量の削減が必要不可欠であった．例えば，従来法では安全面より 1MB のコンテンツに購入者の電子指紋を埋め込んで送る場合，1GB 以上のデータを送信する必要があるため実用的ではなかった．提案方式では，用いる岡本–内山暗号の暗号化率である 1/3 まで理論上プロトコルを効率化できるため，1MB のデータを送信するには 3MB 程度のデータを送れば安全に売買の取引が行える．

以上のように本論文では，画質劣化を抑え，同時に攻撃に対する耐性を向上できるように人間の視覚特性及び画像が有する特徴を応用させる技術に関して検討を行う．次に，比較的少ない計算量で処理できるだけでなく，新しい埋め込み可能な領域の存在を示す．最後に，電子透かしを応用させた技術である電子指紋技術を効率的に行う手法を実現することで，ネットワーク上での売買において障壁となっていた通信量の問題を解決する．また，画質劣化を抑え，攻撃に対する耐性の高い手法を電子指紋技術に実装するために必要な修正法を示す．

目　次

図 目 次

表 目 次

第1章　緒論

コンピュータの進化と共に，ディジタル信号処理の技術革新が進むにつれて，従来では扱うことが難しかった画像や音声データを処理することが比較的容易となった．また，ディジタルカメラにより撮影されたディジタル画像や動画などがコンピュータ上で処理され，保存されるようになった．これらのディジタル情報は，インターネットに代表されるディジタルネットワーク技術の発達により，遠く離れた相手に送信することが容易に行える．ネットワークを利用すれば，ディジタル情報を複数のユーザ間で共有することも可能となる．現在，ネットワークを介して映画や音楽，絵画などのディジタルコンテンツの売買などが行われ始めており，今後更なる発展が期待される．しかし，ディジタル情報はその痕跡を全く残すことなく複製物を作成できることから，著作権侵害問題が深刻となっている．

ディジタルコンテンツを保護するアプローチとして，従来から使われている手法は暗号技術を用いることである．ファイルを送信する前に暗号化すれば，秘密鍵がなければ解読することができないため，不正者がネットワークで送受信される信号から情報を取り出すことができない．しかし，暗号技術だけでは著作権問題を解決することは困難である．なぜならば，暗号通信を行えば通信路上での盗聴に対する脅威は回避することができるが，復号処理を行った後のファイルに関しては，全く保護できないからである．例えば，ある購入者がディジタルコンテンツをネットワークを介して購入した場合，第三者からの盗聴は防ぐことはできるが，購入者が不正にコピーを作成すること，更には配布することは防ぐことはできない．ゆえに，暗号技術とは別の新しい著作権侵害問題を解決できる技術が必要である．そのような技術として注目されているものの一つに電子透かし技術がある．

電子透かしとは，ディジタル情報に別の情報を知覚されないように密かに埋め込む技術である [1]．特に，音声や画像，動画などのディジタルコンテンツは，それ自体に冗長が多く含まれているため，その冗長部分に別の情報を埋め込むことが可能である．冗長成分への埋め込みにより生じる劣化は，人間の目や耳では知覚されにくいことから，埋め込みによる不自然さがあまり生じない [2]．電子透かし技術では，埋め込む情報に応じて，その用途が異なる．例えば，著作者を示す情報を埋め込めば，コンテンツが不正配布された場合に透かし情報を抽出することで著作権を主張できる [3][4][5]．また，購入したユーザの情報を埋め込めば，不正者を特定することができる．後者の使用に関しては，専門的に電子指紋とも呼ばれる [6]．更に，著作権保護対策が施されていることを示せば，不正を抑制する効果が期待される．

本研究は，大きく分けて次の四つの研究テーマからなる．

(1) DCT 係数の加法特性を利用した電子透かし

(2) 画像の局所情報に基づく電子透かし

(3) 埋め込み信号間の距離に基づく電子透かし

(4) 加法性準同型写像の性質を用いた効率の良い電子指紋プロトコル

研究テーマ (1)，(2) では，ディジタル画像を取り上げ，人間の視覚特性に基づいて埋め込みを行うことで，画質劣化を抑える手法を提案する．研究テーマ (3) では，従来とは全く異なる埋め込み手法を用いて動画像に適用可能な方式を提案する．また，岡本–内山暗号 [7] の加法性準同型写像の性質を利用して，効率良く電子指紋を埋め込み，送信できる手法を研究テーマ (4) で述べる．

これまでに提案されたディジタル画像の電子透かしには，透かし情報を画素単位で埋め込む方式 [8][9] や周波数成分に埋め込む方式などがある [3][4][5]．一般に，透かし情報を画素単位で埋め込まれた信号よりも，周波数成分に埋め込まれた信号の方が各画素に拡散されるため，画質劣化が生じにくい．また，画像全体を歪ませなければ，取り除くことが困難となるため周波数成分に埋め込む方式が多く提案されている [1]．画像の周波数成分は離散コサイン変換，離散フーリエ変換，離散ウェーブレット変換などの直交変換を行うことにより得られる [2][10]．一般に，画像の低周波成分には画像信号のエネルギーが集中するため，画像の重要な成分を含むことが知られている [2][10]．画像圧縮や雑音処理では低周波成分をあまり変化させないため，この成分に透かし情報を埋め込めば取り除くことは困難になる．また，計算量や埋め込む透かし情報の情報量を考慮すれば，ブロックに分割し，各ブロックの低周波数成分に埋め込む手法が効果的であると考えられる．しかし，低周波成分に埋め込みを行った場合，隣接するブロック間の境界が不連続となり，知覚されやすいブロック歪みが生じる可能性が高い．ゆえに，低周波成分への埋め込みは有効であることは知られているが，画質劣化が激しいため従来手法では低周波成分は避けて埋め込みが行われている [4][5]．そこで，ブロック歪みが生じないように画像の低周波成分への埋め込みを可能とする手法を第一のテーマで提案する．このテーマでは，まず離散コサイン変換の 4 個の基底画像を重ね合わせることで生成される模様が知覚されにくいことを示す．次に，この特徴を利用して透かし情報の各ビットをそれぞれ対応するブロックの 4 個の DCT 係数に埋め込む手法を提案する．この手法の優れた点は，各ブロックの 4 個の DCT 係数に埋め込まれた透かし信号がブロックの中央に位置するサブブロックの 1 個の DCT 係数から検出可能であるところである．サブブロックはブロックサイズが小さいため，検出に必要な計算量は少ない．

透かしの埋め込まれた画像を幾何学的に歪ませるとブロックの位置が移動するため，透かし情報を正しく検出できなくなる [11][12][13]．従来の手法 [14][15] では，画像全体の回転や拡大縮小，平行移動に対しては対応できるが，ランダムな幾何学的な歪みに対しては対応できな

い．第一のテーマでは，透かしの埋め込み検出操作だけでなく，幾何学的な歪みを受けた場合に元の座標位置を回復するための操作を各ブロックごとに行う手法も提案する．この手法を用いれば，ランダムな幾何学的な歪みに対しても元のブロックを取り出し，そこから透かし情報を取り出すことが可能である．この手法は，大変有効な手法であるため，第二のテーマにおいても用いる．

複雑な図形やエッジの多い高周波領域周辺に存在する誤差や歪みは知覚されにくいため，第二のテーマではこの人間の視覚特性に基づいて埋め込みを行う．画像の全体が複雑な模様であることは少なく，局所的にそのような領域が存在している．そのため，局所的に領域を選出することで，画像の特徴に基づいた埋め込みを行う．複雑な模様に合わせて，埋め込む透かし信号も複雑な模様に変調させた方が画像の特徴を活かすことができる．そこで，スペクトル拡散に基づく電子透かし法 [3] を利用し，透かし信号を複雑な模様に変調させて埋め込みを行う．ただし，高周波成分は信号処理などの操作により改変されやすいため，提案手法では高周波成分を避けて，ある範囲内の周波数成分だけに埋め込みができるようにウェーブレット変換を用いる．

画素単位で埋め込む方式では，埋め込み検出操作が単純に行えるため，周波数領域に埋め込む方式よりも計算量の点で優れている [9]．特に，画像の統計量に基づいて画素の輝度値を変化させる方式 [8] などは，データ量が多くリアルタイム性などを求められる動画像を扱うためには適した方式と考えられる．そこで，第三のテーマでは，統計量に基づく方式を用いて信号の埋め込みを行う．従来法 [16] では，幾何学的な改変に対する対策として，統計量に基づく方式を用いて同期信号が埋め込まれている．もし，幾何学的な歪みが生じていれば，同期信号を検出し，歪みを補正した後に透かし信号の検出を行う．この手法では，透かし情報は別の手法を用いて埋め込まれるため，透かし信号と同期信号の両方を動画像に埋め込まなければならない．また，同期を回復する操作を行った後に透かし検出を行うため，計算量が莫大となり，リアルタイム処理は困難であると考えられる．そこで，同期信号を埋め込む際にその位置関係に情報を与えることで透かし情報を埋め込む手法を提案する．信号処理の観点から電子透かし技術を考えるならば，従来法は輝度値や周波数成分の値を変化させるため，パルス振幅変調とみなすことができる．一方提案手法は，同期信号の位置関係を変化させて埋め込みを行うため，パルス位置変調とみなせる．この手法は，透かし情報を埋め込むことのできる新しい領域を示したという意味において，斬新な手法である．

ネットワーク上の売買において，電子指紋技術では販売者は購入者を特定する情報 (電子指紋) の埋め込まれたコンテンツを購入者に販売する．この技術を用いれば，たとえ不正コピーが流出したとしても，埋め込まれた情報を正しく検出できれば不正者を特定することができる [6]．ただし，販売者が取り引き終了後に電子指紋の埋め込まれたコンテンツを持っている

ならば，不正者を発見してもその事実を別の第三者に証明することができない．なぜなら，販売者自身がそのコンテンツを配布して，購入者を陥れようとする可能性があるからである．そこで，電子透かし技術と暗号プロトコルを組み合わせて，取引終了後に購入者だけが電子指紋の埋め込まれたコンテンツを得ることができる手法が提案されている [17][18][19][20]．これらの手法では，平方剰余に基づくビットコミットメント [21] を用いて，電子指紋を生成し，埋め込み操作を行っているが，暗号化率が極めて低いため実用的ではない．そこで，第四のテーマでは，岡本–内山暗号が有する加法性準同型写像の性質を用いて，効率的な電子指紋プロトコルを提案する．この手法では，購入者が販売者に電子指紋を委託して，コンテンツに埋め込んでもらうプロトコルを提案する．また，委託する電子指紋の正当性を示すためのプロトコルも提案する．本手法を用いれば，取引中において，電子指紋及びコンテンツは岡本–内山暗号で暗号化されており，その暗号文を復号できるのは購入者だけである．また，販売者は，複数の暗号文を乗算などの処理を行うことで暗号化された電子指紋を暗号化したコンテンツに埋め込むことができる．提案電子指紋プロトコルに適用できる電子透かし法に関して，簡単な手法を示す．その手法は，第一，第二テーマで提案した手法にも拡張できる．

以下，本論文の構成について述べる．第 2 章では，本研究で用いる各種信号処理の技術及び従来法について述べる．また，電子透かし技術の評価方法を紹介する．第 3 章では，第一の研究テーマである DCT の加法特性を利用した電子透かしの手法を提案し，幾何学的な歪みから同期位置を回復する手法を示す．第 4 章では，第二の研究テーマとして画像の局所情報に基づく電子透かしの手法を提案する．第 5 章では，第三の研究テーマである埋め込み信号間の距離に基づく電子透かしを提案する．第 6 章では，電子透かし技術の応用である電子指紋技術として，加法性準同型写像の性質を用いた電子指紋プロトコルを提案する．最後に，第 7 章では，結論として研究成果をまとめる．

第2章　電子透かし

2.1　緒言

電子透かしは，画像や音声，動画などのディジタル情報をあまり歪ませることなく別の情報を密かに埋め込むことができる技術であり，利用する目的により埋め込む情報や埋め込み方法を変化させることで，様々なシステムに応用できる．

本章では，まずディジタル画像の電子透かし技術の基礎となる画像処理技術について述べる．次に，本論文で提案する方式の基礎となる電子透かし技術をいくつか紹介する．また，電子透かし技術と暗号技術を応用させた電子指紋技術の概要について説明し，その技術を理解する上で必要となる暗号技術を述べる．

2.2　ディジタル画像処理技術

ディジタル画像の処理技術は多岐にわたって存在するため，ここでは電子透かし技術で主に用いられる一部についてのみ紹介する．まず，画像から雑音を取り除く処理や画像の特徴を調べるために用いられるフィルタ処理やエッジ検出について示す．次に，画像圧縮をする際に使われる基本的な直交変換を紹介し，その圧縮の手順などを示す．

2.2.1　フィルタ処理

画像にフィルタ処理を施す方法として，マスクを利用する方法と，隣接する画素間の中央値や平均値などを利用する方法がある．LPF(Low Pass Filer) や HPF(High Pass Filter)，雑音除去などにフィルタ処理が使われている．

まず，初めにマスクを利用する方法を説明する．マスクは一般に $(2k+1) \times (2k+1)$ 行列で表され，画像の輝度値と行列演算させることでフィルタ操作が行われる．マスクの行列を $m(i,j), (-k \leq i,j \leq k)$ とし，画像の輝度値を $f(x,y)$ とするとフィルタ処理を行った後の画像 $f'(x,y)$ は，次の式により計算することができる．

$$f'(x,y) = \sum_{i=-k}^{k} \sum_{j=-k}^{k} m(i,j) f(x-i, y-j) \tag{2.1}$$

例えば，3×3 サイズのガウシアンフィルタには次のマスクが用いられる．

$$\frac{1}{16} \begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{bmatrix}$$

中央値や平均値を利用する方法では，フィルタを施す領域として窓を設定し，注目する画素を中心とした領域内の中央値もしくは平均値を求める．中央値を出力するフィルタを特にメディアンフィルタと呼ぶ．例えば，窓の中の各画素の輝度値が $\{12, 32, 2, 28, 9, 13, 21, 16, 11\}$ のとき，メディアンフィルタの出力は 13 となり，平均値フィルタの出力は 16 となる．代表的なメディアンフィルタの窓としては，3×3 の正方形であり，本論文ではこの窓サイズを用いることにする．

2.2.2 エッジ検出

画像の雑音を無視することができるならば，画像の高周波成分を強調することでエッジ検出を行うことができる．しかし，画像に雑音が含まれる場合は，雑音が大きくなるにつれてエッジ検出が難しくなる．そのため，平滑化処理を行った後にエッジ検出を試みることが望ましい．

エッジを強調する方法としては，HPF を利用する方法と微分オペレータを利用する方法が考えられる．HPF では，マスクの値を適切に設定すれば簡単に処理を行うことができる．しかし，雑音に弱いため，LPF などの平滑化が必要である．一方微分オペレータを利用する場合，HPF に比べ雑音の影響を比較的受けにくいことが知られている [2]．ここでは，微分オペレータとして Sobel の勾配を紹介する．

Sobel の勾配を得るオペレータは，

$$Df(x,y) = \sqrt{\{v(x+1) - v(x-1)\}^2 + h(y+1) - h(y-1)^2} \tag{2.2}$$

で定義される．ただし，

$$v(x+1) = f(x+1, y-1) + 2f(x+1, y) + f(x+1, y+1), \tag{2.3}$$

$$v(x-1) = f(x-1, y-1) + 2f(x-1, y) + f(x-1, y+1), \tag{2.4}$$

$$h(x+1) = f(x-1, y+1) + 2f(x, y+1) + f(x+1, y+1), \tag{2.5}$$

$$h(x-1) = f(x-1, y-1) + 2f(x, y-1) + f(x+1, y-1). \tag{2.6}$$

ここで，D は Sobel オペレータと呼ばれている．

2.2.3 離散コサイン変換

離散コサイン変換 (Discrete Cosine Transform:DCT) は，画像信号を周波数領域に直交変換する方法の一つである [10]．この DCT により変換された周波数成分は，符号化効率に直接影響を及ぼす低周波成分へ電力が集中する．また，高速演算アルゴリズムが存在することから，画像の直交変換符号化の際には DCT がよく用いられている．一次元直交変換は水平方向の成

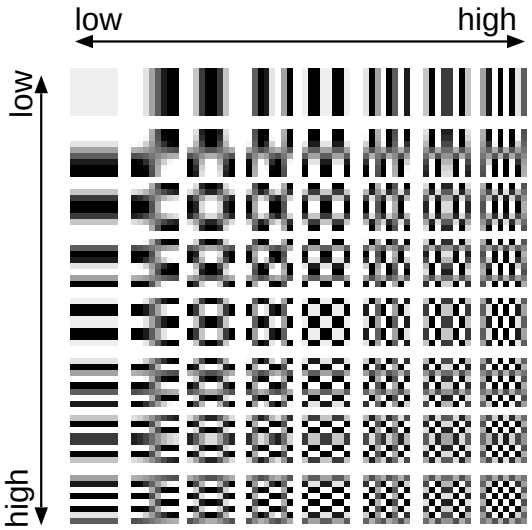


図 2.1　2 次元 DCT(8×8) の基底画像

Fig. 2.1　The basic matrices of 2-dimensional DCT(8×8).

分に対する変換であり，二次元である画像情報に対しては二次元直交変換が用いられる．二次元 DCT は，$M \times N$ 画素の画像を $f(x, y), (0 \leq x \leq M-1, 0 \leq y \leq N-1)$ とし，変換後得られる $M \times N$ 個の DCT 係数を $F(X, Y), (0 \leq X \leq M-1, 0 \leq Y \leq N-1)$ とすると，次のように表される．

$$F(X,Y) = \frac{2c(X)c(Y)}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos\left\{\frac{(2x+1)X\pi}{2M}\right\} \cos\left\{\frac{(2y+1)Y\pi}{2N}\right\} \tag{2.7}$$

また，逆変換 (IDCT) は次式で表される．

$$f(x,y) = \frac{2}{\sqrt{MN}} \sum_{X=0}^{M-1} \sum_{Y=0}^{N-1} c(X)c(Y)F(X,Y) \cos\left\{\frac{(2x+1)X\pi}{2M}\right\} \cos\left\{\frac{(2y+1)Y\pi}{2N}\right\} \tag{2.8}$$

ただし，$c(t)$ は次の式で与えられる．

$$c(t) = \begin{cases} \frac{1}{\sqrt{2}} & (t=0) \\ 1 & \text{その他} \end{cases} \tag{2.9}$$

例として，$M, N = 8$ の場合の DCT 係数 $F_8(X, Y)$ に対する基底画像を図 2.1 に示す．$F_8(0, 0)$ は，直流成分の係数を表し，$F_8(X, Y)$ は X や Y が大きくなるほど高周波成分に相当する基底画像の変換係数に対応する．

2.2.4　離散ウェーブレット変換

DCT はブロック単位で実行される場合，隣接するブロック間において不連続となる可能性があり，その結果ブロック歪みが発生しやすい欠点がある．画像全体に DCT を施すとブロッ

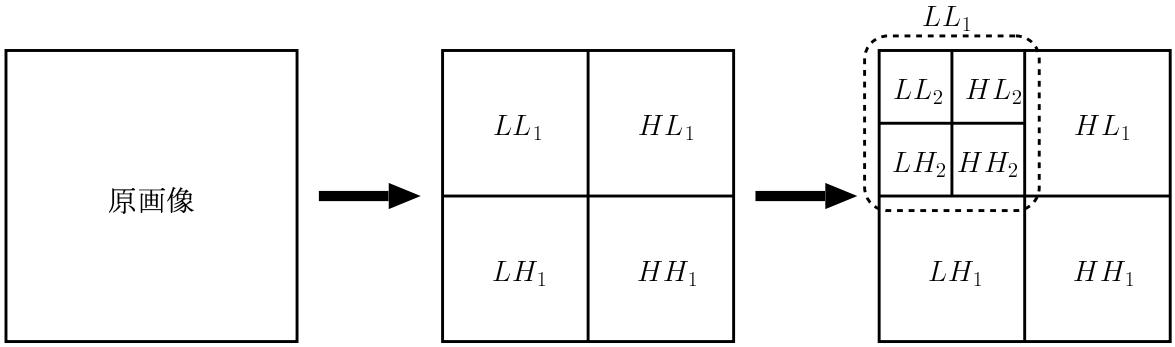


図 2.2　ウェーブレット変換の流れ

Fig. 2.2　The procedure of wavelet transform.

図 2.3　ウェーブレット変換による画像表現

Fig. 2.3　The representation of wavelet transformed image.

ク歪みは生じないが，計算量が莫大となってしまう．そこで，比較的少ない計算量で，画像全体を直交変換する方法としてウェーブレット変換がある．

ウェーブレット変換には，使用される基底によりいくつかの方法があるが，本論文中では，最も簡単なハール基底によるウェーブレット変換を扱う．まず，画像は 4 つのサブバンド LL_1, LH_1, HL_1, HH_1 に分割される．ここで，LL_1 は多重解像度近似 (MultiResolution Approximation: MRA) 部と呼ばれ，画像の縦横の比率を 1/2 に縮小させた画像となる．LH_1, HL_1, HH_1 は多重解像度表現 (MultiResolution Representation: MRR) 部と呼ばれ，LH_1 は縦方向の変化を，HL_1 は横方向の変化を，HH_1 は斜め方向の変化を示す．LL_1 は縮小画像なので，更に 4 つのサブバンド LL_2, LH_2, HL_2, HH_2 に分割することができる．同様に LL 部は 1×1 要素になるまで分割を繰り返すことができる． 図 2.2 に第二階層まで分割する手順を示す．また，256×256 画素，白黒濃淡 256 階調の画像 “lena” にウェーブレット変換を階層ごとに施した際の結果を図 2.3 に示す．

ウェーブレット変換では，各階層ごとに周波数が異なり，階層が高いほど高周波成分となる．階層ごとに周波数成分を分割できるため，周波数ごとに適応的に圧縮符号化を行うことが可能となる．

2.2.5 JPEG 圧縮

静止画像の符号化国際標準として規格化されたものを JPEG(Joint photographic experts group) と呼んでいる [2]．画像を非可逆圧縮する場合には DCT が用いられており，可逆圧縮として予測符号化の手法が用いられている [2][10]．ここでは，非可逆圧縮の手順について述べる．静止画像には白黒濃淡画像とカラー画像があるが，まず白黒濃淡画像の圧縮に関して説明し，その後でカラー画像へと拡張させる方法を説明する．

初めに，画像を 8×8 画素のブロックに分割し，それぞれに DCT を施す．次に表 2.1 に示す量子化テーブルに基づいて各 DCT 係数値を量子化する．ここで，この量子化テーブルの値を

表 2.1　JPEG 圧縮の量子化テーブル

Table 2.1　Quantization table of JPEG compression.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

直接量子化操作に使うのではなく，画質パラメータ $q, (0 < q \leq 100)$ によってスケーリング操作を行った値を用いる．スケーリング操作は，量子化テーブルの値を $Q(x, y)$ とすると次の式に基づいて行われる．

$$Q'_{x,y} = \begin{cases} \dfrac{50}{q} Q(x, y) & q < 50 \\ \dfrac{100 - q}{50} Q(x, y) & 50 \leq q \leq 100 \end{cases} \tag{2.10}$$

この量子化テーブルは人間の視覚特性に基づいて作成されており，低周波成分ほど細かく，高周波になるほど荒く量子化されるようになっている．そのため，このテーブルを使えば，適応的な量子化が行える．量子化を行った後に，周波数の低い順に並べてから算術符号化を行うことで高周波成分に発生する係数の偏りを効率よく圧縮符号化することができる．

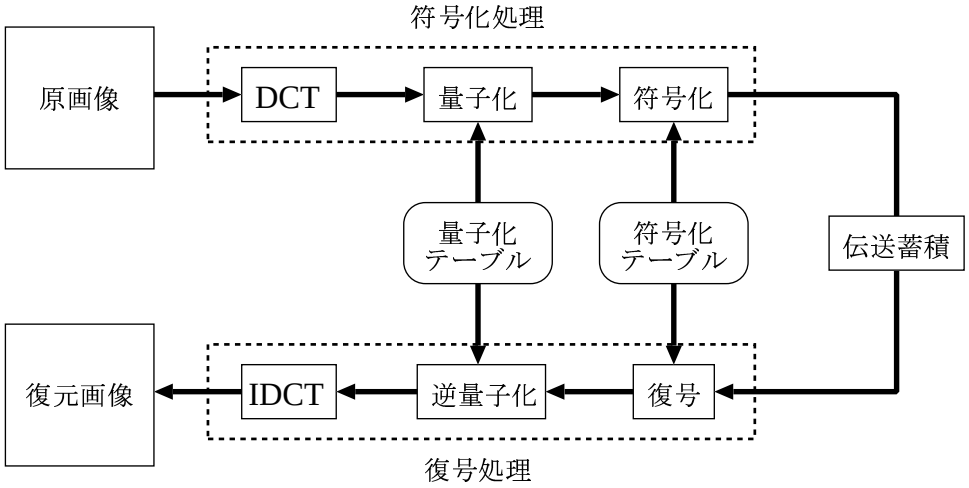


図 2.4　JPEG の基本処理の流れ

Fig. 2.4　The precedure of JPEG operation.

圧縮された画像を伸長するには，圧縮操作の逆操作をそれぞれ行えばよい．まず，算術符号化された符号語を復号し，次に量子化された DCT 係数をそれぞれ逆量子化させる．これらの操作には，圧縮の際に用いた各テーブルが必要となる．最後に逆離散コサイン変換 (IDCT) を行えば，復元画像が得られる．以上，圧縮伸長操作の流れを図 2.4 に示す．

次に，カラー画像へと拡張させる場合に関して述べる．通常カラー画像は赤 (R) 緑 (G) 青 (B) の各 8 ビットで表現され，白黒濃淡画像に比べ，3 倍のデータ量からなる．そのため，直接伝送したり，保存したりすることは極力避け，RGB 表示系から YC_rC_b 表示系に変換し圧縮を行う．その変換方法を次に示す．

Step 1 入力 (R, G, B) を 0 から 1 の範囲に正規化する．これを (r, g, b) で表す．

Step 2 (r, g, b) を以下の式にしたがって (y, c_r, c_b) に変換する．

$$y = 0.701 \cdot r + 0.587 \cdot g + 0.114 \times b \tag{2.11}$$

$$c_r = 0.713 \cdot (r - y) \tag{2.12}$$

$$c_b = 0.564 \cdot (b - y) \tag{2.13}$$

Step 3 (y, c_r, c_b) を以下のように (Y, C_r, C_b) に変換する．

$$Y = 219 \cdot y + 16 \tag{2.14}$$

$$C_r = 224 \cdot c_r + 128 \tag{2.15}$$

$$C_b = 244 \cdot c_b + 128 \tag{2.16}$$

ここで，Y は輝度成分，(C_r, C_b) は色差成分となる．JPEG 圧縮では，これらの成分においてサンプリング間隔を

$$Y : C_r : C_b = 4 : 2 : 2 \tag{2.17}$$

の割合でデータを間引く操作が行われる．その結果，符号化効率を大幅に向上させることができる．ここで，輝度成分には表 2.1 の量子化テーブルが用いられ，色差成分は別の量子化テーブルが用いられる．

2.3 電子透かし技術

電子透かし (digital watermark) 技術とは，あるディジタル情報に別の副情報 (透かし情報) を知覚されないように埋め込む技術である．透かし情報として著作権情報を用いれば，不正コピーから埋め込まれた情報を取り出すことにより著作権を主張できる．紙幣の場合，その真偽を見分けるために色合いやインク，紙質などの印刷条件と紙幣番号，透かしなどの付加条件を用いる．特に，自動販売機などで機械的に真偽を判定する際に，この透かし模様は重要な役割を果たす．この概念をマルチメディアに応用したものが電子透かしである．紙幣の透かしでは光学的な手法を用いるが，ディジタル情報では数学的な手法を用いる．また，電子透かしでは透かし情報は必ずしも意味のある模様である必要はなく，ディジタル情報として読み取ることができるものであればよい．以下に電子透かしに求められる条件をいくつか挙げる．

- 透かし情報はコンテンツ自身に埋め込まれる．ヘッダ部分や特定の領域に集中せずに，全域にわたり分散されていることが望ましい．
- 透かし情報は各種信号処理に対して変質，若しくは消失しない．
- 埋め込みにより激しい品質劣化を生じない．
- 透かし情報の埋め込み検証に必要な処理は簡単で，処理時間は短いほうが望ましい．

この電子透かし技術を用いて，ディジタル情報の著作権保護を目指す研究が現在盛んに行われている [3][4][5]．従来の暗号化技術では，通信路上での安全性は保証できるが，復号された後の複製や再配布に対して取り締まることは難しい．そこで，コンテンツ自体に著作権情報を埋め込むことにより，それらを抑制する効果が期待される電子透かし技術に注目が集まっている．

2.3.1 量子化方式

アナログ信号をディジタル信号に変換するには量子化操作が行われる．量子化操作では，信号値はあるステップサイズにより除算され，最も近い整数値に丸められる．この際に生じる

誤差に透かし情報を与える方式が量子化法である．透かし情報が $w = 0$ ならば最も近い偶数値に，$w = 1$ ならば最も近い奇数値に丸めることにより 1 ビットの情報を埋め込むことができる．この操作は，直接画素値をあるステップサイズで量子化する場合にも用いることができるが，主に画像の周波数成分などへの埋め込みに使われる．

例えば，画像を DCT やウェーブレット変換し，秘密情報により選出した変換係数に透かし情報を埋め込む場合を考える．この場合，その係数値をあるステップサイズで量子化する際に，奇数値もしくは偶数値に丸めることで透かし情報 1 ビットを埋め込むことができる．検出する場合，埋め込みに用いた同じ係数を取り出し，同じステップサイズで量子化してその値の偶奇により透かし情報ビットを判定する．そのため，量子化法では検出対象の画像さえあれば，透かし情報の検出操作を行うことができる．ステップサイズを Q とし，元の係数値 $F(x, y)$ に透かし情報 $w \in \{0, 1\}$ を量子化法で埋め込む流れを図 2.5 に示す．

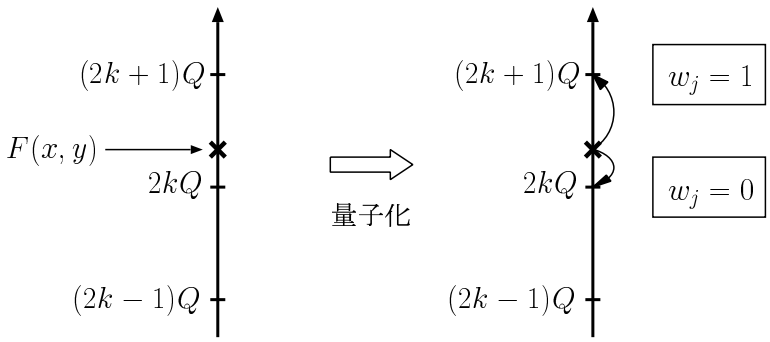


図 2.5　量子化法

Fig. 2.5　Quantization method.

2.3.2　スペクトル拡散方式

スペクトル拡散システムでは，情報を伝送するのに必要な帯域幅を，情報とは独立した信号により広帯域に拡散させて通信している．その結果，雑音による干渉や妨害を受けにくくなり，信号の秘匿性も向上させることができる．

スペクトル拡散では，送信する信号はそれよりもはるかに広帯域の信号を乗算することで変調される．その広帯域信号として，擬似乱数 (Pseudo-Random: PN) 系列を用いる．この PN 系列はランダムな 0 と 1 からなる 2 値系列 (0 を -1 と置き換えて使う場合もある) であり，その周波数成分には偏りがほとんどなく一様分布をする．また，自己相関値は信号位置が少しでもずれると低く抑えられる．

PN 系列の特性を利用したスペクトル拡散を透かし信号の埋め込みに用いることで得られる特徴を以下に示す．まず，透かし情報を変調させてから埋め込みを行えば，広帯域に拡散され

た信号は雑音成分のように振る舞う．また，埋め込みに用いたPN系列は正しい同期位置で相関を取らなければ検出されない．ゆえに，元のPN系列が分からなければ攻撃者が透かし信号を改ざんすることは困難である．更には，透かし信号が広帯域に拡散されるため，視覚的な劣化も生じにくい．

次に，スペクトル拡散通信を例を挙げて説明する．送信信号を $a(t)$，PN系列を $pn(t) \in \{-1, 1\}$，拡散された送信信号 $A(t)$ は，

$$A(t) = a(t) \cdot pn(t), \tag{2.18}$$

となる．通信路上で雑音 $n(t)$ が加わったとすると，受信信号は，

$$A'(t) = A(t) + n(t), \tag{2.19}$$

である．$\{pn(t)\}^2 = 1$ となるので，この信号に再度PN系列を乗算すれば，

$$\begin{aligned} y(t) &= A(t) \cdot pn(t) + n(t) \cdot pn(t), & (2.20)\\ &= a(t) \cdot \{pn(t)\}^2 + n(t) \cdot pn(t), & (2.21)\\ &= a(t) + n(t) \cdot pn(t), & (2.22) \end{aligned}$$

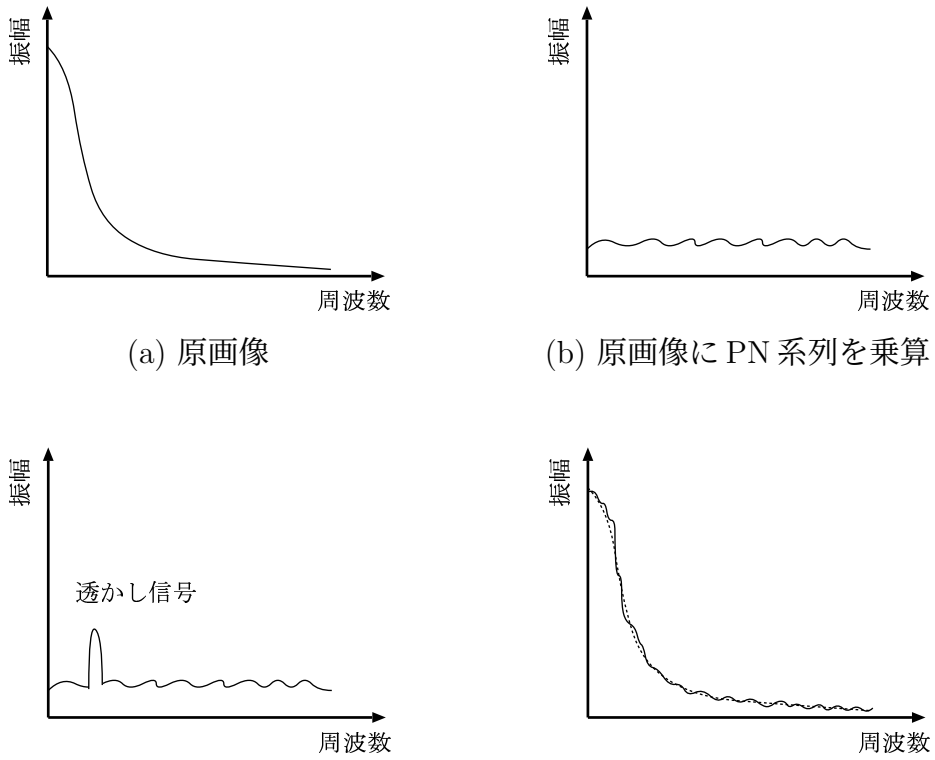
となる．故に受信側において，雑音 $n(t)$ はPN系列により拡散されており，送信信号 $a(t)$ に及ぼす影響は小さく抑えられる．

画像の特徴としてエネルギーが低周波成分に集中することが知られている．そこで，透かし情報を埋め込む場合には，まず画像信号にPN系列を乗算することでそのエネルギーを周波数成分全体に拡散させる．次に，特定の周波数成分に透かし信号エネルギーを与える．最後に，もう一度PN系列を乗算することで埋め込み画像を得る．透かし信号エネルギーは，PN系列を乗算することで広帯域に拡散されるため，実際には画像の周波数成分全体に拡散されて透かし信号エネルギーが与えられたことになる．これらの操作による周波数成分の変化を図2.6に示す．この透かし信号を除去もしくは改ざんするためには，PN系列が分からなければ難しい．なぜならば，透かし信号を除去するためには，画像をあまり劣化させずに周波数成分全体を変化させなければならないからである．

スペクトル拡散方式では，透かし信号を埋め込む際に量子化法を用いて埋め込めば，検出に原画像を必要としない方式として用いることができる．

2.3.3 統計量に基づく方式

パッチワーク法は，1995年にBenderら [8] によって提案された手法であり，統計的な性質に基づいて透かし情報の埋め込み，検出を行う．統計的な性質とは，ランダムに選出した二つ



(a) 原画像　(b) 原画像に PN 系列を乗算

(c) 透かし情報の埋め込み　(d) 逆拡散

図 2.6　拡散系列により生じる周波数成分の変化

Fig. 2.6　Changes in the frequency components caused by PN sequence.

の画素の輝度値をそれぞれ a_i, b_i とし，その差を

$$s_i = a_i - b_i, \tag{2.23}$$

とすると，

$$E[s_i] = 0 \tag{2.24}$$

となる性質のことである．ただし，$E[\cdot]$ は期待値演算とする．ここで，複数の s_i の和を

$$S(n) = \sum_{i=0}^{n-1} s_i = \sum_{i=0}^{n-1} (a_i - b_i) \tag{2.25}$$

とすると，その値は n の値が十分大きければガウス分布する．また，その平均値は式 (2.24) より 0 となる．透かし情報ビットを埋め込むためには，α を埋め込み強度として，式 (2.23) を次のように変形させる．

$$s_i{}' = (a_i + \alpha) - (b_i - \alpha) \tag{2.26}$$

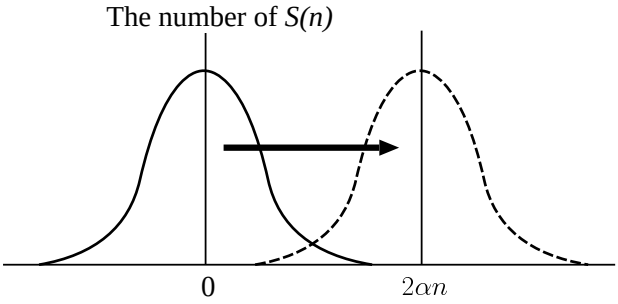


図 2.7　$S(n)$ の分布

Fig. 2.7　The distribution of $S(n)$.

その結果，その期待値は，

$$E[s_i'] = E[a_i - b_i + 2\alpha], \tag{2.27}$$

$$= E[s_i + 2\alpha], \tag{2.28}$$

$$= E[2\alpha] \tag{2.29}$$

となる．ゆえに，s_i' の和は

$$S(n)' = \sum_{i=0}^{n-1}((a_i + \alpha) - (b_i - \alpha)), \tag{2.30}$$

$$= \sum_{i=0}^{n-1}(a_i - b_i) + 2n\alpha, \tag{2.31}$$

となり，その平均値は $2n\alpha$ だけ増加する．その様子を図 2.7 に示す．統計的な性質により，この増加分が十分大きければ，透かし情報を判別することができる．

2.3.4　視覚特性を利用する方式

周波数成分への埋め込みでは，主に高周波成分の値を改変することにより行われる．それは，複雑な図形やエッジの多い高周波領域周辺に存在する誤差や歪みが知覚されにくいという人間の視覚特性に基づくためである．しかし，高周波成分だけでなく低周波成分もまた知覚されにくいことが知られている [22]．例えば，ω を周波数，$H(\omega)$ を視覚感度とすると次式のような特性がある．

$$H(\omega) = 2.6(0.0192 + 0.114\omega)\exp\{-(0.144\omega)^{1.1}\} \tag{2.32}$$

この式は，角度 (視野角)1 度あたりの周波数 (白黒のストライプ) の模様を一定距離の場所から見せ，その間隔がある値以下になると，人間の視覚ではそれをストライプとして知覚できなくなることを表している．図 2.8 に周波数と視覚感度の関係を示す．

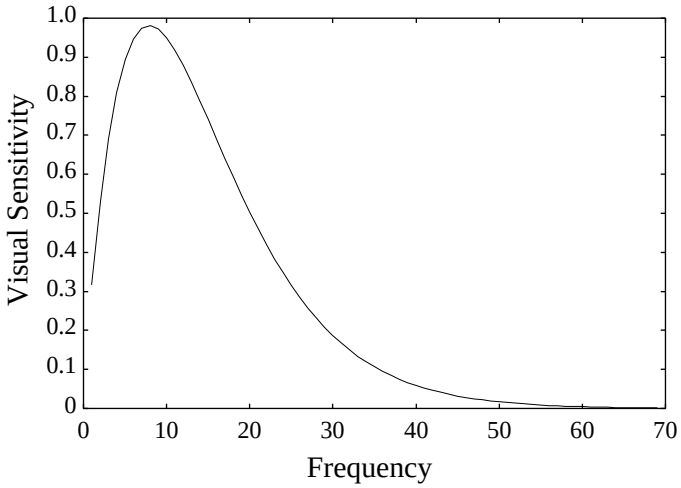


図 2.8　周波数と視覚感度の関係

Fig. 2.8　Visual sensitivity versus frequency.

図 2.8 より高周波成分の感度は低いことが分かる．そのため高周波成分に埋め込まれた信号は視覚的にあまり影響を及ぼさないと考えられる．しかし，高周波成分は画像圧縮の際に大幅に削減されてしまうため，この成分に埋め込まれた信号は各種信号処理の影響を受けやすい．対照的に，低周波成分は画像の重要な成分を含むため，各種信号処理などによる影響を受けにくい．また図 2.8 に示すように，低周波成分もまた感度が低下することが分かる．以上のような特徴を適切に活用すれば，ディジタル画像に適した埋め込みが可能である．

2.4　電子透かしの評価

電子透かしでは，埋め込みによる劣化が知覚されにくいこと，攻撃に対する耐性が高いことなどを評価することが重要である．画質劣化は，一般的な画像や動画像の評価指標として使われる PSNR の値により評価される．電子透かしの耐性評価は，透かし情報が埋め込まれた画像に攻撃を加え，その攻撃後の画像から透かし情報が正しく検証されるか否かにより判定する方法が用いられている．ここで攻撃とは，透かし情報を正しく取り出せないように画像を歪ませるものであり，各種信号処理や情報源圧縮や幾何学的な処理などに分別される．以下に，想定される攻撃法と本論文で扱う StirMark 攻撃 [11][12][13] について説明する．

2.4.1　PSNR

一般に，信号の劣化を評価するためには信号対雑音比が用いられる．しかし，この指標を用いる場合，信号値の大きさに依存するため，相対的な評価には向いていない．そこで，画質劣

化を評価するには，ピーク信号対雑音比である PSNR(Peak Signal to Noise Ratio) が用いられる．$M \times N$ 画素，256 階調の原画像 $f(x,y)$ と埋め込み画像 $f'(x,y)$ に対する PSNR は次の式で定義される．

$$\mathrm{PSNR} = 10\log_{10} \frac{255^2}{\dfrac{1}{MN}\displaystyle\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\Big(f(x,y) - f'(x,y)\Big)^2} \tag{2.33}$$

カラー画像の場合，RGB の各成分を 256 階調で表現した場合，式 (2.33) の対数部分の分母において RGB 各成分に関して差分の二乗を計算することで，PSNR を求めることができる．

2.4.2 各種攻撃法

画像に埋め込まれる透かし情報は，各種攻撃に対する耐性を考慮しなければならない．それらの攻撃は，非幾何学的な改変と幾何学的な改変に分類することができる．非幾何学的な改変は，信号処理の手法として広く用いられているものであり，フィルタ操作や圧縮などである．これらの信号処理は，画像に含まれる雑音を除去したり，あまり必要でない成分を削除する．雑音成分として埋め込まれる透かし情報がこれらの信号処理により変質もしくは消失しないことが重要である．一方，幾何学的な改変は，透かし信号自体を除去するために行うのではなく，検出を困難にする攻撃である．

非幾何学的な改変として電子透かしの評価に最も良く用いられる攻撃は，JPEG 圧縮である．攻撃として用いる場合は，透かし信号を除去するために一般的な圧縮率よりも更に低い圧縮率で処理される．他の攻撃としては，各種フィルタ処理が行われ，LPF や HPF などを組み合わせて行うこともある．

幾何学的な改変としては，画像の回転，拡大縮小，平行移動が広く使われる．処理後に不自然さが生じないように，微小な改変が行われた場合の耐性が重要である．また，画像の一部分を切り取る操作なども幾何学的な改変として扱われる．

ディジタル画像の電子透かし評価支援ツールとして StirMark 攻撃が最も活用されているツールの一つであり，この攻撃は上記の攻撃法を複合的にかつランダムに行う．これまでに各種信号処理や JPEG などの圧縮に関しては，耐性を持つ方式が多く提案されている [3][4][5]．それは，これらの攻撃に耐性を持たせることは比較的容易にできるからである．例えば，画質劣化が顕著に現れない範囲内で強い透かし信号を埋め込めばよい．つまり，雑音などにより付加される信号や，データ圧縮や LPF などにより削除される信号よりも大きな信号を透かし情報として埋め込む方式である．また，透かし情報が広範囲にわたり分散されれば画質劣化は知覚されにくくなるため，多くの方式ではこの原理を利用している．しかしながら，線形並びに非線形フィルタリング，非可逆圧縮 (JPEG)，雑音付加などの攻撃をどれも個別に行いその評価を

しており，複合的な攻撃に対してはその耐性が評価されていない場合が多い．また，これまでは幾何学変換である回転，拡大縮小，平行移動に関してあまり評価されていなかった [13]．幾何学変換に耐性を持たせるため，回転，拡大縮小，平行移動に対してその係数が不偏な領域に画像を変換する方式 [14][15] が考案されている．しかし，ランダムにこれらの攻撃を行った場合の耐性に関しては議論されていない．このように従来は，評価方法が確立されておらず，各研究者が独自に攻撃を行い評価をするという体勢であった．そこで一般的な評価ツールとして考案された StirMark 攻撃は，想定される攻撃をランダムにかつ複合的に行う攻撃法として作成され，電子透かしの評価を行う上で重要な役割を果たすようになった．

2.5 電子指紋技術

電子指紋技術では，暗号技術を用いてユーザの電子的な指紋を作成し，電子透かし技術を用いてそれをディジタルコンテンツに埋め込む．もし，ユーザが不正にコピーを配布すれば，埋め込まれている電子指紋を検出することでそのユーザを特定することができる．本節では，電子指紋技術の分類を行い，電子指紋技術に必要となる暗号技術を紹介する．また，本論文で提案する電子指紋プロトコルの基礎となる方式と，用いる岡本–内山暗号について述べる．

2.5.1 分類

ディジタルコンテンツの売買を行う際には，販売者と購入者間で電子指紋プロトコルを行う必要があり，そのプロトコルの特性により電子指紋技術は，次に挙げる三つに分類することができる．

対称方式 販売者と購入者間で売買の取引を行い，販売者が購入者を示す情報を電子指紋として埋め込み，購入者に送信する．電子指紋の埋め込まれたコンテンツは取引終了後，購入者と販売者の両方が所持している．

非対称方式 電子指紋の埋め込み操作は，購入者と販売者の相互プロトコルによって行われる．最終的に購入者だけが自分の電子指紋の埋め込まれたコンテンツを手に入れることができる．

匿名方式 購入者は，匿名で販売者からコンテンツを手に入れることができる．しかし，購入者が不正コピーを流出させれば不正者として特定される．この方式は，非対称方式の特性も有する．

対称方式では，プロトコル終了後に購入者と販売者の両方が電子指紋の埋め込まれたコンテンツを得ることができる．そのため，たとえ販売者が不正コピーを発見し，不正者を特定で

きたとしても，その事実を第三者に証明することはできない．なぜなら，販売者自身が不正コピーを流出させて購入者を陥れようと試みる可能性があるからである．そのため，プロトコル終了後に購入者だけが指紋の埋め込まれたコンテンツを得る非対称方式が提案された [17]．非対称方式の電子指紋プロトコルにおいて，電子指紋自体は販売者に知られないことが重要である．暗号技術を利用した相互プロトコルにより，この特性を可能にしている．匿名方式では，信頼できるセンタに購入者は前もって登録して，その証明書を発行してもらう．購入者は，センタの正規ユーザであることをを販売者に証明できるため，非対称方式の電子指紋プロトコルを匿名でも行うことができる．

Memon と Wong[23] は RSA 暗号 [24] の乗法特性を利用した非対称方式の電子指紋プロトコルを構成している．しかし，作成される電子指紋の正当性やシステムの安全性に関しては議論されていない．Pfitzmann ら [17] は平方剰余に基づくビットコミットメント [21] を利用している．この方式では，購入者は送信する暗号文に正しい電子指紋が含まれていることを証明することができる．また，信頼できるセンタを設置することで匿名方式へと拡張することができ，その安全性も示すことができる [18][19][20]．Pfizmann らによる匿名方式の提案後，計算量の削減に着目した方式 [25] や，センタと販売者の結託に関する購入者の安全性を議論した方式など [26][27] が提案されている．以下では，匿名方式の基礎となる Pfitzmann らの方式で使用されている暗号技術に関して紹介し，そのプロトコルを述べる．

2.5.2 暗号技術とその特性

非対称方式もしくは匿名方式で利用される暗号は，公開鍵暗号方式である．公開鍵暗号方式では，暗号化鍵と復号鍵が異なる暗号方式であり，各ユーザは暗号化鍵は公開リストに登録しておき，復号鍵は秘密に保持しておく．メッセージの送信者は，公開されている受信者の暗号化鍵を使ってメッセージを暗号化して送信する．この暗号文を復号できるのは，復号鍵を持っている受信者だけである．

公開鍵暗号方式の中には，準同型写像の性質を有する方式があり，この性質は暗号プロトコルを構築する上で極めて重要である．準同型写像とは，二つの暗号文を乗算すると別の暗号文となり，そのメッセージが元の暗号文の二つのメッセージにある演算を施したものとなる性質のことである．ここで，ある演算とは，加算，乗算，排他的論理和である．この特徴を利用することでメッセージを公開することなく，特別な処理をメッセージに施すことが可能となる．

定義 2.1 メッセージ m の暗号文を $E(m)$ とすると，準同型写像の性質を有するならば，次の等式を満足する．

$$E(m_1) \cdot E(m_2) = E(g(m_1, m_2)), \tag{2.34}$$

ただし，$g(\cdot)$ は加算，乗算，排他的論理和の演算であり，用いる暗号方式により異なる．

もし，ディジタルコンテンツを m_1，電子指紋を m_2 とすれば，暗号化された情報を暗号化されたコンテンツに埋め込むことができる．

非対称方式の電子指紋プロトコルでは，購入者と販売者が相互プロトコルを行うことで，購入者の電子指紋が販売者のコンテンツに埋め込まれ，購入者だけがその埋め込まれたコンテンツを得ることができる．準同型写像の性質を有する公開鍵暗号方式を用いれば，この相互プロトコルを行うことが可能である．まず，購入者は自分の電子指紋，例えばID情報を自分の暗号化鍵で暗号化し，その暗号文を販売者に送る．販売者は，公開鍵リストから購入者の暗号化鍵を入手し，自分のコンテンツを暗号化する．次に，その暗号文を受信した暗号文と乗算することで暗号化されたコンテンツに暗号化された電子指紋を埋め込む．得られた暗号文は購入者だけが復号できるため，最終的に購入者は販売者から受信した暗号文を復号することで，電子指紋の埋め込まれたコンテンツを得る．以上の操作を図2.9に示す．ただし，Pic は画像を，ID は購入者のID情報とする．

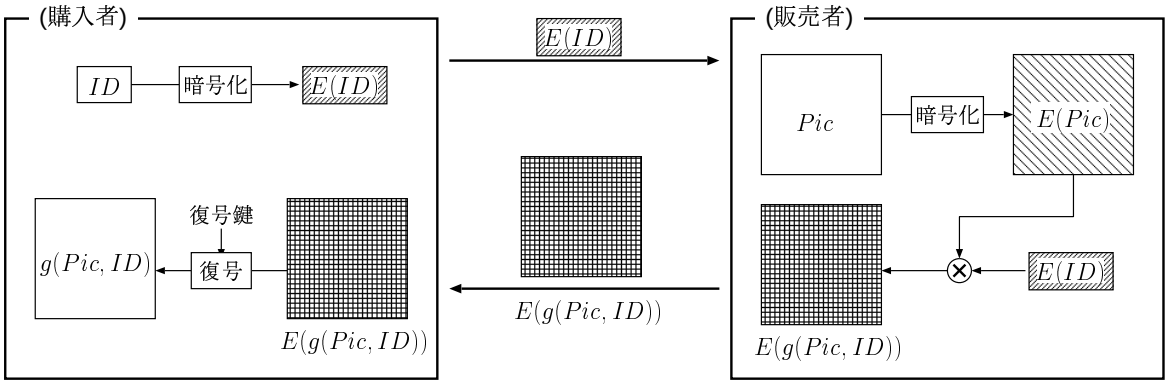


図2.9　非対称方式の電子指紋プロトコルのモデル図

Fig. 2.9　The model of asymmetric fingerprinting protocol.

非対称方式および匿名方式の電子指紋プロトコルを行うためには，暗号のコミットメント手法が必要である．コミットメント手法は，ある情報をある期間内において委託することができる暗号手法である．二者間で取引を行う際に，一方がある情報を委託し，コミットメントを用いた暗号プロトコルによる取引を行った後，委託した情報を公開することで，相手に正当性を示すことができる．このコミットメントには準同型写像の性質があるため，様々な暗号プロトコルに適用が可能である．以下に，これらのコミットメントの生成法を示す．

離散対数問題に基づくコミットメント

大きな素数 P を選び，二つの生成元を g, h とする．ある情報 b のコミットメント com_{DL} は，乱数 $r \in_R (\boldsymbol{Z}/P\boldsymbol{Z})$ を使って次の式で求められる．

$$com_{DL} = g^b h^r \pmod{P} \tag{2.35}$$

この方式では，com_{DL} から b を求めること難しい．ならぜなら，有限体 $\boldsymbol{Z}/P\boldsymbol{Z}$ 上で離散対数問題を解くことと等価であり，この問題は極めて難しいからである．

平方剰余に基づくビットコミットメント

二つの大きな素数 p, q を選び，その積 $n = pq$ を計算する．ある情報ビット b_i のコミットメント com_{QR} は，乱数 $r \in_R (\boldsymbol{Z}/n\boldsymbol{Z})$ を使って次の式で求められる．

$$com_{QR} = (-1)^{b_i} r^2 \pmod{n} \tag{2.36}$$

この方式では，n の素因数分解が分かれば，com_{QR} から b_i を求めることができる．そのため，その安全性は n の素因数分解の困難さに依存している．

離散対数問題に基づくコミットメントは加法性の準同型写像の性質を，平方剰余に基づくビットコミットメントは排他的論理和性の準同型写像の性質を有する．

2.5.3 Pfitzmann らの手法

本論文では，Pfizmann ら [17][19][20] の手法で使用された暗号プロトコルを基本として電子指紋プロトコルを提案する．ここでは，実用面で優れており，非対称方式を内包する匿名方式の概要を示す．

購入者が匿名で販売者からコンテンツを購入するためには，自分の公開鍵でさえ公表できない．そのため，信頼できるセンタに自分の公開鍵を登録し，その際発行してもらう登録証明書を使って販売者に正規ユーザであることを示す．登録証明書は，売買を行う前に行っておく必要があり，また公開鍵と登録証明書の使用は一回限りとしなければ匿名性は保たれない．この登録証明書は，センタから引き出され，コンテンツ購入の際に使われるお金のような役割りを担うため，文献 [19][20] では，ディジタルコインと呼んでいる．

購入者は，登録するたびに異なる公開鍵と秘密鍵のペアを生成し，その公開鍵と自分の ID 情報 ID をセンタに送り登録の手続きを行う．センタは，登録ごとに異なる番号 seq を割り振り，$id = (ID, seq)$ のコミットメント W を計算する．

$$W = g^{id} h^r \pmod{P} \tag{2.37}$$

ただし，W は離散対数問題に基づくコミットメントであり，パラメータ (P, g, h) は電子指紋プロトコルにおいて公開鍵の一部となる．次に，センタは購入者の公開鍵と W の正当性を示す登録証明書を発行する．ここで，電子指紋は id となる．

電子指紋プロトコルは，購入者が公開鍵と W，登録証明書を販売者に送ることにより開始する．販売者は，登録証明書を検証することで購入の依頼者がセンタに登録している正規ユーザ

であることを確認する．離散対数問題に基づくコミットメントは，加法性の準同型写像の性質を有するが暗号文ではないため，復号することはできない．そのため，平方剰余に基づくビットコミットメントを用いる．その際に二種類のコミットメントが内包している情報が等しいことは，零知識会話型証明により示すことができる．各コミットメントの正当性を検証した後，販売者は，排他的論理和性の準同型写像の性質を利用して，暗号化された電子指紋の各ビットを暗号化されたコンテンツに埋め込む．購入者だけが秘密鍵を持っているため，これらの暗号文を復号し，電子指紋の埋め込まれたコンテンツを得ることができるのは購入者だけである．

2.5.4 岡本–内山暗号

1998 年に岡本と内山によって提案された暗号であり，その安全性が素因数分解問題と等価であることが証明されている [7]．また，復号に必要な計算量は代表的な公開鍵暗号方式である RSA 暗号 [24] よりも少ない．更に，一つのメッセージに対して複数の暗号文が存在する確率暗号であり，メッセージに関する情報を完全に秘匿できる強秘匿性の性質を有する．

岡本–内山暗号の暗号化鍵及び復号鍵は以下のように生成される．長さ k ビットの二つの大きな素数 p, q をランダム選び，$N = p^2 q$ を計算する．ただし，p, q は次の関係式を満足するように選出する．

$$g.c.d.(p, q-1) = 1 \tag{2.38}$$

$$g.c.d.(q, p-1) = 1 \tag{2.39}$$

次に，$g_p = g^{p-1} \bmod p^2$ の位数が p となるような $g \in (\boldsymbol{Z}/N\boldsymbol{Z})^*$ を選出する．また，計算量の削減のため，$h = g^N \bmod N$ を計算しておく．この暗号方式の公開鍵は (N, g, h, k) であり，秘密鍵は (p, q) である．法 N の下での指数演算に基づく公開鍵暗号システムを以下に示す．

暗号化 メッセージを m $(0 < m < 2^{k-1})$ とすると，乱数 $r \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$ を用いてその暗号文 C は次の式で計算される．

$$C = g^m h^r \pmod{N} \tag{2.40}$$

復号 受信した暗号文 C を復号するために，まず次の式を計算する．

$$C_p = C^{p-1} \bmod p^2 \tag{2.41}$$

補助関数 $L(x) = (x-1)/p$ を用いて，メッセージは次の式を計算することで復号される．

$$m = \frac{L(C_p)}{L(g_p)} \pmod{p} \tag{2.42}$$

便宜上，岡本–内山暗号の暗号化関数を $E(m,r)$，復号関数を $D(C)$ と表示する．ただし，m はメッセージ，r は乱数，C は暗号文を示す．公開鍵暗号方式である岡本–内山暗号は，次に示す三つの特徴を有する．

P1. 加法性の準同型写像の性質を有する．例えば，メッセージ m_1, m_2 の暗号文を乗算すると，

$$\begin{aligned} E(m_1,r_1)\cdot E(m_2,r_2) &= g^{m_1}h^{r_1}\cdot g^{m_2}h^{r_2} \pmod N, && (2.43)\\ &= g^{m_1+m_2}h^{r_1+r_2} \pmod N, && (2.44)\\ &= E(m_1+m_2, r_1+r_2) \pmod N, && (2.45) \end{aligned}$$

となり，式 (2.34) の関数 $g(\cdot)$ は加算となる．

P2. p 部分群仮定が成り立つならば，暗号文からメッセージに関する情報は 1 ビットも得ることができない．ここで，p 部分群仮定とは，二つの暗号文 $E(0,r_1)$ と $E(1,r_2)$ を区別することは計算量的に困難であることの仮定である．

P3. 誰でも，任意の暗号文 $C = E(m,r)$ を乱数 $r' \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$ により別の暗号文 $C' = E(m, r+r')$ に変更することができる．ただし，内包されているメッセージは変更されない．

$$\begin{aligned} C' &= g^m h^r \cdot h^{r'} \pmod N && (2.46)\\ &= g^m h^{r+r'} \pmod N && (2.47)\\ &= E(m, r+r') && (2.48) \end{aligned}$$

岡本–内山暗号では，k ビットのメッセージ m を暗号化すると，$3k$ ビットの暗号文 C が生成される．ゆえに暗号化率は理論上 $1/3$ となる．

2.6 結言

本章では，ディジタル画像の処理技術及び本論文で提案する手法の基本となる電子透かし技術について述べた．また，ディジタル画像に適した透かし情報の埋め込みを行うために必要となる画像の特徴や攻撃に関することをまとめた．更に，電子透かし技術と暗号技術を組み合わせて構成する電子指紋技術について紹介し，必要となる暗号技術について詳述した．

第3章　DCT係数の加法特性を利用した電子透かし

3.1　緒言

ディジタル画像の電子透かしには，輝度領域に埋め込む手法 [9] と，周波数領域に埋め込む方式 [3][4][5] などがある．最近では周波数成分に透かし情報を埋め込む方式が多く提案されている [1]．それは，一般に周波数成分に埋め込まれた信号は，画像全体に拡散されるため知覚されにくく，攻撃に対する耐性が高いからである．特に低周波成分は各種画像処理による影響を受けにくく，高周波成分と同様に知覚されにくいことが知られている [22]．しかしながら，画像の低周波成分は比較的重要な成分を含むため，埋め込みにより画質が著しく劣化する恐れがある．

本章では，DCT 係数間の加法特性を用いることにより，ブロック歪みの生じにくい電子透かしを提案する．JPEG 圧縮，雑音付加，フィルタリングなどの攻撃は主に画像の高周波成分を変化させるため，低周波領域に透かし情報を埋め込むことにより耐性を持たせることができる．このとき，埋め込む際に生じる歪みが知覚されにくい形状になるように，低周波成分の重ね合わせによる効果を利用する．提案方式では，ブロック歪みが生じにくいだけでなく，透かし情報が埋め込みを行ったブロック中に含まれるサブブロックから検出できる．また，透かし情報と原画像もしくはその一部分を用いて，幾何学変換により生じる同期のずれを回復させる．更に，誤り訂正符号を適用することにより攻撃に対する耐性の向上を目指す．

3.2　DCT係数間の加法特性

DCT 係数は互いに直交する基底関数の成分の大きさを表しており，この基底関数をうまく作用させると，興味深い性質を示す．ここでは，低周波成分のみに着目してその性質を考える．まず，一次元 DCT の場合，その波形の重ね合せを調べる．N シンボルから成る原信号を $f_N(x)$ とし，$F_N(X)$ をその DCT 係数とすると，一次元離散コサイン変換とその逆変換は次式で表される．

$$F_N(X) = \sqrt{\frac{2}{N}} c(X) \sum_{x=0}^{N-1} f_N(x) \cos\left\{\frac{X(2x+1)}{2N}\pi\right\} \tag{3.1}$$

$$f_N(x) = \sqrt{\frac{2}{N}} \sum_{X=0}^{N-1} c(X) F_N(X) \cos\left\{\frac{X(2x+1)}{2N}\pi\right\} \tag{3.2}$$

ただし，

$$c(t) = \begin{cases} \frac{1}{\sqrt{2}} & (t=0) \\ 1 & \text{その他} \end{cases} \tag{3.3}$$

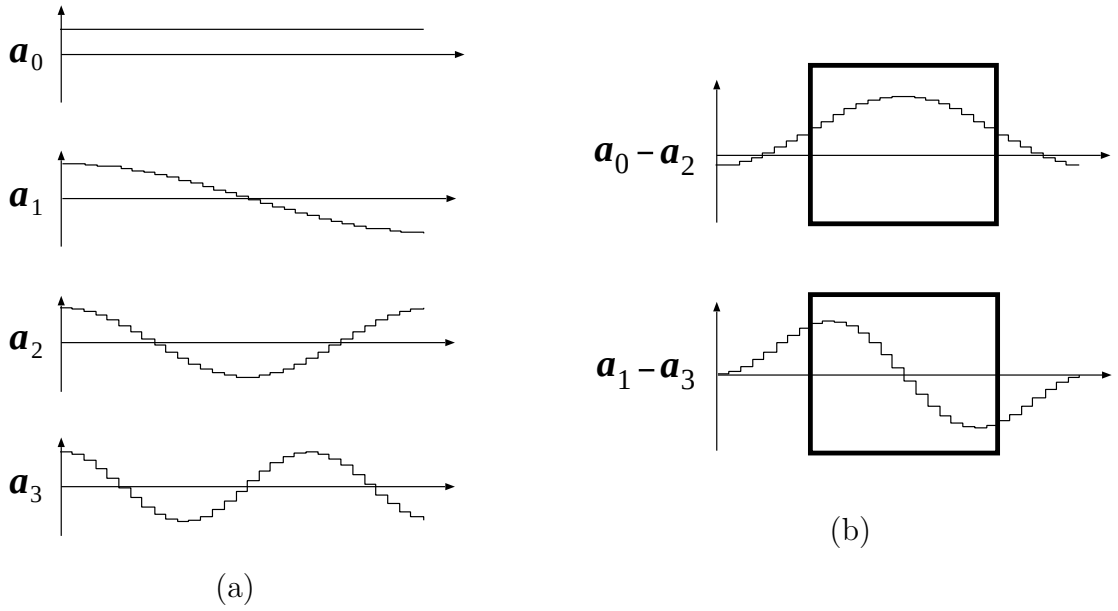


図 3.1　一次元 DCT 基底ベクトルの低周波成分とその加法特性

Fig. 3.1　Low frequency components of 1D-DCT basic vectors and theiraddition property.

図 3.1(a) に $N = 32$ の場合における 4 個の基底ベクトル Ba_0 から Ba_3 を示す.

特別に選出した 2 個の基底ベクトルが互いに作用し合うと，その波形の中心部分の振幅が大幅に増加する．例えば，$\boldsymbol{a}_0 - \boldsymbol{a}_2$ を演算すると，その結果は図 3.1(b) のようになる．図 3.1(b) の太線で示された領域の内側ではその振幅は増加しており，二つの波がお互いに強め合っている．その反面，外側では二つの波がお互いに打ち消し合っている．ここで重要な点は，内側の波形はある基底ベクトルの 2 分の 1 の波形の成分を多く含むことである．例えば，各 DCT 係数の低周波成分にある値 T を与えたときの信号成分は,

$$f_{32}(x) = \begin{cases} \dfrac{\sqrt{2}}{8}T & : F_{32}(0) \\ \dfrac{T}{4}\cos\left\{\dfrac{2x+1}{64}\pi\right\} & : F_{32}(1) \\ \dfrac{T}{4}\cos\left\{\dfrac{2x+1}{32}\pi\right\} & : F_{32}(2) \\ \dfrac{T}{4}\cos\left\{\dfrac{3(2x+1)}{64}\pi\right\} & : F_{32}(3) \end{cases} \tag{3.4}$$

で与えられる．$F_{32}(0) = T$，$F_{32}(2) = -T$ とした場合，次に示す信号が得られる．

$$f_{32}(x) = \frac{\sqrt{2}}{8}T - \frac{T}{4}\cos\left\{\frac{2x+1}{32}\pi\right\} \tag{3.5}$$

この信号の中心部分 $(8 \leq x < 24)$ の成分は，$x' = x - 8$, $(0 \leq x' < 16)$ とおくと，

$$f_{16}(x') = \frac{\sqrt{2}}{8}T - \frac{T}{4}\cos\left\{\frac{2x'+17}{32}\pi\right\} \tag{3.6}$$

で定義され，その DCT 係数 $F_{16}(0)$ は，

$$\begin{aligned} F_{16}(0) &= \frac{1}{4}\sum_{x'=0}^{15} f_{16}(x'), \\ &= \frac{\sqrt{2}}{2}T - \frac{T}{16}\sum_{x'=0}^{15}\cos\left\{\frac{2x'+17}{32}\pi\right\}, \\ &\simeq 1.34T. \end{aligned} \tag{3.7}$$

となる．この際，他の DCT 係数の値は計算すると小さな値に抑えられることが分かる．同様に $F_{32}(1) = T$，$F_{32}(3) = -T$ とした場合，

$$f_{16}(x') = \frac{T}{4}\cos\left\{\frac{2x'+17}{64}\pi\right\} - \frac{T}{4}\cos\left\{\frac{3(2x'+17)}{64}\pi\right\}, \tag{3.8}$$

$$F_{16}(1) \simeq 1.19T, \tag{3.9}$$

となる．故に $\boldsymbol{a}_0 - \boldsymbol{a}_2$ の波形の場合，内側の波形は $\boldsymbol{a}_0/2$ の成分を，$\boldsymbol{a}_1 - \boldsymbol{a}_3$ の波形では $\boldsymbol{a}_1/2$ の成分を多く含む．また，これらの重ね合わせた波の両端の振幅は零に近いため，隣接するブロックにおいて不連続点が生じにくいといった特徴を持つ．

この特徴は，二次元に拡張した場合にも確認される．ただし，一次元の場合とは異なり，4 個の DCT 基底画像の間で演算を行うものとする．図 3.2(a) に二次元 DCT(32×32) の低周波成分である 16 個の基底画像を示す．特別に選出した 4 個の基底画像を加算すると，図 3.2(b) のような特徴を持つ模様がブロックに現れる．注目すべき点は，斜線で囲まれた領域の振幅が大幅に増加しており，その外側では振幅が零付近に抑えられているところである．また，その斜線で囲まれた領域の模様は，ある基底画像の 4 分の 1 の成分を多く含む．ここで，一次元の場合と同様にその変化を定量的に表すために，$f_N(x, y)$ を $N \times N$ 個の画素から成るブロックとし，その DCT 係数を $F_N(X, Y)$ とする．このとき，

$$\begin{aligned} F_{32}(0,0) &= \quad T, \\ F_{32}(0,2) &= -T, \\ F_{32}(2,0) &= -T, \\ F_{32}(2,2) &= \quad T, \end{aligned} \tag{3.10}$$

とした場合に得られるブロック $f_{32}(x,y)$ はそれぞれ以下のように表すことができる．

$$f_{32}(x,y) = \begin{cases} \dfrac{\sqrt{2}}{8}T & : F_{32}(0,0) \\ \dfrac{\sqrt{2}T}{32}\cos\left\{\dfrac{2x+1}{32}\pi\right\} & : F_{32}(0,2) \\ \dfrac{\sqrt{2}T}{32}\cos\left\{\dfrac{2y+1}{32}\pi\right\} & : F_{32}(2,0) \\ \dfrac{T}{16}\cos\left\{\dfrac{2x+1}{32}\pi\right\}\cos\left\{\dfrac{2y+1}{32}\pi\right\} & : F_{32}(2,2) \end{cases} \tag{3.11}$$

これら 4 成分を重ね合わせると，

$$\begin{aligned} f_{32}(x,y) &= \frac{\sqrt{2}}{8}T - \frac{\sqrt{2}T}{32}\cos\left\{\frac{2x+1}{32}\pi\right\} \\ &\quad -\frac{\sqrt{2}T}{32}\cos\left\{\frac{2y+1}{32}\pi\right\} + \frac{T}{16}\cos\left\{\frac{2x+1}{32}\pi\right\}\cos\left\{\frac{2y+1}{32}\pi\right\} \end{aligned} \tag{3.12}$$

となり，このときの中心部分 $(8 \le x, y < 24)$ における DCT 係数は，

$$\begin{aligned} f_{16}(x',y') &= \frac{\sqrt{2}}{8}T - \frac{\sqrt{2}T}{32}\cos\left\{\frac{2x'+17}{32}\pi\right\} \\ &\quad -\frac{\sqrt{2}T}{32}\cos\left\{\frac{2y'+17}{32}\pi\right\} + \frac{T}{16}\cos\left\{\frac{2x'+17}{32}\pi\right\}\cos\left\{\frac{2y'+17}{32}\pi\right\}, \end{aligned} \tag{3.13}$$

$$F_{16}(0,0) \simeq 1.81T \tag{3.14}$$

となる．また，他の DCT 係数は小さい値に抑えられる．同様に，$F_{32}(0,1) = T$, $F_{32}(0,3) = -T$, $F_{32}(2,1) = -T$, $F_{32}(2,3)) = T$ の場合，

$$F_{16}(0,1) \simeq 1.60T, \tag{3.15}$$

となり，$F_{32}(1,0) = T$, $F_{32}(1,2) = -T$, $F_{32}(3,0) = -T$, $F_{32}(3,2) = T$ の場合，

$$F_{16}(1,0) \simeq 1.60T, \tag{3.16}$$

$F_{32}(1,1) = T$, $F_{32}(1,3) = -T$, $F_{32}(3,1) = -T$, $F_{32}(3,3) = T$ の場合，

$$F_{16}(1,1) \simeq 1.41T, \tag{3.17}$$

となる．故に，32×32 画素のブロックの 4 係数に与えたエネルギー T は，逆変換して得られるブロックの 16×16 画素から成るサブブロックの 1 係数に集中することが分かる．提案手法では，以上の結果を巧みに使って，電子透かしの埋め込み，検出を行なう．この結果を図 3.2 に示す基底画像を用いて説明する．図 3.2(b) に示す 4 個の模様は，

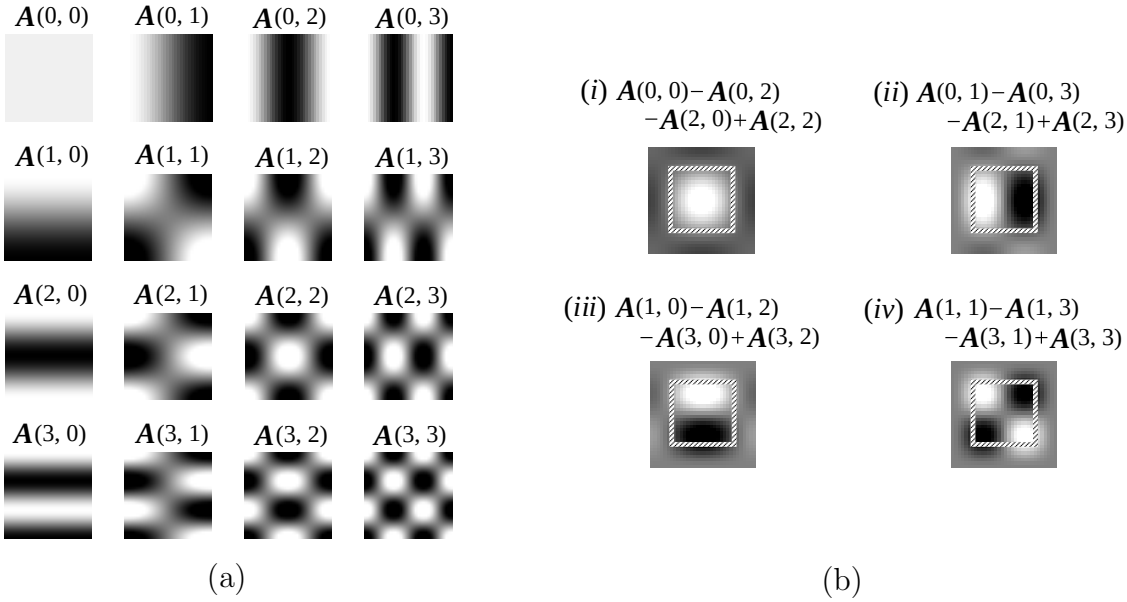


図 3.2　二次元 DCT 基底画像の低周波成分とその加法特性

Fig. 3.2　Low frequency components of 2D-DCT basic matrices and their addition property.

$$
\begin{aligned}
(i) \quad & \boldsymbol{A}(0,0) - \boldsymbol{A}(0,2) - \boldsymbol{A}(2,0) + \boldsymbol{A}(2,2) \quad : \ \tfrac{1}{4}\boldsymbol{A}(0,0) \\
(ii) \quad & \boldsymbol{A}(0,1) - \boldsymbol{A}(0,3) - \boldsymbol{A}(2,1) + \boldsymbol{A}(2,3) \quad : \ \tfrac{1}{4}\boldsymbol{A}(0,1) \\
(iii) \quad & \boldsymbol{A}(1,0) - \boldsymbol{A}(1,2) - \boldsymbol{A}(3,0) + \boldsymbol{A}(3,2) \quad : \ \tfrac{1}{4}\boldsymbol{A}(1,0) \\
(iv) \quad & \boldsymbol{A}(1,1) - \boldsymbol{A}(1,3) - \boldsymbol{A}(3,1) + \boldsymbol{A}(3,3) \quad : \ \tfrac{1}{4}\boldsymbol{A}(1,1)
\end{aligned}
$$

の成分をその斜線で囲まれる領域に持つ．ここで，各ブロックの境界部分ではその振幅が零付近に抑えられるため，低周波成分へ透かしを埋め込む際に問題となるブロック歪みが生じにくい．

3.3　DCT の加法特性に基づく埋め込み

前節で述べた特徴を利用して，透かしの情報ビットを 32×32 画素から成るブロックに埋め込み，そのブロック中の 16×16 画素から成るサブブロックを用いて検出する．その手順は，まず 32×32 画素のブロックに DCT を行い，特別に選出した 4 個の DCT 係数に透かし情報を埋め込む．埋め込み後，IDCT を行うことにより透かし情報は画像全体に拡散される．このブロック中にある 16×16 画素のサブブロックに DCT を行うと，拡散された透かし情報はある特定の係数に集中する．この特性を利用して透かし情報を検出する．

透かし情報を埋め込む DCT 係数は，図 3.2(b) において特別な加法特性を示す 4 個の基底画

像に相当する係数である．また，同図に示されているように各パターンに対応する検出用の基底画像があり，それに相当する係数から透かし情報は検出される．表3.1 に各パターンを形成する埋め込みのための 4 係数と，その検出のための係数を示す．ただし，各セット $(i), (\ddot{u}), (\ddot{\ddot{m}}), (\dot{w})$ はパターンを示しており，(p_1, p_2, p_3, p_4) が埋め込み係数，P が検出係数を示す．

表 3.1　埋め込み，検出のための DCT 係数

Table 3.1　DCT coefficients used for embedding and extracting.

set	埋め込み				検出
	p_1	p_2	p_3	p_4	P
i	$F_{32}(0,0)$	$F_{32}(0,2)$	$F_{32}(2,0)$	$F_{32}(2,2)$	$F_{16}(0,0)$
$\ddot{u}$	$F_{32}(0,1)$	$F_{32}(0,3)$	$F_{32}(2,1)$	$F_{32}(2,3)$	$F_{16}(0,1)$
$\ddot{\ddot{m}}$	$F_{32}(1,0)$	$F_{32}(1,2)$	$F_{32}(3,0)$	$F_{32}(3,2)$	$F_{16}(1,0)$
$\dot{w}$	$F_{32}(1,1)$	$F_{32}(1,3)$	$F_{32}(3,1)$	$F_{32}(3,3)$	$F_{16}(1,1)$

検出係数 P を $F_{16}(x,y)$ とすると，埋め込み係数はそれぞれ

$$\begin{aligned} p_1 &= F_{32}(x,y), \\ p_2 &= F_{32}(x,y+2), \\ p_3 &= F_{32}(x+2,y), \\ p_4 &= F_{32}(x+2,y+2), \end{aligned} \tag{3.18}$$

と表される．ある値 α を p_1, p_4 に加算し，p_2, p_3 から減算することにより P の値を β だけ増加させることができる．この α と β は，式 (3.14)(3.15)(3.16)(3.17) に示した関係を満足するが，ディジタル画像のため変換の際に丸め誤差が生じ，完全にはこれらの関係式は成り立たない．

埋め込み強度を T として，以下の操作により画像 I に透かし情報$\boldsymbol{w} = (w_0, w_1, \cdots, w_{n-1})$, $w_t \in \{0,1\}$ を埋め込む．

Step 1. 画像 I を RGB 表示系から YC_rC_b 表示系に変換する．その輝度成分 Y を 32×32 画素のブロックに分割し，DCT を行う．

Step 2. 各ブロックにおいて，秘密鍵を用いて表 3.1 のセットを 1 個選択する．

Step 3. t 番目のブロックに透かし情報ビット w_t を次のように埋め込む．

もし $w_t = 0$ ならば，

$$\begin{aligned} p_1 &= p_1 + T, \\ p_2 &= p_2 - T, \\ p_3 &= p_3 - T, \\ p_4 &= p_4 + T. \end{aligned} \tag{3.19}$$

$w_t = 1$ ならば,

$$\begin{aligned} p_1 &= p_1 - T, \\ p_2 &= p_2 + T, \\ p_3 &= p_3 + T, \\ p_4 &= p_4 - T. \end{aligned} \tag{3.20}$$

Step 4. 各ブロックに IDCT を行い，YC_rC_b 表示系から元の RGB 表示系に変換して埋め込み画像 I' を得る．

3.4 DCT の加法特性に基づく抽出

DCT 係数間の加法特性に基づいて埋め込まれた透かし信号は，埋め込みに用いたブロックの中のサブブロックから抽出することが可能である．検出精度だけで考えるならば元のブロックから抽出する方が良いかもしれないが，計算量まで考慮するならば，小さなサブブロックの方が望ましい．また，後に述べる量子化方式へ拡張する場合には，サブブロックを用いる必要がある．更に，幾何学的な歪みを考慮して，透かしを正しく抽出する前に同期回復を行う．

3.4.1 探索プロトコル

透かし情報が埋め込まれているブロックは，攻撃によって平行移動されたり，回転される可能性がある．提案方式では，ブロックには直交変換を用いて透かし情報を埋め込むため，直交軸の同期が保たれなければ透かし情報を正しく抽出できなくなる．これを防止するために，透かし情報の検出の前に各ブロックの同期回復を行う必要がある．そこで同期回復のために，元のブロックを用いて平行移動された位置と回転された形を探索し，その座標系を回復する操作を行う．ここで，不正コピーは埋め込み画像そのもの，もしくはそれに攻撃を加えたものであるため，原画像よりも埋め込み画像のブロックを用いる方が効率的である．

まず各パラメータを以下のように設定する．

B : 32×32 画素の埋め込みブロック.

L : ブロック B 中の 16×16 画素の検出サブブロック.

d : 探索距離.

K : $(16 + 2d) \times (16 + 2d)$ 画素の探索範囲ブロック.

T_j : 回転により歪ませたブロック L の歪み候補 $(0 \leq j \leq 12)$.

ただし，すべて YC_rC_b 表示系の輝度成分 Y とする．各パラメータは図 3.3，図 3.4 に示している．透かし情報は，ブロック B に埋め込まれており，サブブロック L から検出される．このと

き，探索は探索範囲 K 内のブロック L が各平行移動及び回転された各ブロックと埋め込み画像のブロック L' との誤差 MSE(Mean Square Error) を計算し，その値が最小となるものを元の透かしが埋め込まれたブロックと推定する．ここで，透かし情報は B の 4 係数 p_1, p_2, p_3, p_4 に埋め込まれているため，直接これらの係数から検出する方が良い結果が得られるように思われる．しかし，B が幾何学変換により受ける影響が L に比べて大きいため，同期回復の操作に莫大な計算量が必要となってしまう．L の場合，少ない計算量で同期回復ができるだけでなく，微小な拡大縮小操作により透かし情報が深刻な影響を受けにくい．このことは 3.6 節で説明する．それゆえ，提案方式では L から透かし情報を検出している．

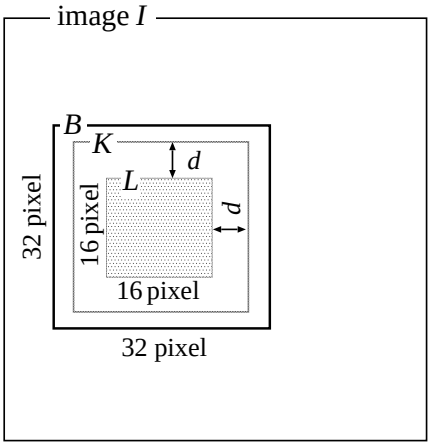


図 3.3　探索範囲
Fig. 3.3　Searching domain.

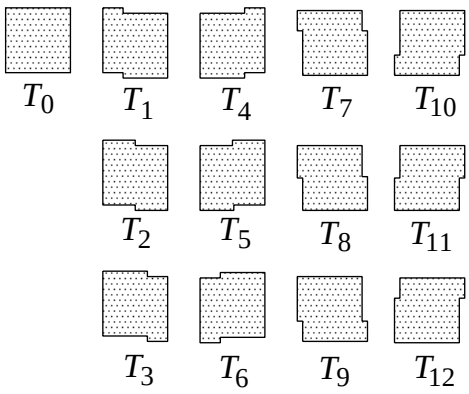


図 3.4　13 個の歪み候補
Fig. 3.4　The 13 candidates of rotated block.

I^* を攻撃を受けた画像として，32×32 画素のブロックに分割したものを B^* とする．このとき，各ブロック B^* に対して探索プロトコルが適用され，その中から L' に相当するブロックを検出する．以下にその手順を示す．

Step 1. ブロック B^* において次の操作を行う．

⟨1⟩ 探索範囲ブロック K^* の左上部から歪みパターン T_0 に相当する部分を抜き出し，L' との MSE を計算する．その MSE の値と抜き出したブロックを保存する．

⟨2⟩ 前回の操作から，1 画素平行移動した位置より抜き出したブロックの MSE を計算し，保存されている値より小さければ MSE とブロックを更新する．

⟨3⟩ 探索範囲ブロック K^* 内で取りうるすべてのブロックに対して操作 ⟨2⟩ を行う．

Step 2. Step 1 を各歪みパターンの候補 T_j において繰り返し行う．ただし，K^* から抜き出されたブロックは，正方形の形に修正してから MSE を計算する．また，操作 ⟨1⟩ では MSE

の値が保存されている値より小さければその値とブロックを更新する．

Step 3. 最終的に保存されているブロック $\hat{L}^*$ を出力する．

3.4.2 サブブロックからの透かし抽出

この節では，探索プロトコルにより同期を回復したブロック $\hat{L}^*$ から透かし情報を検出する手順を示す．透かし情報の抽出には原画像が必要であり，DCT 係数の差分の正負により埋め込み情報の各ビットを判断する．透かし情報の検出は，t 番目のブロックにおいて以下のように行われる．

Step 1. 探索プロトコルの出力ブロック $\hat{L}^*$ と原画像から得られるサブブロック L にそれぞれ DCT を行う．

Step 2. 表 3.1 を用いて秘密鍵により検出係数を選択する．

Step 3. $\hat{L}^*$ の係数から L の係数を減算する．

Step 4. その差が正ならば $w_t^* = 0$，負ならば $w_t^* = 1$ とみなす．

3.5 量子化法への拡張

電子透かしの性質として，透かし情報の検出に原画像を必要としない方が望ましい．前述の手法では，探索プロトコルに埋め込み画像を，検出に原画像を必要とする．そのため，埋め込み画像は検証の際に透かし情報と原画像を用いて作成すると考えても，検証者は少なくとも原画像と透かし情報を保持しなければならない．そこで，量子化法を用いる方式へと拡張させ，透かし情報の検出の際に，情報量の少ない原画像の一部であるテンプレートを用いる方式を提案する．以後，説明の都合のため，前述の手法を提案方式 I と呼び，この節で提案する手法を提案方式 II と呼ぶことにする．

3.5.1 同期化テンプレート

提案方式 I の探索プロトコルは，埋め込み画像 I' と攻撃を受けた画像 I^* との MSE を計算し，最小値を示すブロックを攻撃により歪まされたブロックと推定する方式であった．しかし，埋め込み画像は実際には画像全体が必要なわけではなく，サブブロック L' さえあればよい．その理由は，サブブロック L だけが探索プロトコルで用いられるからである．そこで，サブブロック L を同期化テンプレートとして用いる方式を提案する．また，透かし情報は画像

を表示変換した輝度成分に埋め込まれており，探索プロトコルも輝度成分を用いてMSEを計算する．ゆえに，必要な記憶容量は，サブブロックL'の輝度成分だけであり，原画像に比べて大幅に削減される．ここで，同期化テンプレートは画像の一部分であるため，JPEG圧縮により更に記憶容量の削減が期待できる．

探索プロトコルには，埋め込み画像から得られる同期化テンプレートさえあればよいが，提案方式Iでは透かし情報の検出に原画像が必要であった．そこで，この同期化テンプレートは透かし情報の検出そのものではなく，同期回復だけに適用し，透かし情報の埋め込みと検出には次節で提案する方式を採用する．

3.5.2 埋め込み検出操作

提案方式Iでは，サブブロックにおける特定のDCT係数を原画像との差分を計算し，その値の正負により埋め込み情報を検出するのに対し，提案方式ⅡではDCT係数を埋め込み強度mで量子化した値の偶奇により検出する．具体的には，以下の操作により透かし情報w_tを検出する．まず，探索プロトコルの出力ブロック$\hat{L}^*$にDCTを行う．次に秘密鍵により検出係数を表3.1から選択する．その係数を埋め込み強度Tで量子化し，その値が偶数ならば$w_t = 0$，奇数ならば$w_t = 1$とみなす．このように検出に関しては単純な操作だけでよいが，埋め込みに関しては提案方式Iよりも計算量がやや増加する．その埋め込み操作を以下に示す．

Step 1. 秘密鍵により検出係数であるサブブロックLのDCT係数を選択する．その値を$F_{16}(x, y)$とする．

Step 2. もし$w_t = 0$かつ$\mathrm{int}(F_{16}(x, y)/m)$が奇数ならば，

$$S = (\mathrm{int}(F_{16}(x, y)/T) + 1) \cdot T \tag{3.21}$$

もし$w_t = 1$かつ$\mathrm{int}(F_{16}(x, y)/T)$が偶数ならば，

$$S = (\mathrm{int}(F_{16}(x, y)/T) + 1) \cdot T \tag{3.22}$$

上記以外の場合，

$$S = \mathrm{int}(F_{16}(x, y)/T) \cdot T \tag{3.23}$$

として設定目標値Sを得る．ただし，$\mathrm{int}(*)$は整数化処理を表す．

Step 3. サブブロックLの係数$F_{16}(x, y)$が$(S - F_{16}(x, y))$だけ増加するように，埋め込み係数であるブロックBの4個のDCT係数を変化させる．

Step 3 では，ある値 α を p_1, p_4 に加算し，p_2, p_3 から減算することにより P の値を $(S - F_{16}(x, y))$ だけ増加させる．しかし，埋め込み係数と検出係数の間に成立する関係は，完全に線形の関係ではない．それゆえ，設定目標値が決まったとしても，実際に設定するにはやや複雑な計算が必要となる．今回筆者らは，次に示す方法を用いて設定した．まず式(3.14)(3.15)(3.16)(3.17)の関係を使って T を設定し，ブロックの DCT 係数に加算する．次にブロックに IDCT を行ない，サブブロックの DCT 係数を算出して S との差分を計算する．その差分が 1 未満になるように再度同じ操作を行なう．

3.6 埋め込みにより生じる影響

3.6.1 画質劣化

電子透かし技術を評価する上で，画質劣化は重要な要素であり，また攻撃に対する耐性とトレードオフの関係にある．たとえ攻撃に対して強い耐性を持つとしても，画像の品質が著しく劣化しては実用的とはいえない．例えば，画像の低周波成分に埋め込まれた信号は攻撃の影響を受けにくいが，ブロック歪みが生じる可能性がある．この節では，低周波成分を変化させることにより生じる影響を従来方式と提案方式の場合において比較する．

まず従来方式として，DCT 係数の低周波成分である $F_{16}(1, 0)$ の値を $+50$ 変化させた結果を図 3.5 に示す．次に提案方式 I において，サブブロックの DCT 係数 $F_{16}(1, 0)$ の値が $+50$ 変化するように，ブロック B の DCT 係数である $F_{32}(1, 0)$ と $F_{32}(3, 2)$ の値を $+30$，$F_{32}(1, 2)$ と $F_{32}(3, 0)$ の値を -30 変化させる．図 3.6 はその結果を示している．

二つの図を比べると，明らかに歪みの形状が違うことが分かる．図 3.5 にはブロック状に歪みが生じており，そのため透かし情報が埋め込まれていることを知覚されやすい．ゆえに，単純に低周波成分を変化させる埋め込み方法では，画質劣化が顕著に現れるため有効ではない．これと対照的に，提案方式 I では緩やかな曲線を描いた歪みが生じており，サブブロックの境目に急激な変化が生じない．つまり，提案方式 I のように DCT 係数間の特性を活かした埋め込みでは，大幅な画質劣化を伴わない．更に，次のような特性を有する．

1. 緩やかな曲線状の歪みのため，エッジ検出操作などにより透かし情報の存在を確認することは極めて困難である．

2. 各種フィルタリングにより埋め込まれた透かし情報を取り除かれる可能性は極めて低い．

3. 微少な拡大縮小操作では埋め込みによる歪みの形状は深刻な影響を受けない．

ここで，3 番目の特性が実現できるのは，この歪みの形状を微少に拡大縮小した場合にも，同じような形状が得られるからである．更に，次節で示すエネルギー集中特性も大幅に変化し

ない.

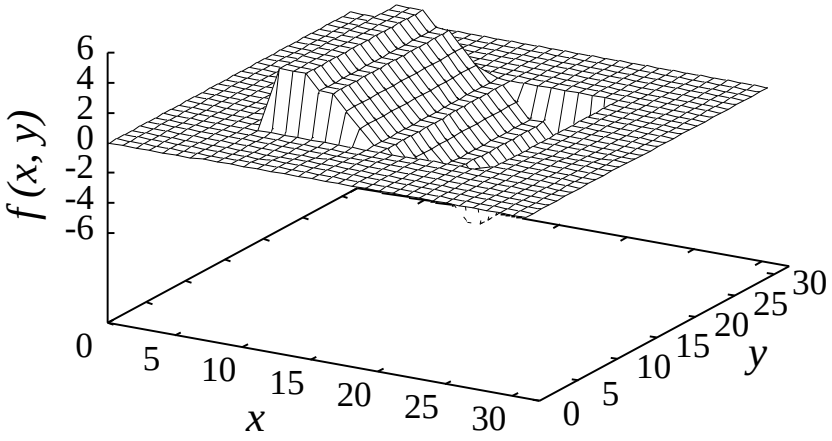


図 3.5　ブロック歪み

Fig. 3.5　Blocking effects.

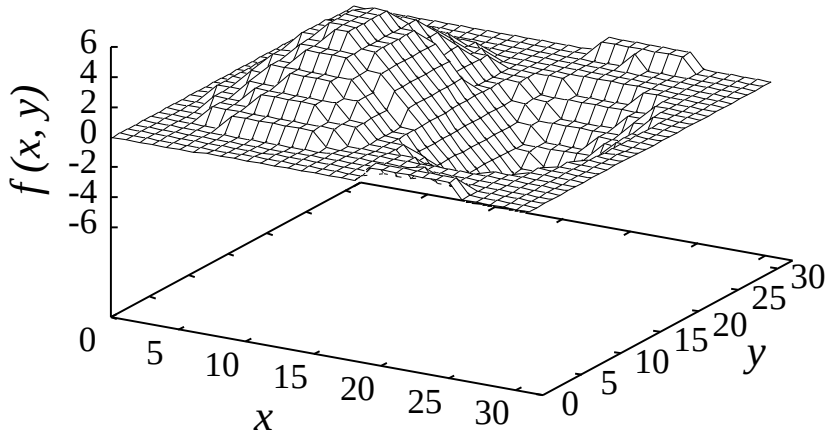


図 3.6　提案方式 I の歪み

Fig. 3.6　Distortion of the proposed scheme I.

3.6.2　エネルギーの集中

32×32 画素のブロックの DCT 係数を 4 個変化させることにより埋め込まれた透かし情報は，16×16 画素のサブブロックの特定の DCT 係数から検出される．実際に図 3.6 に示すブロックのサブブロックに DCT を施して得られた DCT 係数を図 3.7 に示す．図 3.7 から明らかなように，分散されたエネルギーは DCT 係数 $F_{16}(1,0)$ のみに集中している．他の係数では多少エネルギーを持っているが，$F_{16}(1,0)$ に比べてごく僅かである．

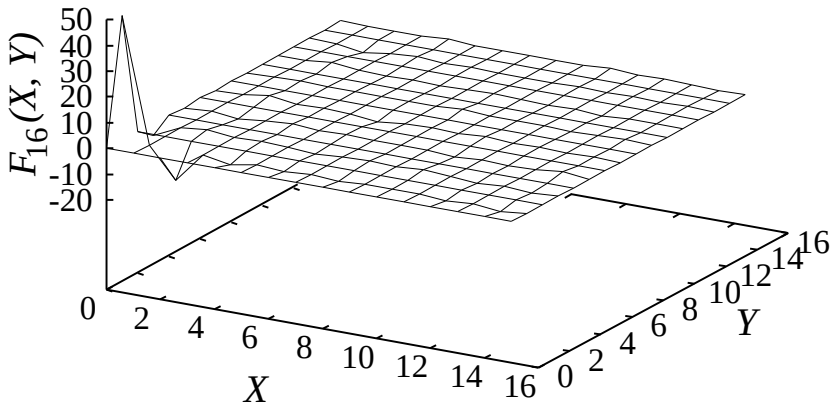


図 3.7　エネルギーの集中

Fig. 3.7　Energy concentration.

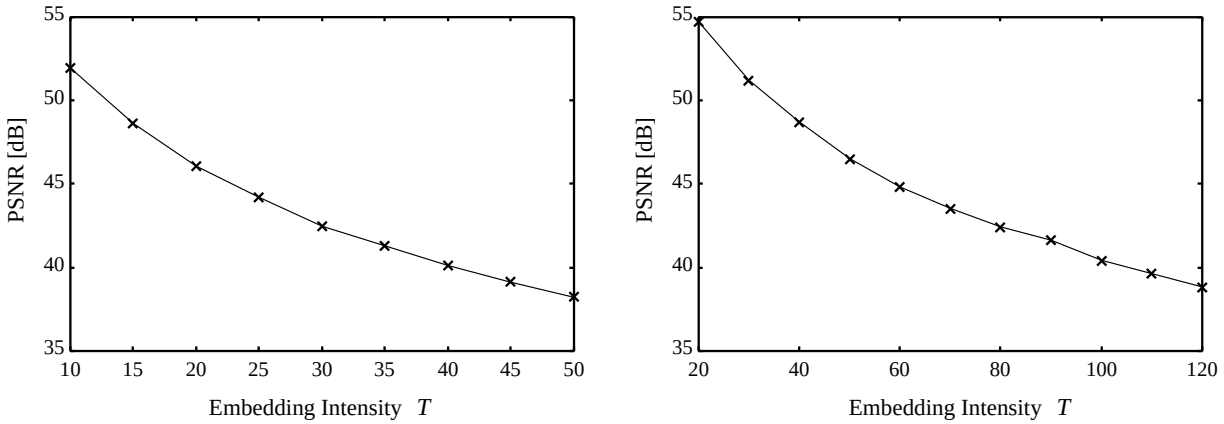
3.7　計算機シミュレーション

3.7.1　シミュレーション条件

今回シミュレーションには，原画像として 256 × 256 画素，RGB 各 8 ビットの画像 “lena”，“girl”，“baboon”，“peppers”，“f16” を用いる．透かし情報に 64 ビットの乱数系列を用いて，10^4 回異なる系列を埋め込み，画質劣化と攻撃に対する耐性を調べる．

3.7.2　画質評価

提案方式の画質劣化を調べるために画像 “lena” を用いて，埋め込み強度とその PSNR の関係を調べた．提案方式 I の結果を図 3.8(a) に，提案方式 II の結果を図 3.8(b) に示す．これらの図より，埋め込み強度が提案方式 I では $T = 50$，提案方式 II では $T = 120$ でも依然として高い品質を維持している．しかし，画像の平坦な部分では埋め込みによる歪みが知覚されやすいため，たとえ PSNR の値が高くても実用に耐えない場合がある．本論文では以上のような特徴を考慮して，埋め込み強度を提案方式 I では $15 \leq T \leq 30$，提案方式 II では $60 \leq T \leq 80$ の範囲に設定し，シミュレーションを行う．図 3.9 に示す原画像 “lena” に透かし情報を埋め込み，得られた画像を図 3.10(a) (提案方式 I)，図 3.10(b) (提案方式 II) に示す．



(a) Proposed scheme I　　(b) Proposed scheme II

図 3.8　画質の劣化

Fig. 3.8　The degradation of image quality.

3.7.3　探索範囲

探索プロトコルではブロックの同期を回復するために，埋め込み画像を用いて MSE を計算し，最小値を取るブロックを推定する．その探索は探索範囲ブロック K の中で行われ，その大きさは $(16+2d)\times(16+2d)$ である．ただし，d は探索距離である．ここで，探索距離を大きく取れば広範囲にわたって探索できるが，同時に計算量も増加してしまう．また，探索範囲を小さく取れば計算量は少なくなるが，正しく探索が行われなくなる可能性がある．そこで，最適な探索範囲を求めるために探索距離 d をパラメータとして，StirMark 攻撃を受けた後の画像からの検出率を比較する．ここで，検出率とは誤りなく正しく透かし情報を検出できる割合であり [%] で表す．埋め込み強度を $T=20$ として，画像 “lena” を用いた場合の結果を図 3.11 に，他の画像を用いた場合の結果を図 3.12 に示す．

図 3.11，3.12 より，探索距離が $d\geq 6$ の場合，検出率特性の改善は余り見られない．ゆえに，ブロックは探索距離が $d=6$ の範囲内で平行移動や回転などの攻撃を受けると考えられる．よって以後のシミュレーションでは探索距離を $d=6$ と固定して，攻撃に対する耐性を調べる．

3.7.4　StirMark 攻撃に対する耐性 (提案方式 I)

5 種類の画像を用いて，StirMark 攻撃に対する耐性を調べる．StirMark 攻撃のツールは version3.1 であり，パラメータはデフォルト値を用いた．図 3.13 は，各埋め込み画像に StirMark 攻撃を施した後，透かし情報の検出を試みた結果である．

画像 “peppers” と “f16” は，攻撃により影響を受けやすいエッジを多く含むため，検出率が

図 3.9　原画像 “lena”

Fig. 3.9　Original image “lena”.

(a) Proposed scheme I,
PSNR = 42.5[dB], $T = 30$

(b) Proposed scheme Ⅱ,
PSNR = 42.8[dB], $T = 80$

図 3.10　埋め込み画像

Fig. 3.10　Watermarked images.

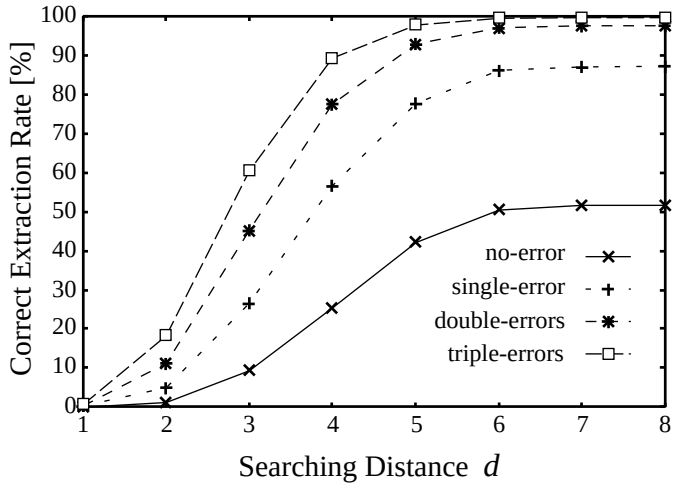


図 3.11　探索距離 d とその検出率特性 “lena”

Fig. 3.11　Correct extraction rate versus searching distance “lena.”

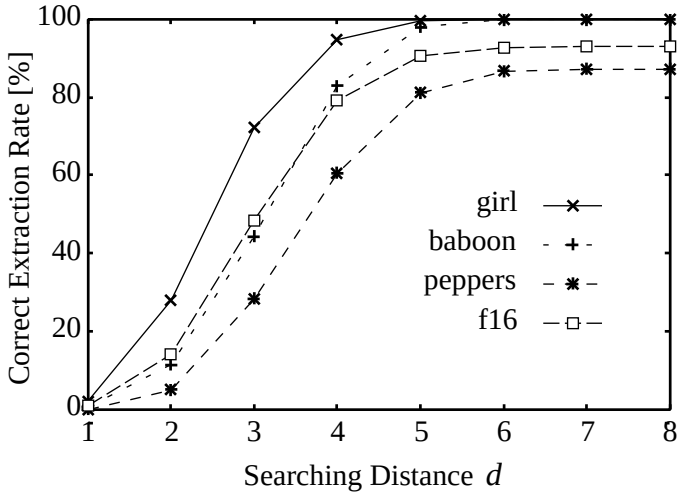


図 3.12　探索距離 d とその検出率特性 (三重誤り訂正)

Fig. 3.12　Correct extraction rate versus searching distance (triple errors correction).

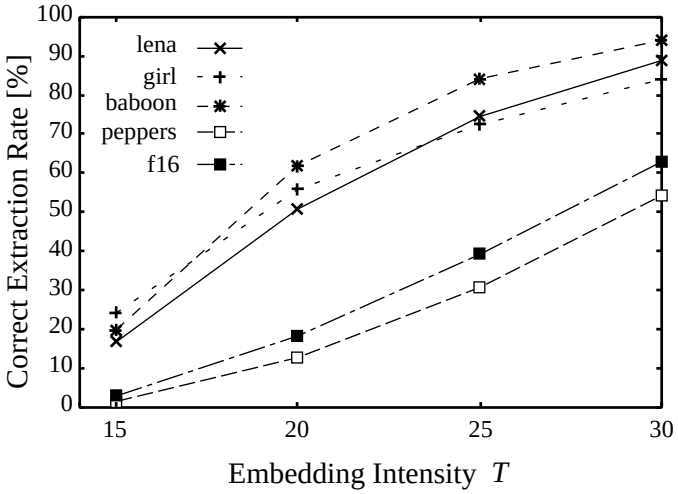


図 3.13　StirMark 攻撃に対する耐性 (提案方式 I)

Fig. 3.13　Tolerance for StirMark attack (Proposed scheme I).

他の画像に比べて低くなっている．また，埋め込み強度が低い場合には，透かし情報の検出率は低下している．しかし，検出された透かし情報の誤りビット数を調べると，数ビット程度であることが確認された．画像 “lena” に関して，各埋め込み強度に対する誤りビット数の分布を表 3.2 を示す．

表 3.2　誤りビット数の分布 “lena”

Table 3.2　Distribution of the number of errors “lena.”

T	0bit	1bit	2bits	3bits	else
15	16.7	31.3	27.9	15.2	9.0
20	50.9	34.8	11.7	2.3	0.4
25	74.7	21.7	3.2	0.3	0
30	88.9	10.5	0.6	0.1	0

この表 3.2 より明らかに誤りビット数は 64 ビット中その大半が 3ット以内に分布していることが分かる．特に，埋め込み強度が $T \geq 25$ の場合には，完全に 3 ビット以内に分布している．同様に他の画像に関しても，誤りビット数の分布を表 3.3 に示す．ただし，$T = 30$ と固定した場合である．

この表 3.3 から，エッジ部分を多く含み，攻撃に対して比較的耐性の低い画像 “peppers” と “f16” も同様に誤りビット数は 3 ビット以内に大半が分布していることが分かる．ゆえに，三重誤り訂正能力を持つ符号を用いれば，提案方式 I は攻撃に対して十分な耐性を持つ．ただし，符号長を最大 64 ビットと設定するため，透かし情報はそれよりも少ない情報量となる．

表 3.3　誤りビット数の分布 ($T = 30$)

Table 3.3　Distribution of the number of errors ($T = 30$).

image	0bit	1bit	2bits	3bits	else
girl	84.0	15.0	1.0	0	0
baboon	93.9	0.3	0	0	0
peppers	54.2	34.5	9.6	1.6	0.2
f16	63.0	29.8	6.4	0.8	0.1

3.7.5　同期化テンプレートの圧縮後のサイズ

同期化テンプレートは，カラー画像の輝度成分から成るサブブロック L' の集合を JPEG 圧縮した画像である．このテンプレートに JPEG 圧縮を施さなければ，提案方式 II の探索プロトコルは提案方式 I と同じ性能を示す．そこで，このテンプレートに JPEG 圧縮を施した場合の性能劣化を調べるため，提案方式 I の埋め込み検出操作により，JPEG 圧縮の画質のパラメータ，“quality” [%] の値をいろいろと変化させた場合の電子透かし情報の検出率を調べる．一例として画像 “lena” を用いた場合に誤り訂正ビット数をパラメー タとする quality に対する検

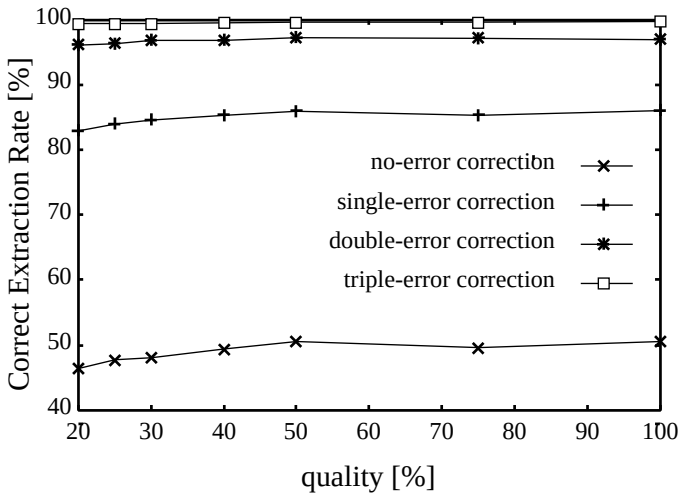


図 3.14　同期化テンプレートの圧縮と検出率の関係 “lena”

Fig. 3.14　Correct extraction rate versus quality for a synchronization template “lena.”

出率を図 3.14 に示している．この例から，同期化テンプレートに高圧縮を施しても，検出率はあまり変化しないことが分かる．また，他の画像の場合でも同様の結果を示すことがシミュレーションにより確認されている．

次に，圧縮をしたテンプレートのファイルサイズを表 3.4 に示す．原画像，若しくは埋め込み画像は，192[kB](256 × 256 画素，RGB 各 8 ビット) であるのに対して，圧縮したテンプレートのサイズは，極めて小さいことが確認された．例えば quality 25[%] の場合，そのサイズは平均で約 1/120 に圧縮される．以後のシミュレーションでは，quality パラメータの値を 25[%] と固定して同期化テンプレートを用いる．

表 3.4　同期化テンプレートの圧縮後のサイズ

Table 3.4　Compressed file size for a synchronization templete.

quality[%]	size[kB]				
	lena	girl	baboon	peppers	f16
20	1.4	1.2	2.0	1.4	1.5
25	1.5	1.2	2.3	1.5	1.6
30	1.7	1.3	2.6	1.7	1.7
40	1.9	1.5	3.2	1.9	2.0
50	2.1	1.7	3.6	2.2	2.3
75	3.1	2.4	4.2	3.0	3.3
100	12.1	10.3	17.5	12.5	12.4

3.7.6　StirMark 攻撃に対する耐性 (提案方式 Ⅱ)

提案方式 I の場合と同じ条件の下で，提案方式 Ⅱ を適用した場合の StirMark 攻撃に対する耐性を調べる．まず，各埋め込み画像に StirMark 攻撃を施した後，透かし情報の検出を試みた結果を図 3.15 に示す．提案方式 I の場合と同様に，画像 “peppers” と “f16” の検出率は低い結果となった．また，全体的に低い検出率となっている．しかし，誤りビット数が 3 ビット以内に抑えられていれば，誤り訂正符号を適用することで十分な耐性を維持できる．表 3.5 に画像 “lena” を用いた場合，表 3.6 に埋め込み強度を $T = 80$ と固定した場合の誤りビット数の分布結果を示す． これらの表から，誤りビット数は大半が 3 ビット以内に分布していることが確認された．ゆえに，誤り訂正能力 3 の誤り訂正符号を適用することにより StirMark 攻撃に高い耐性を持つ方式となる．ただし，符号化に際し冗長ビットを付加する必要があるため透かしの情報量は 64 ビットより少なくなる．

3.7.7　JPEG 圧縮に対する耐性

提案方式 I において，原画像 “lena” を用いて JPEG 圧縮に対する耐性を調べる．実験は，埋め込み画像を JPEG 圧縮した後に復元した画像から透かし情報の検出を試みるものである．図

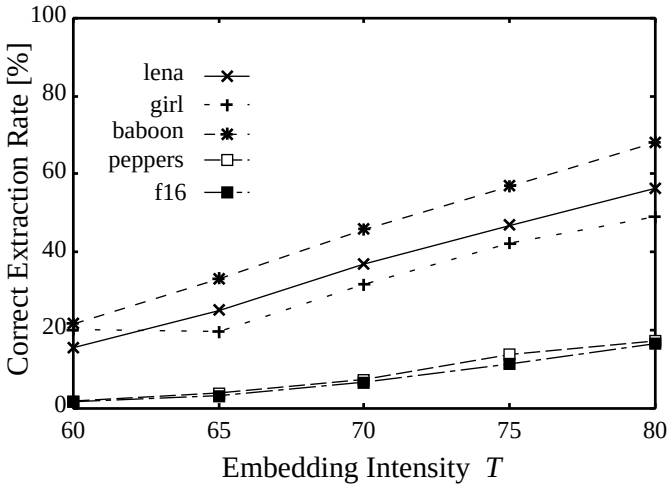


図 3.15　StirMark 攻撃に対する耐性 (提案方式 Ⅱ)

Fig. 3.15　Tolerance for StirMark attack (Proposed scheme Ⅱ).

表 3.5　誤りビット数の分布 “lena”

Table 3.5　Distribution of the number of errors “lena.”

T	0bit	1bit	2bits	3bits	else
60	15.6	30.9	28.3	16.3	8.9
65	25.0	36.8	24.2	10.4	3.7
70	37.0	38.1	18.3	5.3	1.3
75	46.9	36.5	13.2	2.9	0.5
80	56.4	33.4	8.5	1.5	0.2

表 3.6　誤りビット数の分布 ($T = 80$)

Table 3.6　Distribution of the number of errors (T=80).

image	0bit	1bit	2bits	3bits	else
girl	48.9	38.3	11.2	1.5	0.1
baboon	68.2	25.7	5.4	0.6	0.1
peppers	17.2	32.1	28.2	14.8	7.7
f16	16.5	32.3	28.6	14.9	7.7

3.16 は，JPEG の各圧縮品質パラメータ (quality[%]) の各値に対して透かし情報が 1 ビットの誤りもなく正しく検出される割合を示す．ここで，画質のパラメータ (quality) の値が低いほど画質は劣化し，25[%] 未満では画質の劣化が顕著に現れるため実用上は用いられることは極めて少ない．図 3.16 から，埋め込み強度が $T \geq 20$ の場合には高圧縮に対しても耐性を持つことが分かる．また，quality が 10[%] になると急激に検出率が低下している．しかし，圧縮による歪みが容認できる画質 (quality)25[%] を大きく割り込んでおり，JPEG の適用範囲外となるため耐性に関して事実上問題はない．したがって，提案方式 I は JPEG 圧縮に対して十分な耐性を持つ．また提案方式 II に関しても，図 3.17 に示してあるように同様の結果が得られる．

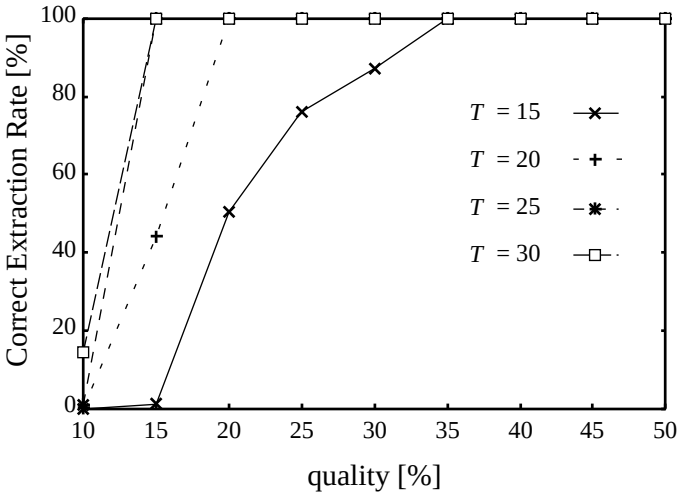


図 3.16　JPEG 圧縮に対する耐性 (提案方式 I)

Fig. 3.16　Tolerance for JPEG compression (Proposed scheme I).

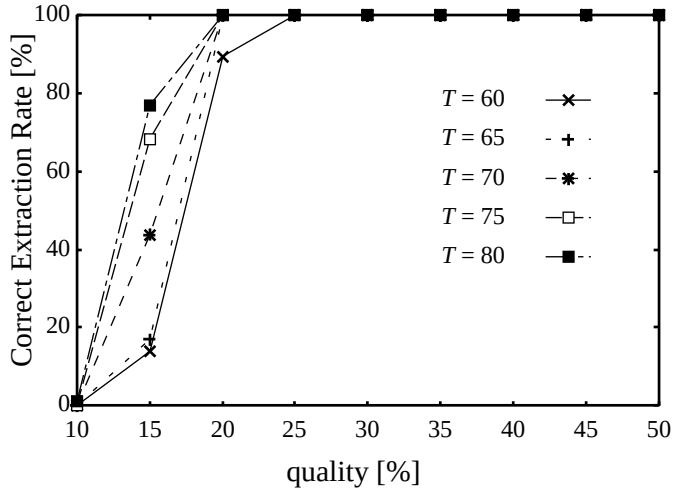


図 3.17　JPEG 圧縮に対する耐性 (提案方式 II)

Fig. 3.17　Tolerance for JPEG compression (Proposed scheme II).

3.7.8 考察

提案方式 I，Ⅱ共に画像によってその検出率が異なり，画像の特徴に依存して攻撃の耐性が変わることが分かる．一般に複雑な模様を表す繊細な画像は，各種の信号処理により変化を受けやすい．埋め込まれた透かし情報も例外ではなく，取り除かれる可能性は高くなる．しかし，複雑な模様は埋め込みにより生じた歪みを知覚されにくくするため，より振幅の大きな透かし信号を埋め込むことが可能である．つまり，画像 “peppers” や “f16” は埋め込み強度を更に上げたとしても，画質劣化は知覚されにくいために，攻撃に対する耐性を向上させることができる．したがって，画像の特徴に依存して埋め込み強度を設定することが望ましい．ただし，実際には各ブロック毎に特徴が異なるため，設定方法を改良した方が良い．このことは今後の課題である．

提案方式Ⅱでは同期化テンプレートを用いて探索プロトコルを適用している．この同期化テンプレートは原画像の一部分であり，データ圧縮も可能であるから，原画像に比べてファイルサイズを大幅に削減できる．また同期化テンプレートはブロック同期の回復後は，ブロックの DCT 係数の値の判別には関与しないため，同期化テンプレートを一種の秘密鍵とみなすことができる．したがって著作者は秘密鍵さえ保持しておれば，不正コピーを発見したときに著作権を主張することができる．

3.8 結言

本章では，DCT 係数間の加法特性を利用した新しい電子透かしの二つの方式を提案した．提案方式 I は原画像を用いる方式であり，提案方式Ⅱは原画像の一部分である同期化テンプレートを用いる方式である．それらの方式には次のような三つの特徴がある．まず最初に，透かし情報は DCT 係数間の加法特性を利用して，低周波成分である特定の 4 係数に埋め込まれる．その結果，埋め込み画像に生じる歪みが知覚されにくい形状となり，従来法で問題となっているブロック歪みが現れなくなった．次に，埋め込みを行ったブロック中のサブブロックから透かし情報は検出される．4 個の DCT 係数に与えられた透かし情報の分散エネルギーは，IDCT を行って埋め込み画像のブロックに変換し，そのブロック中のサブブロックに DCT を施すことにより，特定の周波数成分のみに集中できる．最後に，各種の攻撃により回転や平行移動などの変形を受けた画像を探索することにより，元の位置を復元してブロックの同期を回復することができる．

提案方式の攻撃に対する耐性を調べるために計算機シミュレーションを行った．その結果，JPEG による高圧縮処理画像や StirMark 攻撃を施した画像から埋め込まれた透かし情報を検出できることが確認された．また，誤り訂正符号を併用することにより，更なる耐性を持たせ

ることが可能となった．ただし，誤り訂正符号化により実際に透かし情報として埋め込まれる情報量は 64 ビットより少なくなる．

第4章　画像の局所情報に基づく電子透かし

4.1　緒言

画像の電子透かしには，輝度領域に埋め込む方式や周波数領域に埋め込む方式など，多種多様な方式が提案されている．電子透かしの埋め込みに対して求められる条件として，画質の劣化が知覚されにくいことと各種攻撃に対して耐性があることは重要である．前章では，人間の視覚特性に基づいて低周波成分の特定の成分を用いた．しかし，一般に画像はそれぞれ異なる特徴を持っており，その特徴に適した埋め込み手法を用いることが望ましい．例えば，複雑な模様を多く含む領域では，雑音が付加されたとしてもその影響は知覚されにくい．反対に，あまり変化のない領域，例えば背景などは少しの変化に対しても目立ってしまう．

本章では，画像全体の特徴だけでなく局所的な特徴に基づいて適応的に透かしを埋め込む手法を提案する．基本方式として，画像からいくつかのブロックをサンプリングして，4個のブロックごとにまとめて透かし情報の各2ビットを埋め込む．サンプリングする際に，その局所的なブロックの特徴を識別して，埋め込みに適したブロックだけを埋め込みに用いることで適応的な方式とする．意図的な改ざんに対する耐性を考慮して，サンプリングするブロックは秘密鍵に基づいて画像から不規則に選出されるようにする．透かし情報は，一部の中周波成分にスペクトル拡散させた信号成分を加えることで埋め込まれる．具体的には，4個のブロックをまとめたマクロブロックにウェーブレット変換を2回施し，その HL_2 成分と LH_2 成分にPN系列とDCTを用いたスペクトル拡散方式による埋め込みが行われる．その結果，埋め込まれた信号を信号処理技術を用いて取り除くことが困難になる．ただし，幾何学的な改変に対しては同期のずれを回復する必要が生じるため，前章で提案したテンプレートを用いた探索プロトコルを適用する．

4.2　ウェーブレット変換とスペクトル拡散を用いた埋め込み

画像の局所情報に基づいた透かしの埋め込みを述べる前に，基本となる埋め込み手法を述べる．その手法では，透かし情報は画像からサンプリングした複数のブロックに拡散させて埋め込まれる．従来法では，画像全体にウェーブレット変換を施して透かし情報の埋め込みが行われるが，この場合幾何学的な歪みに対して同期回復が難しい．そこで，前章で提案した探索プロトコルを有効に活用して，局所的にブロックを選出し，それらを複数まとめて処理して透かし情報を埋め込む．提案手法では，局所的に選出したブロックごとに同期回復処理が行えるため，幾何学的な歪みに対して，対策を施しやすい．

4.2.1 埋め込み

透かし情報 2 ビットを埋め込むために，サンプリングした 4 個のブロックを縦横 2 個ずつ並べたマクロブロックを作成する．この際，画像からサンプリングするブロックの大きさは，探索プロトコルを適用できるように 16×16 画素のブロックとする．

透かし情報を $w_t \in \{0, 1\}$ として，以下に，透かし情報 2 ビットを埋め込む操作の手順を示す．

Step 1. 秘密情報に基づいて 16×16 画素のブロックを画像から重複することなく 4 個選出する．それらを $A_i (1 \leq i \leq 4)$ とし，図 4.1 に示すようにマクロブロックを作る．

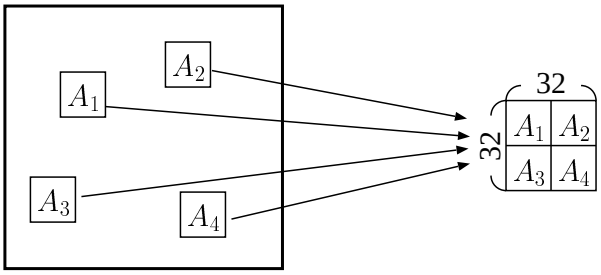


図 4.1　サンプリング
Fig. 4.1　Sampling from an image.

Step 2. マクロブロックにウェーブレット変換 (WT) を 2 回施し，第二階層の横方向の成分 LH_2 と縦方向の成分 HL_2 を取り出す．

Step 3. 秘密鍵である PN 系列を LH_2 と HL_2 に乗算し，そのスペクトル成分を得るために DCT を施す．

Step 4. 透かし情報の埋め込み強度 T を設定し，秘密情報に基づいて LH_2 と HL_2 のスペクトル成分の中からそれぞれ 1 成分を選出し，次に示す規則に従って埋め込みを行う．

- $w_t = 0$ の場合，特別なスペクトル成分の値を $+T$ だけ増加させる．
- $w_t = 1$ の場合，$-T$ だけ減少させる．

Step 5. スペクトル成分に逆 DCT を施し，PN 系列を再乗算することにより，透かし情報の各信号エネルギーが LH_2 と HL_2 のそれぞれに拡散される．更に，逆ウェーブレット変換 (IWT) を施すことでマクロブロック全体に透かし信号が拡散される．

Step.6. マクロブロックを構成する 4 個のブロックを元の画像のブロックと置き換えることで埋め込みを終える．

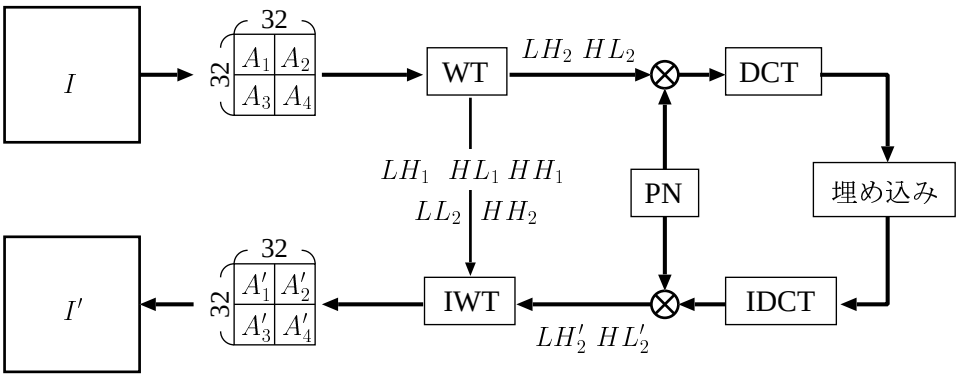


図 4.2　埋め込み操作の流れ

Fig. 4.2　Embedding process.

画像に 2 ビットの透かし情報を埋め込む手順の流れを図 4.2 に示す．以上の操作では，2 ビットの透かし情報を埋め込むことができ，この操作を繰り返すことにより，埋め込む情報量を増やすことが可能である．ただし，繰り返す際には，次のことに気をつけなければならない．

1. 選出する 4 個のブロックはすべて独立して選出され，重複してはならない．

2. 埋め込む情報量と画質の間にはトレードオフの関係がある．

この埋め込みでは，ブロックの選出位置，PN 系列，埋め込みに用いるスペクトル成分の位置が秘密情報となる．

4.2.2　検出

前章と同様に，透かし情報の検出の前に幾何学的な歪みの補正を行う．埋め込む透かし信号自体には幾何学的な歪みに耐性はないが，同期回復を各ブロックに対して行うことで，幾何学的な改変に対する耐性を向上できると考えられる．

透かしを検出する対象のブロックを A_i^* とし，探索プロトコルにより同期回復を行った後のブロックを $\hat{A}_i^*$ として検出操作を以下に示す．

Step 1. 4 個のブロック $\hat{A}_i^*$ からマクロブロックを作る．

Step 2. ウェーブレット変換を 2 回施し，その LH_2 成分と HL_2 成分に PN 系列を乗算した後に DCT を行う．

Step 3. 透かし信号の埋め込まれたスペクトル成分の値を元の値と比較して，その大小関係により透かし情報を判定する．

以上の操作では，2 ビットの情報を検出する操作であり，繰り返し行うことで埋め込まれた透かし情報すべてを検出することができる．

4.3　画像の局所的な特徴を利用した埋め込み

一般に，画像が多くの高周波成分を含むならば透かし情報の埋め込みにより生じる画質劣化は知覚されにくい．また，画質劣化と透かしの情報量はトレードオフの関係にあるので，埋め込み可能な情報量は画像の特徴に大きく依存している．しかしながら，一様な埋め込みでは画像の特徴を活かすことはできないため，適応的な埋め込み手法が求められている [28].

前節の方式を適応的な方式へと拡張するために，選出するブロックの特徴を考慮する．人間の視覚特性によると，複雑な模様やエッジを多く含む領域に付加された雑音は，平坦な領域に付加されたものと比べて知覚されにくい．そこで，前節の埋め込み手法において，複雑な模様やエッジを多く含むブロックだけを選出して埋め込みを行う．

複雑な模様やエッジを含むということは，そのブロック内での輝度値の分散が大きいといえる．しかし，単純にブロック全体の分散値の大きいものを判別すればよいとは限らない．例えば，横方向への変化は激しいが，縦方向の成分はほとんど変化しないようなブロックの場合，分散値は大きいけれど雑音成分は知覚されやすい．そこで，図 4.3 に示す 8 方向の分散値を求めて，偏りなく分散値の高いブロックを判別する．そして，あるしきい値以上の分散値を有するブロックだけが埋め込みに使用される．

透かし情報の埋め込み，検出操作は，前節で述べた方式を用いる．ここで，検出操作の際には探索プロトコルを適用するため，埋め込みに用いられたブロックだけを保存すればよい．ただし，選出したブロックの座標情報を保存しておく必要があることに注意しなければならない．

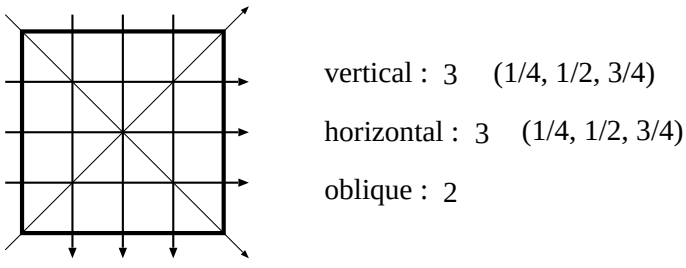


図 4.3　分散値を求める方向
Fig. 4.3　Directions of computing variances.

4.4 計算機シミュレーション結果

提案手法の有効性を調べるために計算機シミュレーションを行う．説明の都合上，4.2 節で述べた方式を提案方式 I とし，適応的な埋め込みに拡張したものを提案方式 II と呼ぶことにする．以下に示すシミュレーションでは，256×256 画素，RGB 各 8 ビットのカラー画像 “lena”, “girl”, “baboon”, “peppers” を用いる．また，透かし情報の埋め込み，検出操作は，画像を RGB 表示系から YC_rC_b 表示系に変換し得られた輝度成分に対して行う．

4.4.1 画質評価

透かし情報の埋め込みにより生じる画質劣化は，埋め込む情報量と埋め込み強度に依存する．ここでは，提案方式 I を用いて透かし情報を 72 ビットのランダムな系列として固定し，埋め込み強度 T を変化させて画質を調べる．図 4.4 に画像 “lena” に関する埋め込み強度と PSNR の関係を示す．透かし情報は，ウェーブレット変換して得られた LH_2 成分と HL_2 成分にスペクトル拡散して埋め込まれており，各スペクトルに $\pm T$ の振幅を持つエネルギーを与えている．そのため，PSNR の値は画像成分自体には依存しないで，埋め込み強度 T にのみ関係を持つ．ゆえに，他の画像に関しても同様の結果が得られた．

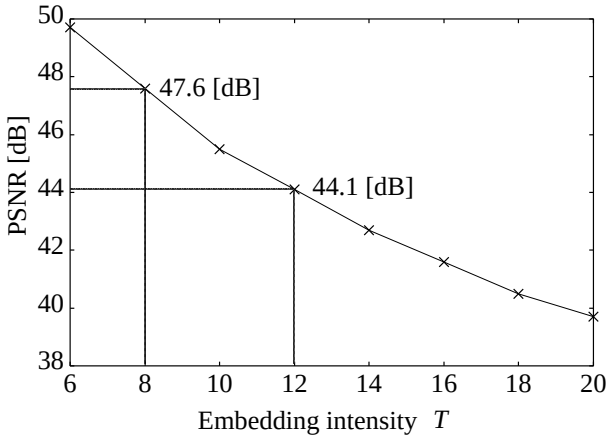


図 4.4　埋め込み強度と PSNR の関係
Fig. 4.4　PSNR versus embedding intensity.

攻撃に対する耐性を向上させるためには，埋め込み強度 T を大きくしなければならない．しかし，画質劣化と耐性はトレードオフの関係にあるため，埋め込みによる劣化が知覚されない範囲内で最大の埋め込み強度を設定する必要がある．以後のシミュレーションでは，この範囲として $8 \leq T \leq 12$ として耐性を調べることにする．PSNR の値だけで判断すれば，T の値は更に大きく設定可能であるが，平坦な領域での劣化が顕著になる恐れがあるため，この範囲内

に設定した．

提案方式Ⅱでは，平坦な領域への埋め込みを避けるため，埋め込み強度の値を大きく設定することができる．ただし，埋め込む透かし情報の情報量は，最大 72 ビットであり，選出するブロックの数によりそのビット数は変化する．72 ビットを埋め込むためにはブロックが 144 個必要であり，その中から分散値の大きさに依存させて埋め込みに用いるブロックを選出する．そのため，各画像ごとにその特性は異なり，埋め込み可能な情報量も異なる．ここで，各画像ごとにブロックの選出を判別する分散値のしきい値と埋め込み可能な情報量の関係を図 4.5 に示す．図 4.5 より，“baboon” は他の画像に比べて多くの情報を埋め込み可能であることが分かる．その理由としては，“baboon” には複雑な模様が多く含まれており，選出されるブロック内の分散値が比較的大きいためである．

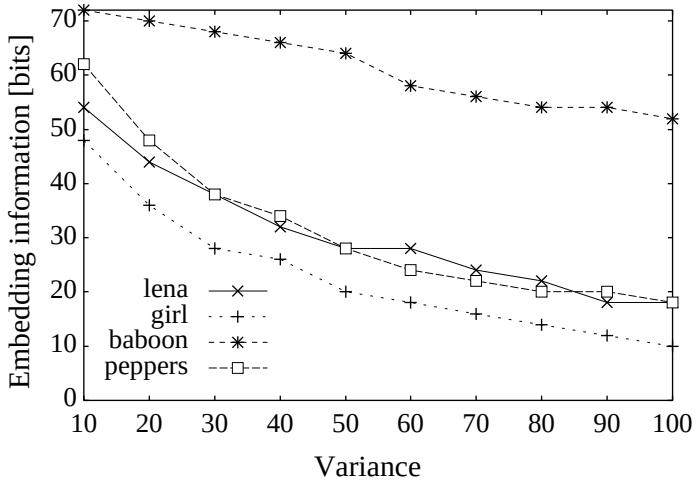


図 4.5　分散値に対する埋め込み可能な情報量

Fig. 4.5　The possible amount of embedding information.

埋め込みによる画質劣化を示すために，原画像 “lena” とその埋め込み画像を図 4.6 から図 4.9 に示す．ただし，図 4.7 と図 4.8 は提案方式Ⅰの埋め込み画像であり，それぞれ埋め込み強度 $T = 12$ と $T = 20$ の場合である．図 4.9 は提案方式Ⅱの画像であり，埋め込み強度 $T = 20$, 分散値のしきい値 50 である．図 4.7 と原画像を比較すると，視覚上その違いはほとんど確認できない程度である．図 4.8 の場合，平坦な領域では透かしの埋め込みにより生じた歪みが少し目立つようになっているが，適応的に埋め込み処理を施した図 4.9 では，視覚上の劣化はあまり確認されない．

図 4.6　原画像

Fig. 4.6　Original image.

図 4.7　埋め込み画像 ($T = 12$)

Fig. 4.7　Watermarked image ($T = 12$).

図 4.8　埋め込み画像 ($T = 20$)

Fig. 4.8　Watermarked image ($T = 20$).

図 4.9　埋め込み画像 ($T = 20$, 分散値 50)

Fig. 4.9　Watermarked image ($T = 20$, variance = 50).

4.4.2 StirMark 攻撃に対する耐性

電子透かしシステムの評価ツールである StirMark[12] を用いて，提案方式の攻撃に対する耐性評価を行う．評価手順として，まず，提案方式 I の埋め込みを各埋め込み強度 T に関して行い，その埋め込み画像に StirMark 攻撃を施す．そして，攻撃を受けた画像から埋め込んだ 72 ビットの情報を正しく検出できた割合を調べる．各画像に関して得られた結果を表 4.1 に示す．シミュレーション結果より，埋め込み強度 $T = 12$ の場合でさえ StirMark 攻撃に対する耐性は十分とはいえない．しかしながら，検出の誤りビット数を調べてみるとそれほど多くないことが分かる．画像 “lena” において誤りビット数の分布を図 4.10 に示す．また，埋め込み強度 $T = 12$ として，他の画像に関する誤りビット数の分布状況を表 4.2 にまとめる．これらの結果より，誤って検出されるビットの数は，せいぜい 3 ビット程度であることが分かる．ま

表 4.1　StirMark 攻撃に対する耐性

Table 4.1　Tolerance for StirMark.

T	lena [%]	girl [%]	baboon [%]	peppers [%]
8	37.1	66.8	14.9	37.4
10	70.5	87.4	47.8	69.1
12	88.4	95.3	75.7	86.6
⋮	⋮	⋮	⋮	⋮
20	99.8	99.8	99.3	99.5

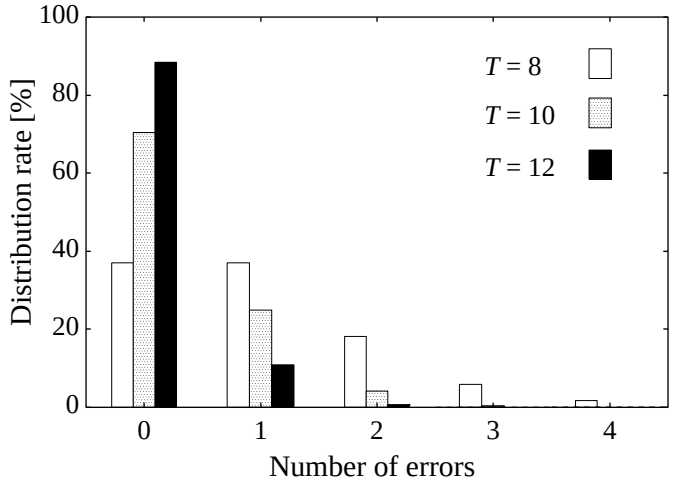


図 4.10　誤りビット数とその分布状況

Fig. 4.10　Distribution rate versus number of errors.

た，その分布は画像にはほとんど依存していない．ゆえに，誤り訂正符号を適切に用いれば，StirMark 攻撃に高い耐性を有する方式となる．

表 4.2　誤りビット数の分布状況 ($T = 12$)

Table 4.2　Error distribution rate ($T = 12$).

image	0bit [%]	1bit [%]	2bits [%]	3bits [%]
girl	95.3	4.6	0.2	0.0
baboon	75.7	20.8	3.1	0.4
peppers	86.6	12.5	0.9	0.0

表 4.1 には，埋め込み強度 $T = 20$ の場合の結果も示してある．埋め込み強度が $8 \leq T \leq 12$ の場合と比べて，非常に高い耐性を有することが分かる．ただし，この強度を使用する場合は提案方式Ⅱに限られるため，埋め込む情報量は 72 ビットよりも少なくなる．

提案方式では，透かし情報はウェーブレット変換して得られた LH_2 成分と HL_2 成分にスペクトル拡散の手法を用いて埋め込まれる．それらのスペクトル成分は，LH_2 成分と HL_2 成分に PN 系列を乗算した後に DCT を施して求めており，秘密情報に基づいて特定の DCT 係数に透かし情報が埋め込まれる．埋め込む透かし信号が一様に拡散されるのであれば，攻撃に対する耐性は DCT 係数に依存しないはずである．そこで，複数の DCT 係数に対して攻撃耐性と画質劣化の関係を調べる．表 4.3 は，埋め込みに用いた DCT 係数と耐性の関係を示しており，表 4.4 は DCT 係数と PSNR の値の関係を示している．

表 4.3　埋め込み係数と耐性の関係 ($T = 12$)

Table 4.3　Robustness for each embedding coefficient ($T = 12$).

image	(0,0)	(3,3)	(7,7)
lena	90.9	90.7	91.9
girl	96.4	96.4	96.7
baboon	77.6	76.2	75.0
peppers	88.0	89.9	88.4

表 4.4　埋め込み係数と PSNR の関係 ($T = 12$)

Table 4.4　PSNR for each embedding coefficient ($T = 12$).

position	(0,0)	(3,3)	(7,7)
PSNR [dB]	44.1	44.0	44.0

これらの結果より，攻撃に対する耐性及び画質はDCT係数とはほとんど依存していないことが確認できる．

4.4.3 JPEG圧縮に対する耐性

この節では，JPEGにより埋め込み画像に高圧縮をかけた場合の耐性を調べる．表4.5は，画像“lena”において1ビットの誤りもなく透かし情報が検出される割合を各埋め込み強度Tに関して示している．埋め込み強度が$T = 12$の場合，高圧縮に対しても高い耐性を有することが分かる．他の画像に関しても表4.11に示すように，同様の結果が得られた．

また$T = 8$の場合，表4.5より高圧縮をかけると耐性は低くなる．しかし，誤りビットの数を調べると，StirMark攻撃の場合と同様に3ビット以内であることが確認される．表4.6，表4.7にその分布を示す．

表4.5　JPEG圧縮に対する耐性 (“lena”)

Table 4.5　Tolerance for JPEG compression “lena”.

T	quality					
	25%	30%	35%	40%	45%	50%
8	11.1	38.4	74.4	88.8	94.0	99.3
10	43.4	79.9	95.0	99.0	99.4	100.0
12	80.6	96.8	99.7	99.9	100.0	100.0

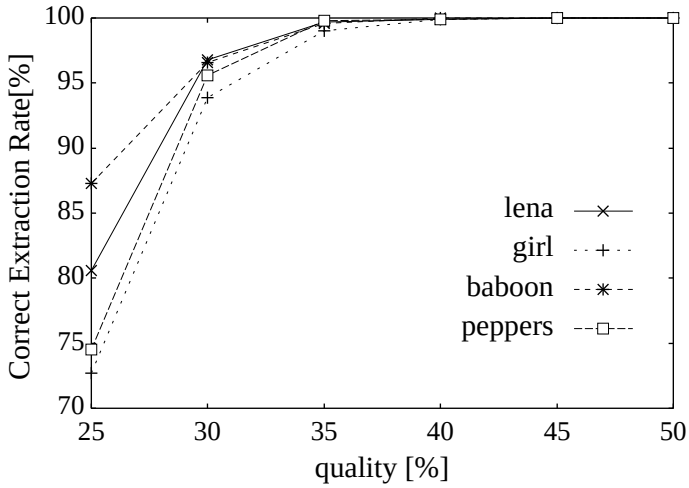


図4.11　JPEG圧縮に対する耐性 ($T = 12$)

Fig. 4.11　Tolerance for JPEG compression ($T = 12$).

表 4.6　JPEG 圧縮により生じた誤りビット数の分布状況 (“lena”, $T = 8$)
Table 4.6　Error distribution rate after high compression (“lena”, $T = 8$).

quality[%]	0bit	1bit	2bits	3bits	else
25	11.1	22.9	24.1	17.5	24.4
30	38.4	33.8	18.7	6.4	2.7
35	74.4	21.2	3.8	0.4	0.2
40	88.8	10.1	1.0	0.1	0.0

表 4.7　JPEG 圧縮により生じた誤りビット数の分布状況 ($T = 8$, quality 30%)
Table 4.7　Error distribution rate after high compression ($T = 8$, quality 30%).

image	0bit	1bit	2bits	3bits	else
girl	34.0	31.5	21.3	8.1	5.1
baboon	45.7	35.6	14.4	3.1	1.2
peppers	39.5	33.1	17.2	7.0	3.2

表 4.8 は，埋め込み強度 $T = 20$ の場合における JPEG 圧縮に対する耐性を提案方式 I に関して調べた結果である．この表より，この程度の埋め込み強度を使えば，JPEG 圧縮に対して非常に高い耐性を示すことが確認できる．ゆえに提案方式 II は必然的に JPEG 圧縮に高い耐性を有することが分かる．

表 4.8　JPEG 圧縮に対する耐性 ($T = 20$)
Table 4.8　Tolerance for JPEG compression ($T = 20$).

image	quality			
	20%	25%	···	50%
lena	98.5	100.0	···	100.0
girl	95.3	100.0	···	100.0
baboon	99.0	100.0	···	100.0
peppers	97.7	100.0	···	100.0

4.4.4　考察

電子透かしシステムを評価する上で，埋め込み可能な情報量や画質は重要な要素である．そこで提案手法と従来手法 [29][30] の比較を行う．提案手法では，埋め込み可能な情報量は提案方式 I においては 72 ビットである．ただし，StirMark 攻撃に対する耐性を考慮すると，誤り

訂正符号化するため 72 ビットより少なくなる．ここで，文献 [29] の方式では 16 ビットであり，文献 [30] の方式では 32 ビットであることから，たとえ符号化しても提案方式の方がより多くの情報を埋め込むことができる．更に，提案手法の方が PSNR の値は従来手法に比べて高い．提案手法の欠点としては，透かし情報を検出するために，原画像の一部分である同期化テンプレートが必要なところである．

次に，提案方式 I と提案方式 II に関して比較を行う．提案方式 I では，埋め込み可能な透かし情報は画像に依存せずに 72 ビットと固定することができる．一方提案方式 II では，画像の特徴に依存するため，一定の情報量を埋め込むことはできない．しかし，提案方式 II では，埋め込みによる画質劣化を方式 I に比べて知覚されにくく設定することができる．ここで重要となることは，埋め込む画像に適した埋め込みをするために，二つの方式を使い分けることである．なぜなら，平坦な領域を多く含む画像には提案方式 II を用いると埋め込み可能な情報量は少ないため適しているとはいえない．しかし，提案方式 I に誤り訂正符号を用いれば，攻撃に対する耐性は高く，多くの情報を埋め込むことができる．また，複雑な模様を多く含む画像には提案方式 I よりも提案方式 II を用いる方が望ましい．例えば，画像 “lena”, “girl”, “peppers” などは，背景に平坦な部分を多く含むため提案方式 I が適しており，一方画像 “baboon” には複雑な模様が多いため提案方式 II が適している．

更に適応的な方式への拡張として，平坦な部分と複雑な模様を含む部分に対してそれぞれ埋め込み強度を可変にする方法が考えられる．そのような方式は，提案方式 I と提案方式 II を組み合わせることで容易に実現ができる．また，埋め込み操作の Step 4 において量子化法による埋め込みを採用することも可能であり，元の情報を用いずに透かし情報を検出できる方式へと拡張することも可能である．

4.5 結言

本章では，ウェーブレット変換を局所的に行い，適応的な埋め込みが可能な電子透かし方式を提案した．透かし情報は，画像からランダムに選出した 4 個のブロックの周波数成分にスペクトル拡散の手法を適用させて埋め込まれる．ブロックの特徴に応じて判別させることにより，適応的に透かし情報を埋め込むことが可能となった．また，幾何学的な歪みに対する耐性を考慮して前章で述べた探索プロトコルを適用できるようにシステムを設計しており，StirMark 攻撃に高い耐性を有する．また，計算機シミュレーションにより，提案方式の有効性を検証することができた．

第5章　埋め込み信号間の距離に基づく電子透かし

5.1　緒言

第3章，第4章では，静止画像に対してStirMark攻撃とJPEG圧縮に耐性のある方式を提案した．本章では，ディジタル情報として，映画などの動画像を扱うことのできる電子透かしを提案する．動画像の電子透かしに求められる条件としては，静止画像と同じく各種攻撃に対して耐性を有することが挙げられる．ここで，動画像は，単純に考えると複数の静止画像 (フレーム) を一定時間ごとに表示すると考えられるため，静止画像への電子透かしの方式を適用することも可能である．しかし，動画像の場合，静止画像に対する攻撃に比べて動画像特有の攻撃があることに注意しなければならない．例えば，複数のフレームに関する相関を利用して圧縮が行われるため，複数のフレームの特徴を考慮して埋め込みを行う必要がある．また，幾何学的な改変に対して第3章で提案した探索プロトコルを行うためには，その同期化テンプレートを保存しておく必要があるが，動画像の場合，そのサイズが大きいため，実用的な方式ではない．

動画像の特徴を活かして幾何学的な歪みを補正する方式が草薙らにより提案されている [16]．その方式では，パッチワーク法 [8] を用いて同期信号が透かし情報とは別に埋め込まれる．透かし情報の検出前に同期信号を検出し，その信号により幾何学的にずれた位置を補正する．その結果，同期が回復されるので，透かし情報を高精度で検出することができる．しかし，この方式では，透かし信号と同期信号が共に同じ動画像に埋め込まれるため，埋め込みにより生じる画質劣化が激しいと推測される．また，透かし情報を検出するために，同期回復操作を前もって行う必要があるため，計算量が比較的多い．

本章では，幾何学的な歪みに耐性を有する動画像用の電子透かしを提案する．提案手法では，同期信号を埋め込む際に，二つの信号の位置関係に情報を与えることで透かし情報を埋め込む．一般に，幾何学的な改変を受けると，埋め込まれた信号の位置はずれてしまうが，比較的近距離に埋め込まれた信号間の距離はあまり影響を受けない．提案方式は，この特性を活かした埋め込み手法である．また，同期信号は，複数のフレームに拡散させて埋め込むことができるパッチワーク法を用いるため，視覚的な劣化を抑えることができる．同期信号の検出の操作さえ行えば透かし情報は検出できるため，透かし情報を検出するために必要な計算は比較的少ない．更に，透かし情報の検出の信頼性を向上させるための修正処理を提案する．その操作により高精度で透かし情報を検出することが可能になる．これらの手法の有効性を計算機シミュレーションにより調べる．

StirMark攻撃などの幾何学的な改変に対する耐性を考えると，同期信号の埋め込みによる

アプローチは最適な手法であるかもしれない．従来では，同期信号の埋め込みと透かし情報の埋め込みは独立して行われていたが，提案手法では埋め込む信号は同期信号だけである．ここで，透かし信号は同期信号により変調されていると考えることができる．この手法は透かし情報の埋め込むことのできる新しい空間として今後の発展が期待される方式である．

5.2 信号間の距離

従来の電子透かしの埋め込みでは，画像に対してその座標系は重要な要素として扱われている．例えば，画像をブロックに分割して埋め込みを行う場合，ある座標から縦横数ビットごとにブロックを構成している．もし，幾何学的な改変を微小でも画像に与えると，座標自体が変化するため正しくブロック分割が行えない．それゆえ透かし信号が画像の中に残っていたとしても，検出することができない．しかし，座標の同期さえ回復できれば，透かし情報は検出することは可能である．なぜなら，信号間の位置関係は微小な幾何学的改変を受けたとしてもあまり変化しないからである．以上のことから次のことが導かれる．

- 絶対的な座標位置は微小な幾何学的改変でも変化する．
- 相対的な座標位置はあまり影響を受けない．

ここで，絶対的な座標位置とは，$(0,0)$ を基準とした座標であり，相対的な座標位置はある信号の座標を対応する信号座標からの位置とみなしたものである．例えば，座標 $(2,3)$ の A 点と座標 $(7,5)$ の B 点を考える．微小な幾何学的改変として x 方向に 3，y 方向に 2 平行移動させると，改変後 A 点は $(5,5)$ に，B 点は $(10,7)$ となる．絶対的な座標位置を考えた場合，改変後の各点は元の座標とは異なっている．しかし，相対的な座標位置では，改変前の B 点は A 点から見て x 方向に 5，y 方向に 2 だけ離れており，この位置関係は改変後も同じである．微小な回転や拡大縮小操作の場合でも，同様に信号間の位置関係はほどんど影響を受けない．

従来法では，幾何学的な歪みを補正するために同期信号を埋め込み，絶対的な座標位置の移動量を計算していた [16]．この同期信号の埋め込みの際に相対的な座標位置関係を与えることができれば，幾何学的な歪みの補正だけでなく，別の情報を位置情報として埋め込むことができる．このことを図 5.1 を使って説明する．ある同期信号が座標 (x,y) を基準として埋め込まれたと仮定する．x 方向に関して同期信号を埋め込む際に，座標 $(x+\delta,y)$ もしくは座標 $(x+\delta,y+8)$ を選択させることで，1 ビットの情報を埋め込むことができる．なぜなら，信号間の距離として，y 方向のずれが 4 以内もしくは以上として判別させることで情報を検出できるからである．図 5.1 において △ で示した二つの座標の内，一方を同期信号の埋め込み位置として選択することで，位置情報を同期信号に与えることができる．同様に y 方向に関しても，

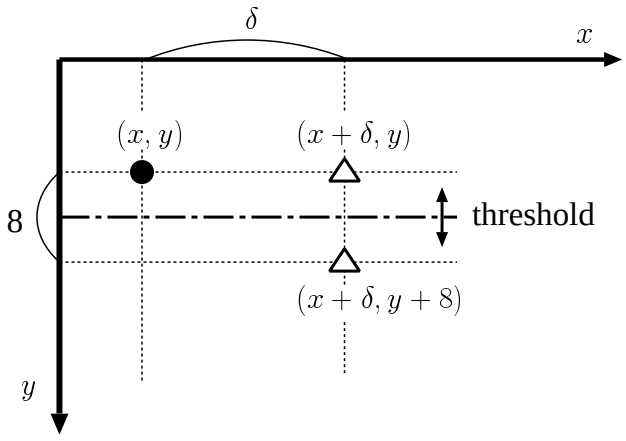


図 5.1　埋め込み位置の候補

Fig. 5.1　The candidates of each embedding position.

座標 $(x, y+\delta)$ もしくは座標 $(x+8, y+\delta)$ を選択させることで，1 ビットの情報を埋め込むことができる．

5.3　埋め込み操作

提案手法では，同期信号が埋め込まれる位置は透かし情報に基づいて決定され，二つの信号間の距離により埋め込まれた情報が検出される．同期信号の埋め込みにはパッチワーク法を用いて，各信号は 18×18 画素の領域 $B(x, y)$, $(0 \leq x < N_X, 0 \leq y < N_Y)$ で動画像の 30 フレームに拡散させて埋め込む．ここで，x 方向に N_X 個の信号を埋め込み，y 方向に N_Y 個の信号を埋め込むことで計 $N_X \times N_Y$ の同期信号を埋め込む場合を考える．この場合，x 方向への埋め込みは $(N_X - 1) \times N_Y$ ビットとなり，y 方向は $(N_Y - 1) \times N_X$ ビットとなるので，埋め込む透かし情報の合計は $2N_XN_Y - N_X - N_Y$ ビットとなる．

透かし情報を埋め込む前に，x 方向，y 方向それぞれ基本となる位置を与える初期信号を埋め込まなければならない．各方向において初期信号と隣接する同期信号の埋め込み位置は，透かし情報に基づいて与えられる初期信号の座標位置からの距離関係によって決定される．その後に埋め込まれる同期信号の場合，一つ前の同期信号の位置との相互関係に透かし情報が与えられる．

$(X_{B(x,y)}, Y_{B(x,y)})$ をフレームの左上に埋め込まれる同期信号の座標位置とする．ただし，その座標は領域 $B(x, y)$ の左上の画素の位置であり，秘密情報により決定する (図 5.2 に示した●の位置である)．この位置を基本として，同期信号の埋め込み座標位置候補 △ を作成する．

Step 1. 最初に初期位置を秘密情報に基づいて選出する．その座標を $(X_{B(0,0)}, Y_{B(0,0)})$, $6 \leq$

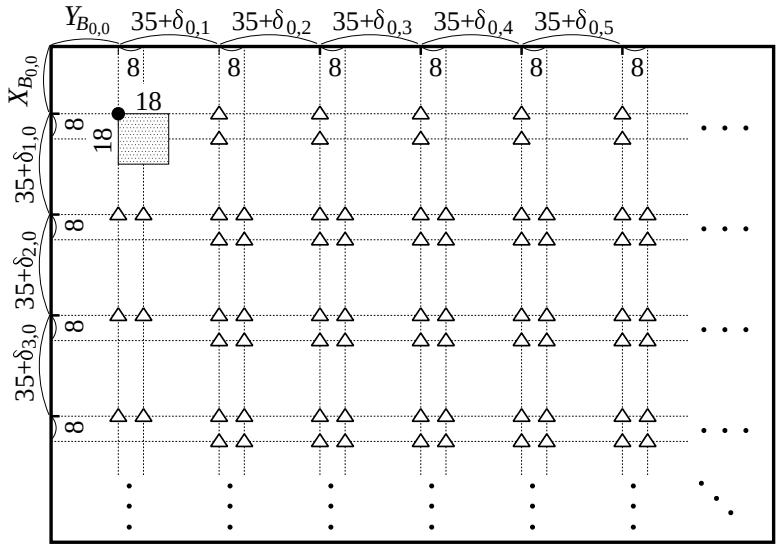


図 5.2　透かし情報に基づいて選択される埋め込み位置の候補
(ただし，△ は埋め込み位置の候補である)

Fig. 5.2　The candidates of each embedding position determined by a watermark. Where △ is the candidates of the embedding positions.

$X_{B(0,0)}, Y_{B(0,0)} \leq 12$ とする．

Step 2. 次に，一行目と一列目の座標を秘密情報に基づいてそれぞれ次のように決定する．

$$Y_{B(0,j)} = Y_{B(0,0)} + 35j + \delta_{0,j},\ (1 \leq j < N_Y), \tag{5.1}$$

$$X_{B(i,0)} = X_{B(0,0)} + 35i + \delta_{i,0},\ (1 \leq i < N_X), \tag{5.2}$$

ただし，$\delta_{0,j}$ と $\delta_{i,0}$ は次の不等式を満たすランダムな整数である．

$$|\delta_{0,j}| < 4, \quad |\delta_{i,0}| < 4 \tag{5.3}$$

初期信号の座標位置の決定には次に挙げる条件を考慮している．

- フレームの端は冗長成分が多く，攻撃により取り除かれる可能性が高い
- StirMark 攻撃によりずれる座標位置はせいぜい 6 画素程度である．

これらの条件により $B(0,0)$ の座標位置をフレームの端より 6 画素以上内側から選出するようにしてある．また，パッチワーク法により同期信号は 18×18 画素の領域内で埋め込まれるため，隣接する信号がお互いに干渉しないように設定しなければならない．また，StirMark 攻撃による座標のずれを許容できるように一行目と一列目の座標位置を式 (5.1) と式 (5.2) のように設定している．

初期信号と一行目，一列目の座標位置により，図5.2に示すような線を引くことができる．この線の交わる点が同期信号を埋め込む候補点となり，その決定は透かし情報に基づいて行われる．ここで，座標位置の決定はx方向，y方向それぞれ独立させて行われ，埋め込み位置の候補は各方向に関して選出される．そのため，x方向に関して隣接するブロックの候補は各行にN_Y-1個あるため，埋め込み可能な透かしの情報量は$P_Y=N_X(N_Y-1)$ビットとなる．同様にy方向に関しては，各列にN_Y-1個の候補があるので透かしの情報量は$P_X=N_Y(N_X-1)$ビットとなる．ゆえに$2N_XN_Y$個の同期信号に対して総計$N_w=P_X+P_Y=2N_XN_Y-N_X-N_Y$ビットの情報を埋め込むことができる．

透かし情報を$w_t\in\{0,1\}$として，同期信号の埋め込み位置は次のアルゴリズムにより決定される．

x**方向** $(t=0)$

for $y=1$ **to** N_Y **do**
{
  for $x=0$ **to** N_X **do**
  {
    if $w_t=0$ **then**

$$X_{B(x,y)}=X_{B(x,y-1)} \tag{5.4}$$

    else
    {
      if $X_{B(x,y-1)} \pmod{35} < X_{B(0,0)}+4$ **then**

$$X_{B(x,y)}=X_{B(x,y-1)}+8 \tag{5.5}$$

      else

$$X_{B(x,y)}=X_{B(x,y-1)}-8 \tag{5.6}$$

    }
    $t=t+1$
}}

y**方向** $(t=P_X)$

for $x=1$ **to** N_X **do**
{

for $y = 0$ **to** N_Y **do**
{
if $w_t = 0$ **then**

$$Y_{B(x,y)} = Y_{B(x-1,y)} \tag{5.7}$$

else
{
if $Y_{B(x-1,y)} \pmod{35} < Y_{B(0,0)} + 4$ **then**

$$Y_{B(x,y)} = Y_{B(x-1,y)} + 8 \tag{5.8}$$

else

$$Y_{B(x,y)} = Y_{B(x-1,y)} - 8 \tag{5.9}$$

}
$t = t + 1$
}}

埋め込み位置が決定された後に同期信号はパッチワーク法に基づいて埋め込まれる．ここで，従来のパッチワーク法において埋め込み領域内の特徴を利用することで適応的な方式へと拡張させる．通常の埋め込み強度での埋め込みに加えて，埋め込み領域内が複雑な成分を多く含むならば，付加的に強く信号を埋め込むように式 (2.26) の埋め込み強度 α を次のように変更する．

$$\alpha_{a_i} = \beta(1 + \gamma \cdot T_{a_i}), \tag{5.10}$$

ただし，β と γ はそれぞれ，一定の重みパラメータとし，T_{a_i} は各画素の分散値に依存して決定される値とする．式 (2.29) と式 (5.10) より，$S(n)$ の分布は少なくとも $2\beta n$ だけ増加することが保証される．更に埋め込み領域内の特徴に応じて $2\beta\gamma T_{a_i} n$ だけ増加する．このことを図 5.3 に示す.

提案手法では，数フレームに拡散させて透かし情報を埋め込むため，分散値を各画素ごとに求めると計算量が莫大となる．そこで，エッジ検出のフィルタ操作を代わりに行う．ここでは，雑音成分にあまり影響を受けない Sobel の勾配を用いる．

画素 a_i に対して Sobel 勾配を施して得られた値を $f(a_i)$ とする．埋め込み強度 T を定めると T_{a_i} は次のように求められる．

$$T_{a_i} = \begin{cases} f(a_i) & \text{if } f(a_i) < T \\ T & \text{otherwise} \end{cases} \tag{5.11}$$

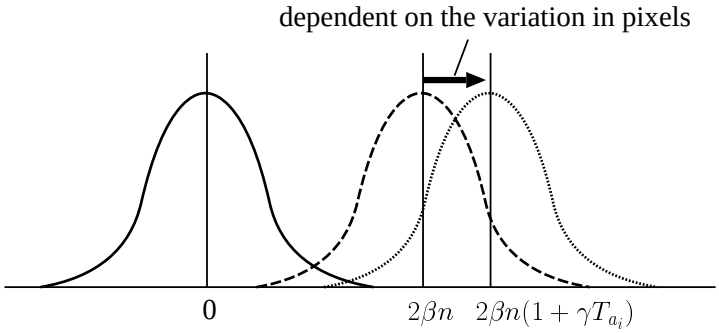


図 5.3　$S(n)$ の分布の偏り

Fig. 5.3　Changes in a distribution of $S(n)$.

5.4　検出操作

透かし情報の各ビットは，二つの同期信号間の距離により判定される．そのため，透かし情報の検出の前に，まず同期信号の検出を行う．同期信号の検出において，初期信号の座標が分かれば，他の信号は図 5.2 に示す埋め込み候補点の座標に関してのみ確認すれば良い．しかしながら，ランダムな幾何学的改変を受けると，その位置関係は完全には保たれず，微小に変化してしまう．それゆえ，図 5.4 に示すような探索範囲を設けて，各同期信号においてそれぞれの探索範囲内で検出操作が行われる．

同期信号の検出操作は，次のように段階的に行われる．まず，埋め込み候補点において同期信号の検出操作を行う．検出された $S_{B(x,y)}(n)$ の総和を計算し，その値があるしきい値 $N_X N_Y h$ 以上であれば，同期信号の検出操作を終了する．しきい値未満であれば，各同期信号において $S_{B(x,y)}(n)$ の値を埋め込み候補点だけでなく探索範囲内で行い，その値が最大となる点を検出する．

以下に，同期信号の検出手順及び透かし情報の検出手順を示す．

Step 1. 埋め込み操作で決定した初期位置と一行目，1 列目の座標位置を決める．

Step 2. 図 5.2 に示す埋め込み候補点においてパッチワークの検出操作を行う．その際，$S_{B(x,y)}(n)$ が最大となる候補点を同期信号の埋め込まれた座標として検出する．

Step 3. もし，$S_{B(x,y)}(n)$ の総和がしきい値 $N_X N_Y h$ 以上であれば，Step 5 に進む．しきい値未満の場合は Step 4 に進む．

Step 4. 各同期信号の検出のために，それぞれの探索範囲 K 内のすべての座標に対して $S_{B(x,y)}(n)$ の値を求め，最大となる座標をその同期信号が埋め込まれた座標として検出する．

Step 5. x 方向，y 方向に関してそれぞれ次に示す操作により透かし情報を検出する．

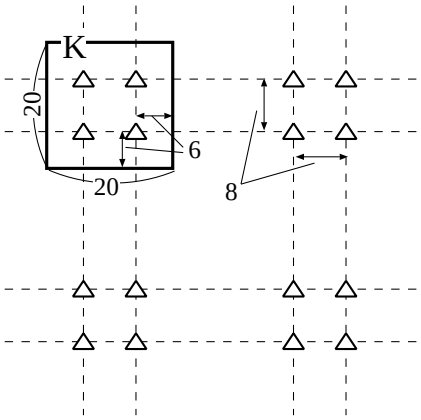


図 5.4　埋め込み位置の探索領域 K

Fig. 5.4　The searching area K for each embedded position.

x **方向** $(t = 0)$

for $y = 1$ **to** N_Y **do**

{

for $x = 0$ **to** N_X **do**

{

$$D_x = |X_{B(x,y)} - X_{B(x,y-1)}| \tag{5.12}$$

$$\hat{w}_t = \begin{cases} 0 & D_y < x \\ 1 & 4 < D_x < 12 \\ NULL & \text{otherwise} \end{cases} \tag{5.13}$$

$t = t + 1$

}}

y **方向** $(t = P_X)$

for $x = 1$ **to** N_X **do**

{

for $y = 0$ **to** N_Y **do**

{

$$D_y = |Y_{B(x,y)} - Y_{B(x-1,y)}| \tag{5.14}$$

$$\hat{w}_t = \begin{cases} 0 & D_y < 4 \\ 1 & 4 < D_y < 12 \\ NULL & \text{otherwise} \end{cases} \tag{5.15}$$

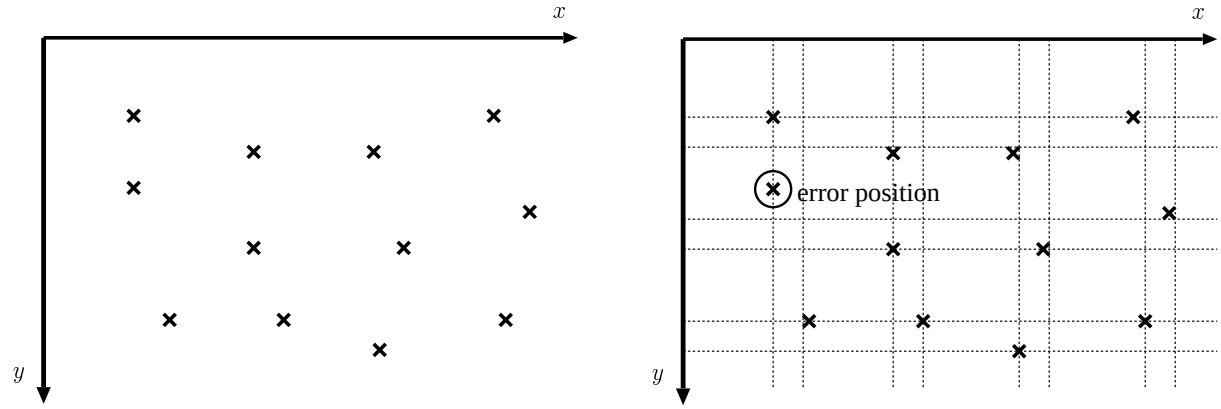
$t = t + 1$

}}

ただし，$NULL$ は透かし情報が検出されなかったことを意味する．

5.5 探索範囲の推定による修正

透かし情報の検出操作において，同期信号の位置が必ずしも正しいと保証することはできない．ここで，同期信号の位置を誤って検出される場合として，他の埋め込み位置候補の付近で検出される場合と，どの埋め込み候補からも遠い距離に位置する場合がある．偶然他の埋め込み位置候補付近で同期信号が検出されれば，透かし情報は正常に出力されるため誤り検出とは判定できない．しかし，誤り検出位置が後者の場合であれば，式 (5.13) と式 (5.15) より $NULL$ が出力されるため，明らかに誤り検出と判定できる．複数の同期信号の座標が検出されれば，x 方向及び y 方向に図 5.2 で描かれた線を引くことが可能である．その線の交点付近に同期信号の検出される座標があるはずなので，もし離れたところで検出されていれば，その交点付近だけで再検出操作を行えば修正処理が行える．例えば，図 5.5(a) に示すように同期信号が検出されたとする．このとき x 方向，y 方向にそれぞれ推定される線を図 5.5(b) のように引くことができる．その結果，明らかに不自然な位置で検出された同期信号を判定できるため，この同期信号は誤り検出であると分かる．



(a) 同期信号の検出　　(b) 誤り検出位置

図 5.5　同期信号の誤り検出位置の判定

Fig. 5.5　Discrimination of error position from detected synchronization signals.

以下に，検出操作の Step 4 と Step 5 の間に挿入される同期信号の誤り検出位置を修正するプロトコルを示す．

1. x 方向に二本の推定線 $hline1[i]$，$hline2[i]$ を検出した同期信号の x 座標 $X_{B(i,j)}$ により求める．y 方向にも同様に二本の推定線 $vline1[j]$，$vline2[j]$ を y 座標 $Y_{B(i,j)}$ により求める．

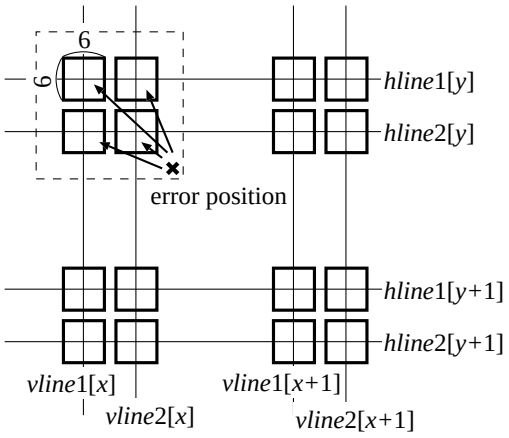


図 5.6　推定線により限定された探索領域

Fig. 5.6　The reduced searching area using estimated lines.

2. 図 5.6 に示すように各推定線の交点付近に検出領域を設け，その範囲外に位置する同期信号の座標を見つける．

3. 発見された同期信号において，絞りこまれた領域内で再び検出操作を行う．

推定線は必ずしも水平方向，垂直方向に引く必要はなく，少し傾きを持つ場合がある．その際には，透かし情報の検出操作で $NULL$ が出力されるかもしれない．例えば，もし $X_{B(x,y)} = hline1[x] - 2$，$X_{B(x,y-1)} = hline1[x] + 2$ の場合，$D_x = 4$ となり，式 (5.13) より $NULL$ となる．それゆえ，透かし情報の検出操作の Step 5 を次のように変更する．x 方向において，各 $vline1[j]$ と $vline2[j]$ の中間に中線 $vline[j]$ を引く，もし，二つの同期信号の検出座標位置が共に $vline[j]$ より上もしくは下にあれば，透かし情報を $w_t = 0$ と判定する．同様に y 方向においても $hline1[j]$ と $hline2[j]$ の中間に中線 $hline[j]$ を引いて透かし情報の検出を行う．

5.6　計算機シミュレーション

提案手法の有効性を調べるために，352×240 画素，150 フレームの動画像 “Flower Garden” と “Tennis” を用いてシミュレーションを行う．同期信号は 30 フレームごとにパッチワーク法を用いて，$N_X = 6$，$N_Y = 9$ として計 54 箇所に埋め込む．パッチワーク法では $\beta = 1$，$\gamma = 0.1$ とし，サンプル数は $10,000$ とする．この際，透かし情報は合計 93 ビット $(= 2N_XN_Y - N_X - N_Y)$ を埋め込む．以下に示す結果は，シミュレーション回数を 1,000 回として求めた値である．

5.6.1 画質評価

動画像の画質評価に関しても静止画像と同様に PSNR を用いる．ただし，パッチワークにより埋め込まれる信号は 30 フレームに拡散されているため，30 フレーム全体における PSNR の値を求める．図 5.7 に埋め込み強度 T に対する PSNR の値を示す．実際に動画像を再生し

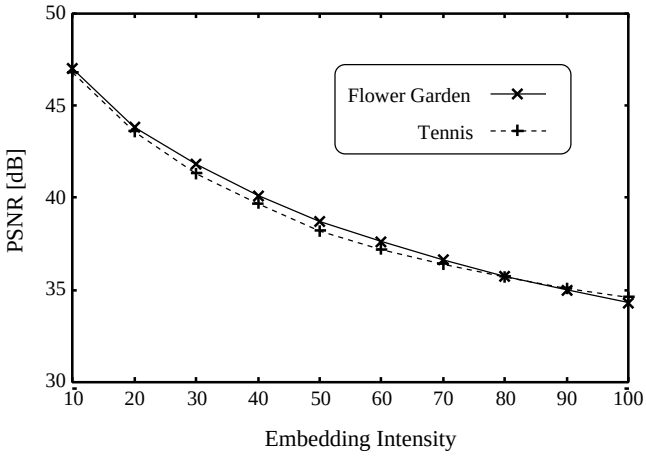


図 5.7　埋め込み強度と PSNR の関係
Fig. 5.7　PSNR versus embedding intensity.

て確認した画質としては，“Flower Garden” では $T = 50$，“Tennis” では $T = 30$ 程度までならば視覚上の劣化はほとんど確認されなかった．

5.6.2 非幾何学的改変に対する耐性

非幾何学的改変に対する耐性を調べるために，透かし情報の埋め込まれた動画像に MPEG 圧縮，ガウシアンフィルタ，メディアンフィルタを施し，透かし情報の抽出を試みる．非幾何学的改変では，同期信号の座標は変更されないので，それらの検出には候補点のみにおいて検出操作を施せば良い．もし，その際に得られる $S(n)$ の値が非常に小さければ，同期信号自体が取り除かれたことになり，透かし情報も消去されている．ゆえに，シミュレーションでは，$S(n)$ の値がしきい値 h 未満の場合は，透かし情報の検出は失敗とみなす．

最初に，低ビットレートで MPEG 圧縮を行った場合の透かし情報の検出率を調べる．表 5.1 は各ビットレートにおける検出誤りビット数の平均値を示している．“Tennis” では低ビットレートにおいても検出誤りはほとんど生じていないが，“Flower Garden” では埋め込み強度を高くしなければ MPEG 圧縮に対する耐性が低い．ここで，透かし情報を誤り訂正符号化すれば，耐性を向上させることが可能である．

次に，ガウシアンフィルタ及びメディアンフィルタに対する耐性試験の結果をそれぞれ表

5.2，表5.3に示す．各動画像において埋め込み強度を “Flower Garden” では$T = 50$，“Tennis” では$T = 30$とすれば，誤りビット数は十分低く抑えられることが確認できる．ゆえに，誤り訂正符号により，耐性を向上させることが可能である．

表5.1　MPEG圧縮に対する耐性
Table 5.1　Tolerance for MPEG compression

T	bit-rate [Mbps]	bit error rate	
		Flower	Tennis
20	2	6.56	0.33
	3	1.95	0.00
	4	0.50	0.00
30	2	2.86	0.00
	3	0.49	0.00
	4	0.00	0.00
40	2	1.29	0.00
	3	0.97	0.00
	4	0.00	0.00
50	2	0.96	0.00
	3	0.89	0.00
	4	0.00	0.00

表5.2　ガウシアンフィルタに対する耐性
Table 5.2　Tolerance for Gaussian filter

T	bit error rate	
	Flower	Tennis
20	6.39	2.12
30	3.31	0.52
40	0.00	0.52
50	0.00	0.00

表5.3　メディアンフィルタに対する耐性
Table 5.3　Tolerance for Median filter

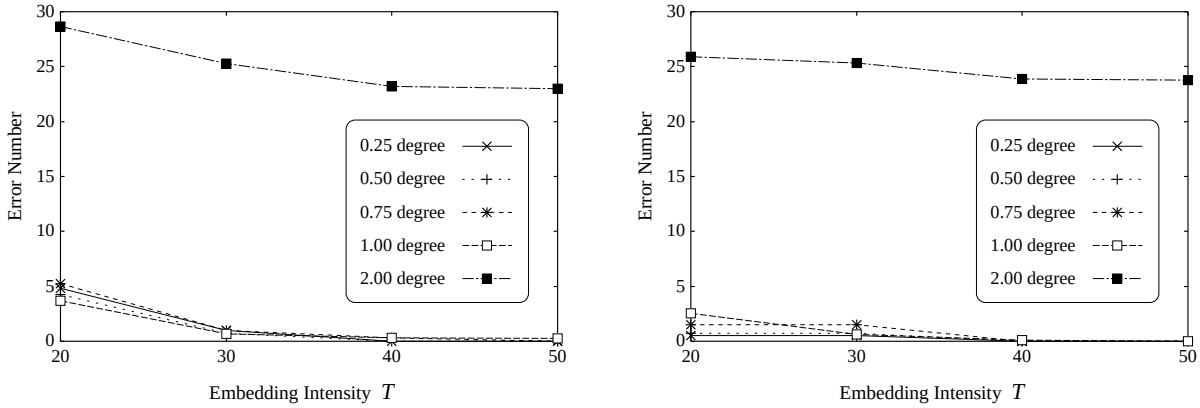
T	bit error rate	
	Flower	Tennis
20	14.81	2.67
30	5.41	1.02
40	2.18	1.02
50	0.97	1.02

5.6.3　幾何学的改変に対する耐性

StirMark攻撃を用いて，幾何学的改変に対する耐性を調べる．透かし情報の埋め込まれた動画像に対して幾何学的な改変を加える場合，フレームごとに独立して行うことはできない．なぜならば，動画像ではフレーム間に強い相関があるため，幾何学的改変により一つのフレームだけ座標位置をずらせば，奇妙な動きが動画像に現れてしまう．そこで，シミュレーションを行う場合には，すべてのフレームにおいて同じ幾何学的な改変を加える．

最初に，不自然さが生じない程度に画像を回転させ，その際の透かし情報の検出率を調べる．図5.8(a)には “Flower Garden”，図5.8(b)には “Tennis” における結果を示す．これらの結果より，回転角度が2度未満であれば回転により生じる誤りビット数は少ないことが分かる．

次に，行や列の抜き取り操作に対する耐性を調べる．数行や数列の抜き取りであれば不自然さが生じないため，ここではそれぞれ5行，5列ずつランダムに抜き取り，透かし情報の検出



(a) Flower Garden　　(b) Tennis

図 5.8　回転に対する耐性 (Flower Garden)

Fig. 5.8　Tolerance for rotation (Flower Garden).

を試みる．その結果を表 5.4 に示す．この結果より，行，列の抜き取り操作に対しても高い耐性を示すことが確認された．

表 5.4　任意の 5 行 5 列の削除に対する耐性

Table 5.4　Tolerance for five columns and rows removal attack.

T	bit error rate			
	Flower		Tennis	
20	3.52	(4.16)	0.45	(0.62)
30	1.38	(1.74)	0.15	(0.28)
40	0.62	(0.79)	0.07	(0.15)
50	0.26	(0.30)	0.05	(0.09)

ランダム幾何学的改変に対する耐性を表 5.5 に示す．ここで，括弧内の値は修正手法を用いなかった場合の結果を示している．この結果より，修正手法の有効性が確認できる．また，ランダム幾何学的改変に対しても高い耐性を持つことが示された．

表 5.6 は，StirMark 攻撃に対する耐性を示している．この場合においても修正手法が効果的に誤りを修正していることが確認できる．また，誤り訂正符号を用いれば，“Flower Garden” は $T = 50$，“Tennis” は $T = 30$ の場合，StirMark 攻撃に対して高い耐性を有するといえる．

表 5.5　ランダム幾何学変換に対する耐性

Table 5.5　Tolerance for random geometrical attack.

T	bit error rate			
	Flower		Tennis	
20	6.83	(8.36)	1.35	(2.12)
30	2.10	(3.04)	0.61	(1.01)
40	0.89	(1.59)	0.33	(0.60)
50	0.59	(1.24)	0.37	(0.17)

表 5.6　StirMark 攻撃に対する耐性

Table 5.6　Tolerance for StirMark attack.

T	bit error rate			
	Flower		Tennis	
20	15.03	(16.93)	4.70	(5.92)
30	5.80	(7.23)	2.73	(3.72)
40	2.81	(3.72)	1.89	(2.66)
50	1.93	(2.59)	1.40	(2.04)

5.6.4　考察

埋め込み強度を大きくすれば攻撃に対する耐性は向上するが，画質劣化が激しくなるため，これらはトレードオフの関係にある．提案手法では，動画像に依存してこれらの関係が異なっていることがシミュレーションにより確認された．理由としては，フレーム間での相関が大きく関与していると考えられる．例えば，動きの激しい映像では，フレーム間における変化が激しいため信号の埋め込みにより生じる視覚的な劣化が知覚されにくい．動画像 “Flower Garden” では，フレーム全体が左方向にシフトする映像であり，各フレームにおいて複雑な模様が多く含まれている．一方動画像 “Tennis” の場合，背景はほとんど変化せず，複雑な模様も少ない．それゆえ，埋め込み強度に関して “Flower Garden” の方が高く設定することが可能である．提案手法では，パッチワークを埋め込む際に重みパラメータ T_{a_j} を各フレーム内の情報から求めているが，フレーム間の相関も考慮して決定すれば，更に適応的な埋め込みが可能である．

提案手法の特徴は，同期信号を埋め込む位置関係に透かし情報が与えられるところである．今回は，パッチワーク法を用いて同期信号を埋め込んでいるが，他の方法を用いて同期信号を埋め込む場合においても同様に透かし情報を埋め込むことが可能である．

5.7 性能比較

提案手法の有効性を示すために，他の方式との比較を行う．ランダムな幾何学的改変に対する耐性を有する電子透かし法は大きく分けて次に挙げる 5 つの方法が提案されている．

- 原画像もしくはその一部分を用いて同期を回復させる．
- 画像の低周波成分に透かし情報を埋め込む．
- 画像の特徴点を利用して埋め込みを行う．
- 同期信号を画像に埋め込み，同期を回復させる．
- 周期的な透かし信号を埋め込む．

原画像もしくはその一部分を用いて同期回復を行う手法は多く提案されている [31]．しかし，動画像の場合，透かし情報の検出に元の動画像を使うことはデータ容量を考えると難しい．文献 [32] では，画像の低周波成分に埋め込まれた信号が幾何学的な改変に対して影響を受けにくいことを利用して極めて低周波の DCT 係数に透かし情報を埋め込んでいる．しかし，この手法は，透かし情報が埋め込まれる位置はごく一部の低周波成分に限られるため攻撃者に特定されやすい．また，画像全体に DCT を施すため必要となる計算量が莫大である．パッチワーク法による埋め込みに必要な計算量は，これに比べてはるかに少なく，埋め込みのパターンは莫大にあるため攻撃者に解析される可能性は少ない．

文献 [33] では，特徴点を利用して画像を小さな三角形の領域に分割し，各領域に合わせて透かし情報を埋め込んでいる．幾何学的な改変に対して，元の特徴点が検出されれば，歪んだ画像においても領域分割した各三角形を取り出すことができる．また，その三角形から透かし情報を検出することが可能である．この方式では，特徴点が正しく検出されることが前提条件となっており，攻撃によりこれらの特徴点が変化した場合には透かし情報は正しく検出できない．また，埋め込む情報は 1 ビットであり，ある特定の系列が埋め込まれているか否かを判定するだけである．提案方式のように多くの情報を埋め込むためには改良が必要であり，その場合攻撃に対する耐性は低くなるかもしれない．

同期信号を埋め込む手法は，提案手法でも採用しているが，従来法 [16] では同期信号と透かし情報は別々に埋め込まれる．そのため，画像に生じる視覚的な歪みは提案手法に比べて大きくなる可能性がある．また，提案手法では同期信号に別の情報を載せて画像に埋め込むことができる．この考えは従来にはない全く新しい概念であり，透かし情報の埋め込むことのできる新しい領域を示している．例えば，文献 [16] において同期信号の埋め込みの際に透かし情報を与えるならば，$N_X = 3$, $N_Y = 6$ となり 27 ビット ($N_w = 2N_XN_Y - N_X - N_Y$) の情報を付加的に埋め込むことが可能である．

周期的な透かし信号を埋め込む手法は，同期のずれを回復できる注目すべき方法の一つである．この方法では，周期的な信号により検出器側で同期点を判別することができる．しかし，同時に攻撃者にも多くの情報を与えることになるため，悪意のある攻撃者による意図的な改ざん攻撃に対する耐性は疑わしい．一方提案手法では，同期信号は雑音のように複数のフレームに拡散させているため，攻撃者に解析される可能性は低い．

5.8 結言

本章では，新しい動画像の電子透かし法を提案した．提案手法では，同期信号を埋め込む際，信号の座標に透かし情報を載せることができる．埋め込む同期信号の二点間の距離により透かし情報を判別して検出することができる．提案手法の利点として，画質劣化を抑えられることが挙げられる．従来では同期信号と透かし信号を別々に埋め込んでいたが，提案手法では画像に加える信号は同期信号だけであり，透かし情報はそれらの座標位置の情報なので画質劣化には関与しない．また，誤り検出を防ぐための修正法を提案した．StirMark 攻撃などの幾何学的な改変に対しても高い耐性を有することがシミュレーションにより確認された．

第6章　加法性準同型写像の性質を用いた電子指紋プロトコル

6.1　緒言

電子指紋技術は，ディジタルコンテンツに購入者の情報を電子透かし技術を用いて埋め込みむことで，不正コピーを発見した際にその情報を取り出して不正者を追跡可能にする．2.5 節で述べたように非対称方式でなければ，法的に不正者を訴えることができない．また，購入者の匿名性を守ることも実際の売買では要求される．第 2 章で示した Pfitzmann らの手法のように登録証明書をセンタに発行してもらう操作を非対称方式の電子指紋プロトコルの前に付属すれば匿名方式へと拡張できる．

非対称方式における従来の問題点として，暗号化率や計算量などの問題点が挙げられる．Pfitzmann らは，ビットコミットメントの準同型写像の性質を用いて購入者の情報をディジタルコンテンツに情報を埋め込む手法を提案している [17]．その操作は簡単な乗算や除算で行われるが，暗号化率を考えると実用的ではない．その後に提案された匿名方式 [19][20] は，この非対称方式に付加的なプロトコルを与えて購入者の匿名性を保証するものであるため，暗号化率は改善されていない．また，文献 [26] は計算量の削減を目的とした方式であり，文献 [27] は販売者と信頼できる機関との結託攻撃に関して考慮している．いずれの方式においても，実装という点からすれば暗号化率が悪いため更なる改善が必要である．

非対称方式において，購入者を示す情報をディジタルコンテンツに埋め込むためには，暗号化したコンテンツに暗号化された情報を埋め込まなければならない．そのために暗号方式の準同型写像の性質を用いる必要がある．ここで，電子透かし技術に関して考察する．3 章，4 章で述べたようにディジタル画像に透かし情報を埋め込む場合，攻撃に対する耐性から周波数成分に埋め込む方式が望ましい．しかし，画像の周波数成分を求める場合は実数値計算を行うため，整数の代数学的構造を利用する暗号技術を直接使うことはできない．また，埋め込む透かし情報ビットは暗号化されているため埋め込む際には分からない．それゆえ，埋め込み操作を単純に行うことはできず，特別な操作が必要である．従来法では，その点に関して全く議論されていない．

本章では，岡本–内山暗号を用いて匿名電子指紋法における暗号化率を向上させ，電子透かし法に適用させる方法を提案する．岡本–内山暗号には，加法性準同型写像の性質があるため，暗号化されたコンテンツに暗号化された透かし情報を乗算すると，透かし情報が加算されたコンテンツの暗号文が作成できる．岡本–内山暗号は公開鍵暗号であるため，購入者の公開鍵を用いて暗号化操作を行えば，透かし情報の埋め込まれたコンテンツを入手できるのは，購入者だけに限られる．それゆえ，不正コピーの流出を発見すれば，販売者は透かし情報を検出す

ることで購入者を特定することができる．また，その事実を裁判官などの第三者に証明することができる．プロトコルにおいて，透かし情報は購入者を示す情報であり，購入者は暗号化してから販売者に送る．ここで，販売者は受信した暗号文に購入者を示す情報が含まれることを確認できる方が望ましい．しかし，匿名性を考えると購入者は透かし情報自体を販売者に知らせずに正当性を示さなければならない．そこで，岡本–内山暗号の性質を使ってコミットメントを生成し，正当性を示すプロトコルを行う．また，画像の周波数成分に暗号化された透かし情報を埋め込めるように，量子化する段階で前もって埋め込み位置での周波数成分の値を偶数化しておく．この操作により，透かし情報ビットが 0 ならば何も加算されず，1 ならば加算により値が偶数から奇数になるため，透かし情報ビットを知らなくても埋め込むことが可能となる．更には，埋め込みの際には画質劣化などの要素を考慮して JPEG 圧縮の量子化テーブルを用いる．

6.2 提案電子指紋プロトコル

提案手法では，岡本–内山暗号の加法性準同型写像の性質を匿名電子指紋プロトコルに応用させる．例えば，Pic を画像の成分とし，ID を透かし情報のビットとすれば，埋め込み後の画像は $Pic + ID$ として表現される．購入者は自分の ID 情報を販売者に暗号化して送り，販売者は暗号化した自分の画像に受信した暗号文を乗算することで埋め込みを行う．購入者は販売者から送信される暗号文を復号することで自分の ID 情報の埋め込まれた画像を手に入れることができる．ここで暗号化には購入者の公開鍵を用いているため，その暗号文は購入者だけが復号できる．

6.2.1 電子指紋プロトコル

電子指紋プロトコルは購入者と販売者の二者間で行われる．初めに購入者は，自分の電子指紋 (透かし情報)，$id = \sum w_j 2^j, (0 \leq j \leq \ell - 1)$ を暗号化した com_j を計算し，販売者に送信する．次に，販売者は自分の所有する画像 I_i $(0 \leq i \leq L - 1)$ を暗号化して，受信した暗号文 com_j を乗算する．用いる暗号は岡本–内山暗号であり，2.5.4 節で設定したパラメータ公開鍵 (N, g, h, k)，秘密鍵 (p, q) を用いる．ここで，購入者はすでに信頼できるセンタに自分の ID 情報と公開鍵を登録し，その証明書を発行してもらってあるものとする．説明の簡略化のため，$W = g^{id} \bmod N$ を id のコミットメントとする．これらのパラメータを用いて，提案電子指紋プロトコルを示す．

Step 1. 販売者はある乱数 $a(2^\ell < a < N)$ を選択し，それを購入者に送る．

Step 2. 購入者は次の式を満たすように ℓ の乱数 $a_j \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$ を選択する．

$$a = \sum_{j=0}^{\ell-1} a_j 2^j \tag{6.1}$$

これらの乱数 a_j を用いて透かし情報ビット w_j のビットコミットメント com_j を計算し，それを販売者に送信する．

$$com_j = g^{w_j} h^{a_j} \pmod N \tag{6.2}$$

Step 3. 受信したコミットメントの正当性を検証するために，販売者はまず次の式を計算し，

$$V = h^a \pmod N, \tag{6.3}$$

次の方程式を満足することを確認する．

$$\prod_j {com_j}^{2^j} \stackrel{?}{=} W \cdot V \pmod N \tag{6.4}$$

Step 4. 以下の操作を $0 \leq i \leq L-1$ の間で行う．

Step 4.1 販売者は L 個の乱数 $b_i \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$ を生成し，画像の各成分 I_i を暗号化する．

$$C_i = g^{I_i} h^{b_i} \tag{6.5}$$

Step 4.2 埋め込み強度 T を定め，以下のように暗号化した画像の各成分に暗号化された透かし情報を埋め込む．ただし，T は偶数とする．

$$Y_i = \begin{cases} C_i \cdot com_j^T \pmod N & \text{埋め込み位置} \\ C_i \pmod N & \text{その他} \end{cases} \tag{6.6}$$

Step 5. 購入者が受信する Y_i は次のように書き直すことができるので

$$Y_i = \begin{cases} g^{(I_i + Tw_j)} h^{Ta_j + b_i} \pmod N & \text{埋め込み位置} \\ g^{I_i} h^{b_i} \pmod N & \text{その他} \end{cases} \tag{6.7}$$

画像の成分の内，埋め込み位置のみに透かし情報が与えられた画像が復号される．

$$D(Y_i) = \begin{cases} I_i + Tw_j \pmod p & \text{埋め込み位置} \\ I_i \pmod p & \text{その他} \end{cases} \tag{6.8}$$

埋め込み位置における復号された値は，透かし情報が $w_j = 1$ ならば，埋め込み強度 T の分だけ増加し，$w_j = 0$ ならば変化しない．以上のプロトコルを図 6.1 にまとめる．

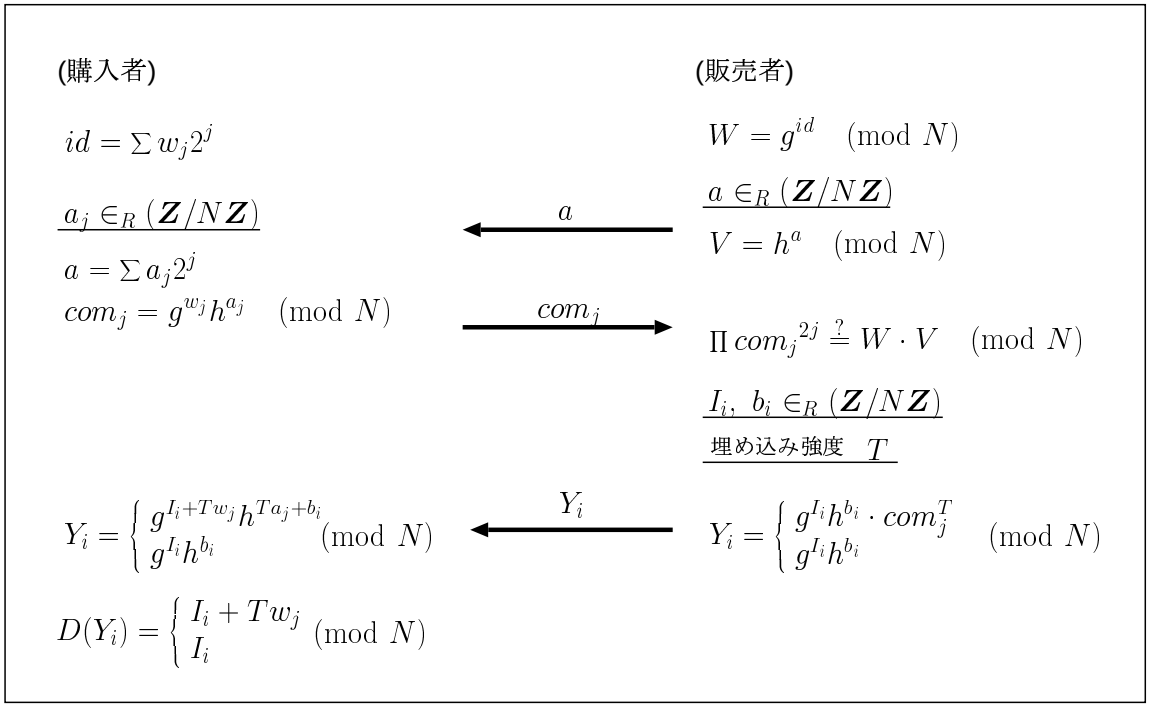


図 6.1　提案電子指紋プロトコル

Fig. 6.1　Proposed fingerprinting protocol.

ビットコミットメント com_j は，w_j をメッセージ，a_j を乱数として暗号文 $E(w_j, a_j)$ と表現できる．そのため，式 (6.6) の com_j^T は，

$$\begin{aligned} com_j^T &= (g^{w_j} h^{a_j})^T \pmod N, \\ &= g^{Tw_j} h^{Ta_j} \pmod N, \\ &= E(Tw_j, Ta_j), \end{aligned} \tag{6.9}$$

と変形できる．また，式 (6.5) の $g^{I_i} h^{b_i}$ は $E(I_i, b_i)$ と表現することができる．それゆえ，加法性の準同型写像の性質より，埋め込み位置における暗号文 Y_i は以下の式に書き換えることができる．

$$\begin{aligned} Y_i &= E(I_i, b_i) \cdot E(Tw_j, Ta_j) \\ &= E(I_i + Tw_j, Ta_j + b_i) \end{aligned} \tag{6.10}$$

画像の成分 I_i を単純に各画素とする場合には，埋め込み強度 T を埋め込み手法に応じて選択すれば実装することは簡単である．しかし，もし I_i が画像の周波数成分を示すのであれば，整数化処理などをしなければ直接暗号化することはできない．詳細に関しては 6.3 節で述べる．

6.2.2 ビットコミットメントの正当性

提案電子指紋プロトコルにおいて，購入者は自分のID情報の各ビットをビットコミットメントとして送信せずに，別の情報を送信するかもしれない．なぜなら，com_j は岡本–内山暗号の暗号文であるため，その平文が1ビットである必要はないからである．つまり，$w_j\,(0 \leq j \leq \ell-1)$ は必ず1ビットの情報であることを証明しなければ，購入者は自分が正規ユーザであることを販売者に示すことができない．悪意のある購入者ならば，式(6.4)を満たすように w_j の値を操作して送るかもしれない．最終的に販売者から送られる暗号文 Y_i を復号した場合，w_j の値が大きければ，$I_i + Tw_j$ が異常に大きな値となるため，この埋め込み位置を特定できる可能性が生じる．そこで，購入者は com_j に含まれる情報 w_j はバイナリであることを示すためのプロトコルが必要である．そのプロトコルを以下に示す．

Step 1. 販売者は com_j の正当性を調べるために，まず $t_j + c_j < 2^{k-1}$ を満たす乱数 $t_j, c_j \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$ を選択し，次に com_j に以下の操作を施す．

$$COM_j = com_j^{t_j} \cdot g^{c_j} \pmod{N} \tag{6.11}$$

Step 2. 購入者は，受信した COM_j を復号する．

$$D(COM_j) = w_j t_j + c_j \pmod{N} \tag{6.12}$$

乱数 $r_j \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$ を選択し，$w_j, a_j, COM_j, D(COM_j)$ を用いて，次の式を満たす $\widehat{com}_j$ を計算する．

$$\widehat{com}_j = com_j^{t_j+c_j} \cdot h^{r_j} \pmod{N} \tag{6.13}$$

Step 3. 販売者は，$\widehat{com}_j$ を受信した後に t_j, c_j の値を購入者に公表することで，COM_j が確かに com_j とこれらを用いて計算されたことを証明する．

Step 4. もし，t_j, c_j が式(6.11)を満たすならば，購入者は r_j を販売者に公表する．もし，満たさなければ，販売者が不正を行ったとして主張できる．

Step 5. 式.(6.13)を検証することで，販売者は com_j に含まれる w_j はバイナリであることを確信することができる．

以上のビットコミットメントの正当性を証明するプロトコルの流れを図6.2に示してある．ここで，プロトコルのStep 2において $w_j = 0$ ならば，

$$D(COM_j) = c_j, \tag{6.14}$$

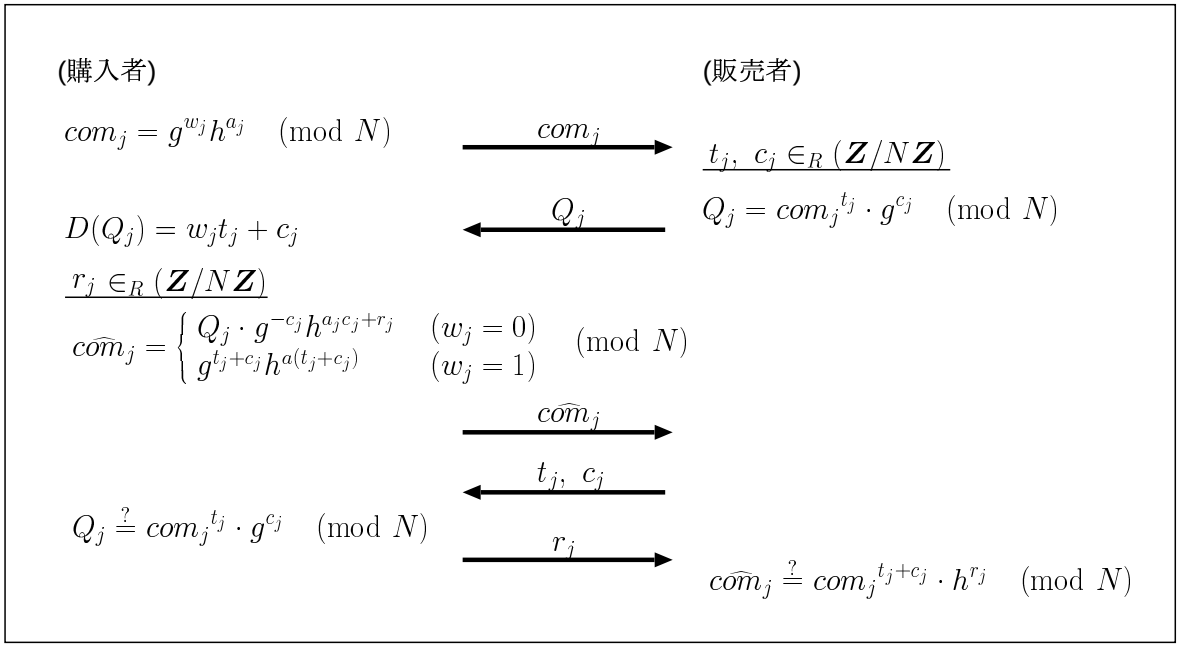


図 6.2　ビットコミットメントの正当性の証明

Fig. 6.2　Binary proof protocol.

であり,

$$COM_j = g^{c_j} h^{a_j t_j} \bmod N, \tag{6.15}$$

である．この場合，購入者は $COM_j, D(COM_j)$ を用いて次のように $\widehat{com}_j$ を計算することができる．

$$\begin{aligned} \widehat{com}_j &= COM_j \cdot g^{-D(COM_j)} h^{a_j D(COM_j) + r_j} \pmod N \\ &= g^{c_j} h^{a_j t_j} \cdot g^{-c_j} h^{a_j c_j + r_j} \pmod N \\ &= h^{a_j (t_j + c_j) + r_j} \pmod N \\ &= E(0,\, a_j (t_j + c_j) + r_j) \\ &= com_j^{t_j + c_j} \cdot h^{r_j} \end{aligned} \tag{6.16}$$

もし，$w_j = 1$ ならば,

$$D(COM_j) = t_j + c_j, \tag{6.17}$$

なので，$\widehat{com}_j$ は次の式により計算できる．

$$\begin{aligned} \widehat{com}_j &= g^{D(COM_j)} h^{a_j D(COM_j) + r_j} \pmod N \\ &= g^{t_j + c_j} h^{a_j (t_j + c_j) + r_j} \pmod N \\ &= E(t_j + c_j,\, a_j (t_j + c_j) + r_j) \\ &= com_j^{t_j + c_j} \cdot h^{r_j} \end{aligned} \tag{6.18}$$

上述の場合以外では，購入者は復号した COM_j から $\widehat{com}_j$ を作成することができないことに注意しなければならない．なぜなら，$\widehat{com}_j$ の作成には，乱数 t_j, c_j の両方の情報もしくはそれらを足し合わせた $t_j + c_j$ が不可欠であるからである．ゆえに，w_j がバイナリでなければ情報不足により $\widehat{com}_j$ を計算することはできない．以上の議論より，次に示す定理が導かれる．

定理 6.1 p 部分群仮定が成り立つならば，購入者は w_j がバイナリであることをコミットメントを用いて示すことができる．

(証明) 購入者は COM_j から $w_j t_j + c_j$ の情報は得ることができるが，t_j と c_j の両方の情報は得ることはできない．w_j がバイナリの場合を除いて，これら二つの値が分からなければ，$com_j^{t_j+c_j}$ を計算することはできない．購入者は $w_j, a_j, w_j t_j + c_j$ の値を知っているので，w_j がバイナリであれば式 (6.16)，式 (6.18) より $\widehat{com}_j$ を計算することができる．岡本–内山暗号の特徴より，乱数 r_j は暗号文 $com_j^{t_j+c_j}$ を次のようにメッセージ $w_j(t_j + c_j)$ の値自体を変えることなく別の暗号文に写像することができる．

$$com_j^{t_j+c_j} \cdot h^{r_j} = E(w_j(t_j + c_j),\, a_j(t_j + c_j) + r_j) \tag{6.19}$$

この写像により，透かし情報 w_j に関する情報は販売者に全く洩れないことを保証することができる．なぜなら，販売者は暗号文 $E(0,\, a_j(t_j + c_j) + r_j)$ と暗号文 $E(t_j + c_j,\, a_j(t_j + c_j) + r_j)$ を区別することができないからである．購入者が r_j の値を公表すれば，販売者は式 (6.13) を検証することで w_j がバイナリであることを確信できる．しかし，それ以上の情報は何も得られない．更に，販売者は Step 2 において購入者を騙すことは難しい．なぜなら後で t_j, c_j の値を公表しなければならないからである．ゆえに，$\widehat{com}_j, COM_j$ もまたコミットメントとしての役割を果している．これらコミットメントを解読するには p 部分群仮定が成立するならば，極めて困難である． (証明終)

6.2.3 安全性

まず，販売者に関する安全性を考える．電子指紋プロトコルにおいて，定理 6.1 により購入者は w_j がバイナリであることを示すことができるため，販売者は購入者が正規ユーザであり正当なコミットメント com_j を送信していることを確認できる．それゆえ，購入者が行う攻撃は，埋め込まれている透かし情報 id を埋め込み画像から改ざんもしくは消去することが考えられる．このことから次の定理が導かれる．

定理 6.2 用いる電子透かし法が攻撃に対して耐性があり，p 部分群仮定が正しいならば，販売者に関する安全性は保証される．

残念ながら，攻撃に対して完全な耐性を持つ電子透かし法は存在しない．電子透かし技術では，ある基準の画質までならば埋め込まれた透かし情報を正しく検出できることを保証することしかできない．もし，画質劣化がある基準を下回るときには，正しく検出できない可能性がある．しかしながら，電子透かし技術の攻撃に対する耐性向上は電子指紋技術においては重要な要素である．

次に，購入者に関する安全性を考えるためには，販売者が購入者の ID 情報である透かし情報を得ることができないことを示さなければならない．そのために，次に示す三つの条件を仮定する．

A1　離散対数問題を解くことは困難である．

A2　岡本–内山暗号は安全である．

A3　購入者は不正コピーを配布しない．

これらの三つの仮定の下，以下の定理を導くことができる．

定理 6.3 仮定 *A1*，*A2*，*A3* が成り立つならば，購入者は販売者から匿名でディジタル画像を購入することができる．

(証明)　$W = g^{id} \bmod N$ なので，W から直接 id を求めることは離散対数問題を解くことと等価であり，これは仮定 A1 より難しい．電子指紋プロトコルの Step 2 において，ビットコミットメント com_j はその性質上，$E(0, r)$ か $E(1, r)$ のどちらかである．ここで，岡本–内山暗号が安全であると仮定すれば，p 部分群仮定も成立することを意味する．それゆえ，販売者が com_j から w_j の値を解析することは困難である．もし，購入者の ID 情報 id が埋め込まれた画像を手に入れることができれば，販売者は電子透かしの検出操作により id を得ることができる．しかし，提案手法ではプロトコル終了後に購入者の id が埋め込まれた画像を持っているのは購入者だけであるため，購入者が不正コピーを流出させない限り販売者は購入者の id を手に入れることはできない．　(証明終)

定理 6.3 より，購入者の匿名性は保証されるため，販売者は購入者の id を悪用することはできない．ゆえに，購入者の安全性は保証される．

電子指紋技術においては，複数の購入者間の結託により埋め込まれた電子指紋を消去もしくは改ざんされる恐れがある．このような攻撃に対する対策として，結託耐性符号 [34][35] が提案されている．しかし，符号長が非常に長いため，現時点では直接適用することはできない．今後，電子指紋プロトコルに適用可能な結託耐性符号を考案することが必要不可欠である．

6.3　電子指紋プロトコルの実装法

6.3.1　埋め込み

電子指紋技術の非対称方式では，暗号化された情報ビットを暗号化された画像に埋め込むために，公開鍵暗号の準同型写像の性質が用いられる．提案手法でも，岡本–内山暗号の加法性の準同型写像の性質を用いて埋め込み操作を行う．3 章，4 章で述べたように，画像に透かし情報を埋め込むには周波数成分に埋め込む方が一般に耐性が高い．しかし，画像の周波数成分を求める際には実数値計算が伴うため，整数しか扱うことのできない暗号方式に直接適用することができない．そのため，実数値を整数化する処理が必要になる．その際に，量子化法による電子透かしの埋め込み操作を扱うことができる．

量子化操作において，周波数成分は最も近い整数値に量子化される．その際，透かし情報ビットを埋め込むために，複数の周波数成分を秘密情報により選出し，その成分は特別な量子化ステップを用いて量子化させる．しかしながら，電子指紋プロトコルでは，透かし情報ビットが暗号化された状態で埋め込み操作を行わなければならない．ここで，販売者は透かし情報ビット自体が分からないため，単純に量子化法を適用することができない．量子化法では，透かし情報ビットが $w_j = 0$ ならば，周波数成分を最も近い偶数値に，$w_j = 1$ ならば奇数値にしなければならないが，この場合その判別ができない．このことを図 6.3 に示す．

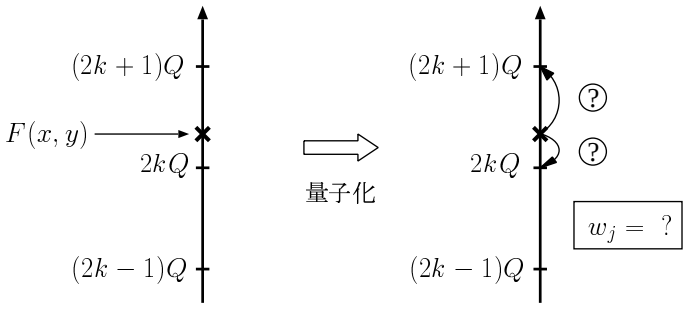


図 6.3　暗号化された情報埋め込みの問題点

Fig. 6.3　Problem to embed an encrypted fingerprint.

本節では，透かし情報ビットの値を知ることなく画像に埋め込むことができる簡単な一手法を提案する．本手法は，他の量子化法による埋め込みに簡単に拡張することが可能である．まず，周波数成分 $F(x, y)$ を量子化ステップ $Q(x, y)$ において最も近い偶数値に量子化する．

$$\overline{F(x, y)} = int_e(F(x, y)/Q(x, y)) \tag{6.20}$$

ただし，$int_e(\cdot)$ は最も近い偶数値を出力する関数とする．ここで，元の周波数成分の値 $F(x, y)$ に応じて埋め込み操作を二つの場合に分ける必要がある．もし，$F(x, y)$ がそれを量子化した

値 $\overline{F(x,y)}$ よりも小さいならば，$\overline{F(x,y)}+w_j,(w_j=1)$ は最も近い奇数値ではない．それゆえ，周波数成分の値に応じて次のように二つの場合に分ける．

Case1. もし $F(x,y)$ が量子化した値よりも大きいならば，

$$E(\overline{F(x,y)},b_i)\cdot E(w_j,a_j)=E(\overline{F(x,y)}+w_j,b_i+a_j)\pmod N. \tag{6.21}$$

Case2. 量子化した値よりも小さければ，

$$E(\overline{F(x,y)},b_i)\cdot E(w_j,a_j)^{-1}=E(\overline{F(x,y)}-w_j,b_i-a_j)\pmod N. \tag{6.22}$$

以上の式を計算することで，量子化された周波数成分の値は $w_j=0$ ならば偶数値となり，$w_j=1$ ならば奇数値となる．それゆえ，透かし情報ビットの値が分からなくても，画像の中に埋め込むことができる．また，特定の周波数成分だけを秘密情報により選出して上述の埋め込み操作を行えば，購入者が埋め込み画像から透かし情報を意図的に改ざんするような攻撃を難しくすることができる．

電子指紋プロトコルの Step 4 において，販売者は次に示す操作により暗号化された透かし情報を埋め込むことができる．

Step 1. 画像を 16×16 画素のブロックに分割し，各ブロックに DCT を施す．

Step 2. 販売者の秘密情報を用いて複数の DCT 係数を選出し，量子化ステップ $Q(x,y)$ により，最も近い偶数値に量子化する．

$$\overline{F(x,y)}=int_e(F(x,y)/Q(x,y)) \tag{6.23}$$

他の DCT 係数は，最も近い整数値に量子化する．

$$\overline{F(x,y)}=int(F(x,y)) \tag{6.24}$$

Step 3. 各量子化された DCT 係数 $\overline{F(x,y)}$ を購入者の公開鍵と乱数 b_i を用いて暗号化する．その暗号文は $E(\overline{F(x,y)},b_i)$ となる．

Step 4. 秘密情報により選出された DCT 係数に各透かし情報ビットを次のような場合に分けて埋め込む．

- もし $F(x,y) \geq \overline{F(x,y)}Q(x,y)$ ならば，埋め込みされた DCT 係数 $F'(x,y)$ の暗号文は次のように計算される．

$$\begin{aligned} E(F'(x,y),r') &= \Big(E(\overline{F(x,y)},b_i)\cdot E(w_j,a_j)\Big)^{Q(x,y)} \\ &= \Big(E(\overline{F(x,y)}+w_j,b_i+a_j)\Big)^{Q(x,y)} \\ &= E((\overline{F(x,y)}+w_j)Q(x,y),(b_i+a_j)Q(x,y)) \end{aligned} \tag{6.25}$$

- もし $F(x,y) < \overline{F(x,y)}Q(x,y)$ ならば，次の式により求められる．

$$\begin{aligned} E(F'(x,y),r') &= \Big(E(\overline{F(x,y)},b_i)\cdot E(w_j,a_j)^{-1}\Big)^{Q(x,y)} \\ &= \Big(E(\overline{F(x,y)}-w_j,b_i-a_j)\Big)^{Q(x,y)} \\ &= E((\overline{F(x,y)}-w_j)Q(x,y),(b_i-a_j)Q(x,y)) \end{aligned} \tag{6.26}$$

Step 5. 透かし情報の埋め込まれた画像の暗号文を購入者に送信する．

購入者は暗号文を受け取ると，まず復号し，そして IDCT を施すことで埋め込み画像を得る．ここで，攻撃に対する耐性を向上させるため，埋め込み位置は高周波成分を避けるべきである．なぜなら一般に使用される画像信号の処理操作により高周波成分は影響を受けやすいからである．また，各透かし情報ビットを埋め込む際に，複数の係数に分散させてその信号を埋め込むことにより耐性を向上させることができるため，上述の埋め込み操作で各透かし情報ビットを μ 個の DCT 係数に埋め込む．

6.3.2 量子化テーブル

透かし情報を画像に埋め込む際には，画質劣化を考慮しなければならない．提案手法では，画像を周波数領域に変換し，その成分を量子化することで埋め込みを行っている．ここで，量子化が一様に行われた場合，画像の特徴を活用することができないため，適応的な埋め込みはできない．そこで，画像の周波数成分を量子化する際に人間の視覚特性に基づいて作成された JPEG 圧縮の量子化テーブルに着目する．このテーブルに基づいて量子化を行えば，画質を著しく劣化させることなく最適な処理が行えるため，透かし情報の埋め込みにも適していると考えられる．ただし，このテーブルのサイズは 8×8 であるため，攻撃に対する耐性に関してはあまり適していない．更に広い範囲に拡散させて埋め込む方が耐性は向上すると考えられるため，このテーブルを基本として 16×16 のサイズに拡張させる．

元の量子化テーブルを $q(x,y), (0 \leq x, y \leq 7)$ とする．まず，x 方向に対して以下のように拡張させる．

$$b(x,y) = \begin{cases} q(x, \frac{y}{2}) & (y\text{=}0,\ 2,\ 4,\ \ldots,\ 14) \\ \dfrac{q(x, \frac{y}{2}) + q(x, \frac{y}{2}+1)}{2} & (y\text{=}1,\ 3,\ 5,\ \ldots,\ 13) \\ q(x,7) & (y\text{=}15) \end{cases} \tag{6.27}$$

次に，x 方向に拡張されたテーブルを y 方向に拡張させる．

$$Q(x,y) = \begin{cases} b(\frac{x}{2}, y) & (x\text{=}0,\ 2,\ 4,\ \ldots,\ 14) \\ \dfrac{b(\frac{x}{2}, y) + b(\frac{x}{2}+1, y)}{2} & (x\text{=}1,\ 3,\ 5,\ \ldots,\ 13) \\ b(15,y) & (x\text{=}15) \end{cases} \tag{6.28}$$

ただし，小数点以下の値は切り捨てる．

画像を JPEG 圧縮する際には，画質パラメータを設定することで圧縮率を可変にすることができる．実際に量子化するステップのサイズを量子化テーブルからこのパラメータに基づいて計算される．上述の通り拡張させた量子化テーブルにおいても同様の操作を適用させる．埋め込み強度を画質パラメータ T_q として，上記の操作を以下に示す．

$$Q'(x,y) = \frac{(100 - T_q)}{50} Q(x,y), \quad (50 \leq T_q \leq 100) \tag{6.29}$$

JPEG 圧縮において画質パラメータが減少すれば，画質が劣化するように，提案手法においても T_q が減少すれば強く透かし信号を埋め込むことになり画質は劣化する．ここで，画質と攻撃に対する耐性はトレードオフの関係にあることに注意して T_q の値を設定しなければならない．

6.3.3 検出

透かし情報は，特定の DCT 係数を偶数値もしくは奇数値に量子化して埋め込まれるので，検出操作は秘密情報さえあれば簡単に行うことができる．もし，販売者が不正コピーを発見した際には，以下の手順により不正者を特定する．

Step 1. 画像をブロックに分割し，各ブロックに DCT を施す．

Step 2. 埋め込み位置の DCT 係数を対応する量子化ステップ $Q'(x,y)$ で量子化する．

Step 3. 量子化した DCT 係数 μ 個の内，偶数となるものが奇数となるものよりも多く存在するならば $w_j = 0$，少なければ $w_j = 1$ と判定する．

一般に量子化されたDCT係数の値は，IDCTを施し輝度領域に変換した際に生じる丸め誤差の影響を受けるため，攻撃を受けなくても変化してしまう．圧縮やフィルタリングなどの信号処理が施されれば，その値は更に変化する．これらの変化はそれほど大きくないと考えられるため，DCT係数の値自体は量子化して偶奇を判定するだけよりも，変化分を考慮してその係数値を判定に活用すれば，検出率を向上させることができる．

6.3.4 考察

提案手法では，画像の信号処理操作に対する耐性を考慮するために，低周波成分のDCT係数μ個に透かし情報ビットw_jの信号エネルギーを拡散させて埋め込んでいる．多くの埋め込み位置に透かし情報を埋め込むため，解析されやすいように思えるが，反対に安全性は高まっている．その理由を以下に示す．画像のエネルギーは低周波成分に集中するため，低周波成分のDCT係数は大きな値を持つ．また，それらの値はランダムな値とみなすことができる．そのような係数値をある量子化ステップ$Q'(x,y)$で量子化した場合，その値もまたランダムな振る舞いをするとみなすことができる．それゆえ，透かし情報の埋め込まれた係数と他の係数との判別は難しい．ここで，透かし情報ビットが一つのDCT係数に埋め込まれる場合は，攻撃者はいくつかのDCT係数値を変化させることで透かし情報を改ざんできるかもしれない．しかし，その可能性は多くのDCT係数に拡散させて透かし情報ビットを埋め込むことで低く抑えることができる．提案手法の場合，少なくとも$\mu/2$個のDCT係数値を画質を著しく劣化させることなく改ざんしなければならないため，成功する可能性は極めて低い．

電子透かし法を評価するためには，幾何学的な改変に対する耐性を考慮しなければならない．一つの解決策として5章で述べたように同期信号を埋め込む方式が考えられる．同期信号の埋め込み操作は，電子指紋の埋め込み操作とは独立に行うことができるため，簡単に導入できる．なぜなら，販売者は電子指紋の埋め込みの前処理として画像を暗号化する前に同期信号の埋め込みを行えるからである．この場合，不正コピーから不正者を特定するには，まず同期信号を検出し，幾何学的な歪みを補正した後に，透かし情報の抽出を行うことができる．

6.4 計算機シミュレーション

提案方式の有効性を示すために計算機シミュレーションを行う．電子指紋プロトコルに関しては，岡本–内山暗号の安全性と使用する電子透かし技術に依存することは定理6.2，定理6.3で説明した．特に電子透かし技術の攻撃耐性が重要であるため，ここでは提案した電子透かし法の攻撃に対する耐性と画質劣化の関係に関して調べる．シミュレーションには256×256画素，256階調の白黒濃淡画像 “lena” を用いる．カラー画像への拡張は，RGB表示形から

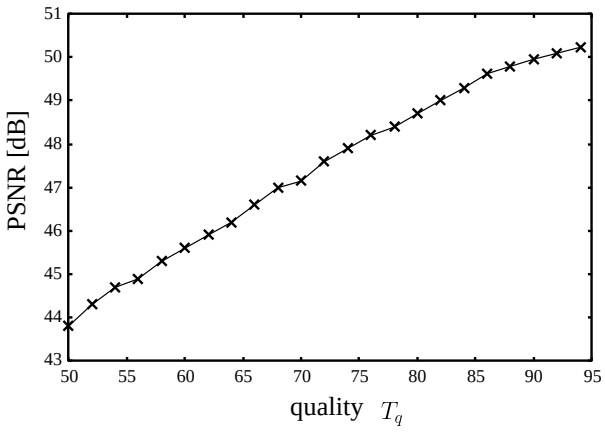


図 6.4　埋め込み強度 T_q に対する PSNR ($\mu = 75$)
Fig. 6.4　PSNR versus quality parameter T_q ($\mu = 75$).

YC_rC_b 表示形に変換してその輝度領域に提案手法を適用すればよい．攻撃に対する耐性を考慮すると μ の値は大きく設定する必要がある．しかし，あまり大きいと埋め込み位置候補の数が少なくなってしまうので，今回は $\mu = 75$ でシミュレーションを行う．

埋め込み強度 T_q の値が減少するに従って，画質も劣化する．初めに，提案手法の画質を評価するために図 6.4 に T_w と PSNR の関係を示す．埋め込み強度 T_q が減少すれば画質は劣化するが，攻撃に対する耐性は反対に向上する．これらにはトレードオフの関係があるため，実装する際にはシステム設計の段階でこの関係を考慮しなければならない．シミュレーションでは，埋め込み強度の値を $55 \leq T_q \leq 75$ として攻撃耐性を評価する．図 6.5 に原画像を，図 6.6 に $T_q = 55$ とした場合の埋め込み画像を示す．

幾何学的な改変に関しては，同期信号の埋め込みを前もって行うことである程度耐性を向上させることが可能であると考えられる．ゆえに，ここでは非幾何学的な改変に関する耐性評価だけを行う．図 6.7 に JPEG により高圧縮を施した際に透かし情報が度正しく検出できる割合を調べた結果を示す．この結果より，埋め込み強度 T_q を下げることにより耐性が向上することが分かる．ガウシアンフィルタ，メディアンフィルタに対する耐性に関しては，埋め込み強度が $55 \leq T_q \leq 75$ の範囲において 1 ビットの誤りなく正しく検出することができた．これらの結果より，提案手法は攻撃に対する耐性は高いと考えられる．

以上で述べた電子透かし法は，量子化法に基づく手法を拡張させた手法である．第 3 章，第 4 章で提案した電子透かし法においても量子化法による埋め込みが可能であるため，本節で提案した手法をこれらにも拡張させて使用することが可能である．

図 6.5　原画像

Fig. 6.5　Original Image.

図 6.6　埋め込み画像 (PSNR=44.5[dB])

Fig. 6.6　Fingerprinted Image (PSNR=44.5[dB]).

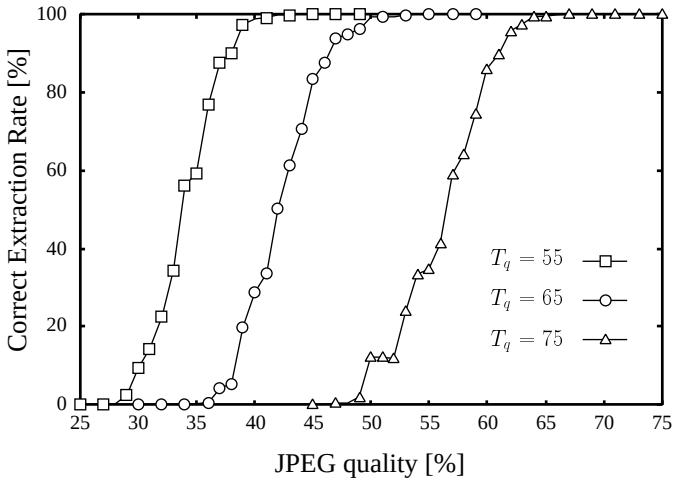


図 6.7　JPEG 圧縮に対する耐性

Fig. 6.7　Tolerance for JPEG Compression.

6.5 暗号化率の改善法

6.5.1 修正電子指紋プロトコル

提案電子指紋プロトコルでは，画像の各成分 I_i が暗号化され，加法性の準同形写像の性質に基づいて電子指紋が埋め込まれる．ここで，岡本–内山暗号のメッセージサイズを考えると，I_i の値ははるかに小さい．岡本–内山暗号の暗号化率は 1/3 であるが，電子指紋プロトコルにおいて I_i ごとに暗号文を作成するならば，その暗号化率は著しく低くなる．そこで，メッセージ空間を最大限活用して暗号化率を向上する手法を提案する．

埋め込み処理後の画像の i 番目の成分 m_i をする．

$$m_i = \begin{cases} I_i + w_j & \text{埋め込み位置} \\ I_i & \text{その他} \end{cases} \tag{6.30}$$

m_i のサイズを s ビットとすると，メッセージサイズ k ビットに対してはるかに小さい．そこで，m_i を複数まとめて k ビットの $M_{i'}$ を次のように作成する．

$$M_{i'} = \sum_{t=0}^{c-1} m_{i'c+t} 2^{st}, \quad 0 \le i' \le L/c - 1 \tag{6.31}$$

ただし，

$$c = \left\lceil \frac{k}{s} \right\rceil, \tag{6.32}$$

とする．この際のメッセージ空間の使用状況を図 6.8 に示す．もし販売者が $M_{i'}$ の暗号文を com_j と I_i を用いて作成できるならば，暗号化率を理論上 1/3 まで改善することができる．以上の操作を行うために，電子指紋プロトコルの Step 4 と Step 5 を次のように修正する．

Step 4. 販売者は，受信した com_j と画像の成分 I_i を用いて次式で示す y_i を計算する．

$$y_i \quad = \quad \begin{cases} g^{I_i} \cdot com_j \pmod N & \text{埋め込み位置} \\ g^{I_i} \pmod N & \text{その他} \end{cases} \tag{6.33}$$

複数の y_i をまとめて一つの暗号文 $Y_{i'}$ を生成するために，乱数 $b_{i'} \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$ を用いて次の計算を行う．

$$Y_{i'} = \Big(\prod_t (y_{i'c+t})^{2^{st}} \Big) \cdot h^{b_{i'}} \pmod N \tag{6.34}$$

Step 5. 購入者は受信した $Y_{i'}$ を復号し，$M_{i'}$ を得る．ここで，購入者が m_i のビット長 s を知っていれば，$M_{i'}$ を m_i に分割することができ，最終的に電子指紋の埋め込まれた画像を得ることができる．

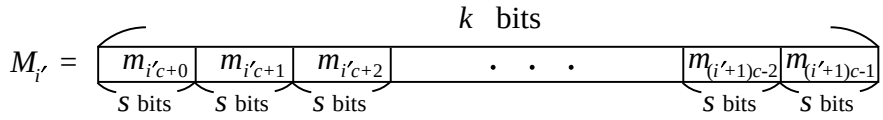


図 6.8　メッセージの構成

Fig. 6.8　Composition of the message $M_{i'}$.

式 (6.30) から式 (6.33) と岡本–内山暗号の性質 P3 により，式 (6.34) の変形は次のように示される．

$$\begin{aligned} Y_{i'} &= \Big(\prod_t g^{m_{i'c+t}2^{2^{st}}}\Big) \cdot h^r \pmod N \\ &= g^{\sum m_{i'c+t}2^{2^{st}}} h^r \pmod N \\ &= g^{M_{i'}} h^r \pmod N \\ &= E(M_{i'}, r) \end{aligned} \tag{6.35}$$

ゆえに，販売者は $M_{i'}$ の暗号文を com_j と I_i を用いて作成できることが示された．

6.5.2　安全性

修正手法においてその安全性を考察するには修正を加えた Step 4 と Step 5 だけに関して議論すればよい．初めに，$Y_{i'}$ とそのデータ構造について考える．もし岡本–内山暗号が安全であり，$M_{i'}$ のビット長が k 以下であれば，購入者は $Y_{i'} = E(M_{i'}, r)$ を正しく復号することができる．式 (6.34) と式 (6.35) より，$M_{i'}$ を構成する複数の $m_{i'c+t}$ は一つの暗号文として処理されている．そのため，$M_{i'}$ は式 (6.31) を満たすように作成されなければならない．もし，販売者が少しでも式 (6.31) に変更を加えたならば，購入者は正しい $m_{i'c+t}$ を復号できないため，販売者の不正を主張することができる．また，$M_{i'}$ は単純に $m_{i'c+t}$ にシフト操作を行ってまとめただけなので，購入者は原画像に関する情報は $M_{i'}$ から得ることはできない．

6.5.3　暗号化率の比較

提案手法が実用的であることを示すために，暗号化率に関して従来法と比較を行う．埋め込む電子指紋は ℓ ビットとし，画像の周波数成分に埋め込むことを想定する．ただし，画像は L 個の周波数成分により表現され，各成分のサイズは s ビットとすると仮定する．ここで，$\ell \ll L$ が成り立つと考えられるのため，電子指紋の埋め込まれた画像とその暗号文に関する評価だけを行う．この場合，送信する平文データのサイズは sL となる．比較をする際の便宜上，6.2 節の手法を提案方式 I とし，本節で述べた修正手法を方式 II と呼ぶことにする．

表 6.1　暗号化率

Table 6.1　Enciphering rate

Pfitzmann らの方式	提案方式 I	提案方式 II
$1/3k$	$s/3k$	$1/3$

Pfitzmann らによる方式 [19][20] では，平方剰余に基づくビットコミットメントを扱っており，法 n は二つの大きな素数の積である．そのため，平文のサイズは必ず 1 ビットであり，その暗号文は $\log_2 n$ ビットとなるため，暗号化率は $1/\log_2 n$ となる．一方提案手法では，岡本–内山暗号を用いており，法は $N = p^2q$ でありそのサイズは $3k$ ビットである．提案方式 I では，画像の周波数成分ごとに暗号化，埋め込み操作を行うことができるため，L 個の周波数成分がそれぞれ $\log_2 N = 3k$ ビットの暗号文となるため，合計 $3kL$ ビットのデータを送信しなければならない．ゆえに，暗号化率は $sL/3kL = s/3k$ となる．提案方式 II では，複数の周波数成分をまとめて一つの暗号文として扱うことができるため，更に暗号化率が向上する．式 (6.32) より，$M_{i'}$ には最大 L/c 個の周波数成分をまとめることができるため，送信するデータの合計は $(L\log_2 N)/c(\simeq 3sL)$ となる．ここで $\log_2 n \simeq \log_2 N = 3k$ が成立する場合の暗号化率の比較を表 6.1 に示す．もし，代数学的構造が岡本–内山暗号と類似する Paillier 暗号 [36] を用いれば，暗号化率は理論上最大で 1/2 まで向上させることができる．

暗号化率を更に向上させる方法として，埋め込み位置を制限する方法が考えられる．例えば，画像の性質より高周波成分への埋め込みは攻撃に対する耐性を考慮すれば，避けた方がよい．そのため，高周波成分は暗号化するより圧縮符号化することで，送信するデータ量の削減に貢献させる方が望ましい．ただし，圧縮符号化して送信する周波数成分の選択には注意が必要である．なぜならば，多くの周波数成分を圧縮して送信すれば，電子指紋を埋め込む周波数成分の候補が少なくなるため，解析される恐れが高くなるからである．ゆえに，埋め込み位置を制限し，一部の周波数成分を圧縮符号化して送信する手法を用いる場合，送信するデータ量と安全性トレードオフの関係を考慮しなければならない．

6.6　結言

本章では，岡本–内山暗号を利用した新しい匿名方式の電子指紋プロトコルを提案した．加法性の準同型写像の性質を用いて，暗号化された電子指紋を暗号化された画像に埋め込むプロトコルを提案した．また，購入者が不正を行わないように暗号化された電子指紋の正当性を示すためのプロトコルも提案した．提案手法の安全性は，岡本–内山暗号の安全性と用いる電子透かし法の攻撃耐性に依存している．提案電子指紋プロトコルで適用可能な電子透かし法

として量子化法を取り上げ，画質劣化を抑えつつ攻撃耐性の高い方式を提案した．提案手法では量子化法の拡張として電子透かし技術を扱っているため，第 3 章，第 4 章で提案した手法にも拡張させることが可能である．更に，実用的な方式とするために暗号化率の改善を図った．従来方式では，極めて効率の悪い暗号化操作を行っていたが，提案手法を用いれば効率良く暗号化操作が行えることを示した．

第7章　結論

本論文では，ディジタル情報に別の情報を知覚されないように埋め込むことができる電子透かし技術に着目し，ディジタル画像や動画などのコンテンツの著作権保護を目的として，四つのテーマについて研究を行った．それらは，DCT 係数の加法特性を利用した電子透かし (第 3 章)，画像の局所情報に基づく電子透かし (第 4 章)，埋め込み信号間の距離に基づく電子透かし (第 5 章)，加法性準同型写像の性質を用いた効率の良い電子指紋プロトコル (第 6 章) である．

第 3 章では，人間の視覚特性に基づいて，ディジタル画像の低周波成分に透かし情報を埋め込む手法を提案した．画像の低周波成分への埋め込みを行うと一般にブロック歪みが生じるが，提案手法では DCT 係数間の加法特性を利用することで，ブロック歪みを抑えることができた．特定の 4 個の DCT 係数に与えた透かし信号エネルギーは，ブロック内の中央領域付近に緩やかな曲線を描いた模様として現れ，ブロックの端ではその振幅がほとんど変化しないことを示した．そのため，ブロック歪みが抑えられ，知覚されにくい信号として埋め込まれていることが分かった．また，DCT 係数間の加法特性により埋め込まれた透かし信号が，ブロックの中心付近のサブブロックからも検出できるため，検出に要する計算量を抑えることができた．微小な回転，拡大縮小，平行移動などの幾何学的な改変に対して，同期を回復するための処理手法を提案した．幾何学的な改変により生じる同期のずれは，計算機シミュレーションにより元の座標の周囲 6 画素程度であることが分かった．

第 4 章では，画像の有する局所的な情報に基づいて，適応的に透かし情報を埋め込む手法を提案した．変化の少ない平坦な領域に加わった雑音信号は知覚されやすいが，変化の激しい領域は人間の視覚特性上，雑音による影響が知覚されにくい．この特性に基づいて，画像の平坦な領域と複雑な模様の領域を分類し，透かし信号を複雑な模様に変調させてその領域に適した信号とすることで，局所的に適応的な埋め込みが可能となった．また，第 3 章で提案した同期回復手法を検出の際に適用したことで，幾何学的な改変に対しても耐性を有する方式であることをシミュレーションにより確認した．

第 5 章では，動画像に適用可能な電子透かし手法とするために，計算量が比較的少ないパッチワーク法による新しい埋め込み手法を提案した．幾何学的な改変を考慮して同期信号を埋め込む手法に改良を加えて，同期信号の位置関係を変化させて埋め込みを行った．また，第 3 章のシミュレーションにより同期のずれが周囲 6 画素程度であることが確認されたので，この事実に基づいて埋め込み位置を設定した．提案手法は，信号処理の分野におけるパルス位置変調の概念を電子透かしの分野に適用させた斬新な手法である．電子透かしの研究において，透かし情報を埋め込むことのできる新しい領域を示した点は，この分野の発展に大きく貢献す

る方式である．

第 6 章では，暗号技術を用いて電子透かし技術を応用させた電子指紋技術を実用的な技術へと前進させる一手法を提案した．購入者と販売者との取り引き終了後，購入者だけが電子指紋の埋め込まれたコンテンツを得るために，岡本–内山暗号の加法性準同型写像の性質を利用した．この手法を用いれば，暗号化された透かし情報を暗号化されたコンテンツに埋め込むことが可能となり，プロトコルの正当性も検証できることを確認した．また，量子化法による電子透かし手法を拡張させれば，このプロトコルに適用することが容易であることを示した．第 3 章，第 4 章の手法においても量子化法を基本として拡張しているため，提案プロトコルに適用が可能である．

以上のように本論文では，電子透かし技術を用いて著作権侵害問題を解決するために必要となる障壁を乗り越えるための手法を提案した．ディジタル情報の品質をあまり劣化させずに別の情報を埋め込むために，人間の視覚特性及び画像自体の特徴を利用した．また，品質だけでなく各種の攻撃に対する耐性向上を考慮した手法を提案した．比較的少ない計算量で処理できるだけでなく，新しい埋め込み可能な領域の存在を示す手法も提案した．更には，ネットワーク上での売買において，販売者と購入者の両方の権利を守ることができる手法を提案した．この手法では，取り引きに必要な通信量を削減することで，実用的な技術へと進歩させた．以上のことをまとめると，本論文で提案した各研究テーマにおける研究成果は，電子透かし技術を用いたディジタル情報の著作権保護に貢献し得ると考えられる．

謝　辞

本研究の機会を与えて頂いた神戸大学工学部電気電子工学科 田中初一教授には，熱心な御指導と貴重な御助言を賜わりました．ここに謹んで感謝の意を表します．

本研究をまとめるにあたり貴重な御教示と多くの御助言を頂きました神戸大学工学部情報知能工学科 上原邦昭教授に深く感謝致します．

本研究を論文としてまとめるにあたって貴重な御教示と御助言を頂きした神戸大学工学部電気電子工学科 増田澄男教授に深く感謝致します．

本研究を推進するために必要となる計算機環境を整えて頂きました神戸大学工学部電気電子工学科 桑門秀典助教授に心より感謝致します．日頃から研究における様々な便宜を図ってくださいました神戸大学工学部電気電子工学科 原田和男技官に深く感謝致します．更に，本研究を進めるにあたって暖かい励まし，御助言を頂いた神戸大学工学部電気電子工学科通信情報工学研究室の諸氏に心より感謝致します．

参考文献

[1] S. Katzenbeisser and F. A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*, Artech House Publishers, MA, 2000.

[2] 谷萩隆嗣，音声と画像のディジタル信号処理，コロナ社，1996.

[3] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol.6, no.12, pp.1673-1687, 1997.

[4] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. of IEEE*, vol.86, no.6, pp.1064-1087, 1998.

[5] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. of IEEE*, vol.87, no.7, pp.1079-1107, 1999.

[6] N. R. Wagner, "Fingerprinting," *IEEE Symposium on Security and Privacy*, pp.18-22, 1983.

[7] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," *Proc. of EUROCRYPT'98*, LNCS 1403, Springer-Verlag, pp.308-318, 1998.

[8] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol.35, no.3-4, pp.313-336, 1996.

[9] I. Echizen, H. Yoshiura, T. Arai, H. Kimura, and T. Takeuchi, "General quality maintenance module for motion picture watermarking," *IEEE Trans.Consumer Electronics*, vol.45, no.4, pp.1150-1158, 1999.

[10] J. S. Lim: *Two-dimensional signal and image processing*, Prentice-hall international, Inc, 1990.

[11] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," *Proc. of IH'98*, LNCS 1525, Springer-verlag, pp.218-238, 1998.

[12] M. Kutter and F. A. P. Petitocolas, "A fair benchmark for image watermarking systems," *Proc. of SPIE*, vol.3657, pp.226-239, 1998.

[13] F. A. P. Petitcolas and R. J. Anderson, "Evaluation of copyright marking systems," *Proc. of IEEE Multimedia Systems'99*, vol.1, pp.574-579, 1999.

[14] J. J.K. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking" *Signal Processing*, vol.66, no.3, pp.303-317, 1998.

[15] C. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller and Y. M. Lui, "Rotation, scale, and translation resilient public watermarking for images" *Proc. of SPIE*, vol.3971, pp.90-98, 2000.

[16] A. Kusanagi and H. Imai, "An image correction scheme for video watermarking extraction," *IEICE Trans. Fundamentals.*, vol.E84-A, no.1, pp.273-280, 2001.

[17] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," *Proc. of EUROCRYPT'96*, LNCS 1070, Springer-Verlag, pp.84-95, 1996.

[18] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," *Proc. of EUROCRYPT'97*, LNCS 1233, Springer-Verlag, pp.88-102, 1997.

[19] B. Pfitzmann and A. Sadeghi, "Coin-based anonymous fingerprinting," *Proc. of EUROCRYPT'99*, LNCS 1592, Springer-Verlag, pp.150-164, 1999.

[20] B. Pfitzmann and A. Sadeghi, "Anonymous fingerprinting with direct non-repudiation," *Proc. of ASIACRYPT2000*, LNCS 1976, Springer-Verlag, pp.401-414, 2000.

[21] G. Brassard, D. Chaum and C. Crepeau, "Minimum disclosure proofs of knowledge," *Journal of Computer and System Sciences*, vol.37, pp.156-189, 1988.

[22] 石塚裕一，酒井康行，櫻井幸一, "錯視に基づく新しい電子透かし方式の提案," 第 20 回情報理論とその応用シンポジウム, pp.65-68, 1997.

[23] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Processing*, vol.10, no.4, pp.643-649, 2001.

[24] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Commu. ACM*, vol.21, no.2, pp.120-126, 1978.

[25] M. Kim, J. Kim, and K. Kim, "Anonymous fingerprinting as secure as the bilinear diffie-hellman assumption," *Proc. of ICICS2002*, LNCS 2513, Springer-Verlag, pp.97-108, 2002.

[26] H. S. Ju, H. J. Kim, D. H. Lee, and J. I. Lim, "An anonymous buyer-seller watermarking protocol with anonymity control," *Proc. of ICISC2002*, LNCS 2587, Springer-Verlag, pp.421-432, 2003.

[27] J. G. Choi, K. Sakurai, and J. H. Park, "Does it need trusted third party? Design of buyer-seller watermarking protocol without trusted third party," *Proc. of ACNS2003*, LNCS 2846, Springer-Verlag, pp.265-279, 2003.

[28] M. Kutter, S. K. Bhattacharjee and T. Ebrahimi, "Toword second generation watermarking schemes" *Proc. of ICIP'99*, vol.1, pp.320-323, 1999.

[29] J. Tanimoto, M. Iwata and A. Shiozaki, “An improvement of watermark robustness against StirMark utilizing average brightness in local areas” *Proc. of SCIS2000-C07*, 2000.

[30] M. Iwata, A. Shiozaki and J. Tanimoto, “Improvement of watermark robustness against affine transform” *Proc. of SCIS2000-C08*, 2000.

[31] Z. Duric, N. F. Johnson, and S. Jajodia, “Recovering watermarks from images,” *Images, Information & Software Engineering*, Technical Report, ISE-TR-99-04, 1999.

[32] 中森真尋，岩田基，汐崎陽，“色差成分の DCT 係数と乱数系列との内積値を用いた微小な幾何学的改変に耐性のある電子透かし,” コンピュータセキュリティシンポジウム 2002, pp.431-436, 2002.

[33] P. Bas, J. M. Chassery, and B. Macq, “Geometrically invariant watermarking using feature points,” *IEEE Trans. Image Processing*, vol.11, no.9, pp.1014-1028, 2002.

[34] D. Boneh and J. Shaw, “Collusion-secure fingerprinting for digital data,” *IEEE Trans. Inform. Theory*, vol.44, no.5, pp.1897-1905, 1998.

[35] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, “Anti-collusion fingerprinting for multimedia,” *IEEE Trans. Signal Processing*, vol.51, no.4, pp.1069-1087, 2003.

[36] P. Paillier, “Public key cryptosystems based on degree residuosity classes,” *Proc. of EUROCRYPT’99*, LNCS 1592, Springer-Verlag, pp.223-238, 1999.

関連発表

学術論文

[1] M. Kuribayashi and H. Tanaka, "A new watermarking scheme applying locally the wavelet transform," *IEICE Trans. Fundamentals*, vol.E84-A, no.10, pp.2500-2507, Oct. 2001.

[2] 栗林稔，田中初一，"DCT 係数間の加法特性に基づく電子透かし," 電子情報通信学会論文誌, vol.J85-A, no.3, pp.322-333, 2002 年 3 月.

[3] M. Kuribayashi and H. Tanaka, "Video watermarkgin of which embedded information depends on the distance between two signal positions," *IEICE Trans. Fundamentals*, vol.E86-A, no.12, pp.3267-3275, Dec. 2003.

[4] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for digital images based on the additive homomorphic property," *IEEE Trans. Image Processing* (条件付採録)

国際学会

[1] M. Kuribayashi and H. Tanaka, "A watermarking scheme based on the characteristic of addition among DCT coefficients," *Proc. of Information Security , Third Int. Workshop, ISW2000*, LNCS 1975, Springer-Verlag, pp.1-14, Dec. 2000.

[2] M. Kuribayashi and H. Tanaka, "A new aonymous fingerprinting scheme with high enciphering rate," *Proc. of the Progress in Cryptology, Second International Conference, INDOCRYPT2001*, LNCS 2247, Springer-Verlag, pp.30-39, Dec. 2001.

[3] M. Kuribayashi and H. Tanaka, "A watermarking scheme applicable for fingerprinting protocol," *Proc. of International Workshop on Digital Watermarking, IWDW2003*, LNCS 2939, Springer-Verlag, pp.532-543, Mar. 2004.

学術機関の紀要

[1] M. Kuribayashi and H. Tanaka, “An efficient protocol for anonymous fingerprinting,” *Memoirs of the Faculty of Engineering*, Kobe Univ., no.49, pp.25-39, Nov. 2002.

学術講演

[1] 栗林稔，田中初一，“ID ベース署名を用いた新しい著作権保護方式,” 電子情報通信学会 ISEC 研究会, pp.35-40, 1999 年 5 月.

[2] 栗林稔，田中初一，“ウェーブレット変換を局所的に適用した電子透かし,” 第 23 回情報理論とその応用シンポジウム, pp.311-314, 2000 年 10 月.

[3] M. Kuribayashi and H. Tanaka, “A new anonymous fingerprinting scheme using Okamoto-Uchiyama cryptosystem,” *Technical Report of IEICE, ISEC*, pp.105-110, Sept. 2001.

[4] M. Kuribayashi and H. Tanaka, “Video watermarking of which embedded information depends on the distance between two signal positions,” *Proc. of the 2002 Symp. on Cryptography and Information Security*, pp.751-756, Jan. 2002.