マルチメディア通信と分散処理 80－8
グループウェア 21－8
（1997. 1. 30）

個別情報埋め込みによる画像データの保護方式

阿部剛仁† 藤井 寛† 串間和彦†

ディジタル画像の流通において不正なコピー等による権利の侵害が問題になっている．権利保護の仕組みとしては，「電子透かし」の技術を用いて，画像内部に購入者ごとの個別IDを埋め込み，不正コピーを検出・摘発するという方法が考えられる．しかしながら提供者が個別情報の入った画像を作成し，個々に配布するのは大きな負担であり，CD-ROM等の安価な媒体を用いた大量生産が不可能になるといった難点がある．

本研究では，暗号を用いた画像スクランブルの技術を応用し，同一画像ファイルをCD-ROM等で配布した後に，個別管理用IDを埋め込む流通の方式を提案する．

Image Distribution Method with Identifier Embedding Scheme for Copyright Protection

TAKEHITO ABE,† HIROSHI FUJII† and KAZUHIKO KUSHIMA†

Copyright violation by illegal copying in digital image distribution has been a serious problem. Embedding user identifier information on an image with digital watermarking technique is proposed to specify the origin of illegal copies. But it is difficult to embed the user ID information on the provider side for each user, and such images cannot be distributed through economical media such as CD-ROM.

We propose a new distribution method that embeds user ID information on the user side in order to distribute images through economical media by extending the image distribution using scrambling technique.

1. はじめに

インターネットやCD-ROM等の普及によって，ディジタル画像情報の流通が活発に行われるようになり，これらディジタル著作物（コンテンツ）における著作権等の権利をどのように保護するかということが注目されるようになった．ディジタルの情報はコピーが容易で劣化しないという特徴を持ち，情報の利用者（買い手）から見ると得られた情報を様々に活用するチャンスとなるが，提供者（売り手）から見ると不法なコピーを招く脅威ともなる．

画像データの取り引きにおいては，各取り引きプロセスに対応した画像の保護が必要である．ひとつには画像の流通段階での不正コピーを防止することであり，さらには正当に取得された画像について，それ以降での不正な利用を防止することである．前者については流通段階で画像にスクランブルをかける方式が有効であり，筆者らは暗号を用いて画像の一部を隠蔽し，大まかな画像の内容のみ判別可能なスクランブル画像を作成・流通する「映像半開示方式」[1]を提案してきた．また後者については，表示される画像データそのものに著作権に関する情報や流通管理のための情報を埋め込み，権利の主張や違法な画像の使用に対処する「情報埋め込み方式」がある．画像データの場合，最終的に画像をキャプチャーされる可能性があり，特殊なフォーマットによる画像の利用や，コンピュータソフトウエアで用いられるコピープロテクト等の技術でコピーを防ぐことは難しい．

本稿では，画像スクランブル方式と情報埋め込み方式の特徴を活用し，公正な画像の取り引きと，画像の権利保護を兼ね備えた流通の方式を提案し，有効性と問題点を検討する．

2. 画像データ保護のための従来技術

2.1 画像スクランブル

画像データが正当な取り引きによって利用者に渡される前に，盗み見られないよう内容を隠蔽する方式としては，画像のデータであることを考慮せずに，データ全体を単純なビット列と捉えて，暗号化手法を適用することが考えられる．この方式では輸送・保管時に安全性を高めることはできるが，データ自体は画像符号化の規則に反するため，暗号を解読するまではデータが画像情報

† NTT 情報通信研究所
NTT Information and Communication Systems Laboratories

であることすら確かめられない．画像情報の流通を考えた場合，「宣伝したいが対価をとるまでは見せられない」，「内容が分からないと安心して買えない」という，画像の提供者，購入希望者双方の欲求から，おおよその内容確認が可能な見本画像の提供が必要になる．スクランブル画像（図1）を用いた画像の流通では，画像提供者はまずオリジナル画像から可逆性のあるスクランブル画像(見本画像)とスクランブル解除鍵を作成し，スクランブル画像は予め広く配布しておく．購入希望者の代金の支払いを確認した後，提供者はスクランブル解除鍵を送付し，購入者はオリジナル画像を復元して取り引きを完了する．この方式の利点は，ひとつの画像データが宣伝広告のための見本画像の働きと，最終的な商品として両方を兼ねるとともに，画像のデータ量に比べると極めて少ないデータ量の鍵情報の取り引きによって，実際の商品の取り引きを代替できるという点にある．

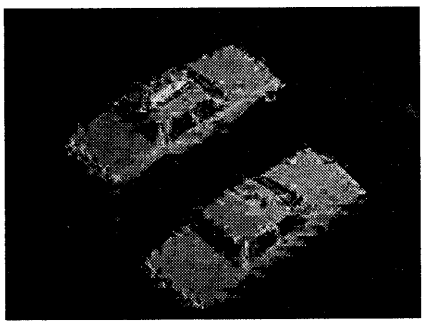

図1　スクランブル画像

2.2　情報埋め込み

画像データには冗長性があり，データの一部分をわずかに変更しても視覚的にほとんど感知できない．これを利用して画像データの一部を一定のアルゴリズムによって変更し，密かに別の情報を埋め込むことができる．こうした技術は電子透かし[2]，データハイディング[3]等と呼ばれている．画像保護の目的で埋め込む情報には，目的に応じて以下の2種類が考えられ単独または組み合わせて使われる．

(1) 画像に対する権利情報を埋め込む方法．

画像に対する権利の所在や連絡先，使用許諾の範囲などを記録しておくことで，主権者は権利を明確に主張でき権利関係の管理が可能となる．また，従来の著作物で行われてきたCopyright表示による権利保護の仕組み[4]への活用も期待できる．さらに不当に利用されている画像に対しては，管理者が画像に対して持つ権利の証明を行なうことができる．こうした権利情報は各画像に固有の情報として埋め込み，通常の画像と同様に流通させる．

(2) 個別ID情報を画像に埋め込む方法．

画像を入手して利用する者ごとに，固有のIDを割り付けて画像に埋め込む．これによって，画像データを一枚一枚個別に見分けることができるようになり，流通する画像を強力に監視することが可能になる．例えばある利用者が自分の持っている画像データをコピーし，他人へ不正に譲渡した場合，その画像の埋め込み情報を調べることで，誰が管理していたデータが流出したのかを特定することができる．これにより正当な画像の利用者が，安易にコピーを作成したり，管理を怠ったりするのを抑止する効果がある．

いずれの場合も情報の埋め込みによる画像の劣化を防ぎ，画像の加工や意図的な改竄によっても簡単に情報が消失しない埋め込みの技術が必要である．

2.3　従来技術のまとめと問題点

画像スクランブル方式には以下の特徴がある．

- 提供者が対価を得るまでは，画像内容を保護する．
- 画像データの輸送にCD-ROM等の安価な経路を選択できる．

正当な購入者であってもスクランブル解除後にオリジナル画像を不正にコピーしたり，鍵情報をスクランブル画像を所有する他人に譲渡するなどの行為が行われることで，画像の著作権等が侵害されるケースがあり，スクランブル解除後の画像保護についての方策が必要となる．

一方情報埋め込み方式には以下の特徴がある．

- 画像に付与した情報が改竄・消去されにくい．
- 提供者が著作権情報を画像に付与すれば，権利の証明ができる．
- 提供者が個別IDを埋め込むことで，違法な利用者をチェックできる．

画像の提供者側は多量のデータを扱うため，提供するデータの処理はできるだけ少ないことが望ましい．しかし個別にIDを埋め込む方法では，画像の提供者側で画像データ一枚一枚に個別の情報を埋め込み，個々に配送するといった負荷の高い作業が必要となってしまう．

画像データは情報量が大きく，大量な画像のやり取りにおいては，CD-ROM等の情報記録媒体を用いて物流に乗せる方法が現在一般的である．同盤プレスによるCD-ROMの生産では，低コストで数百メガバイトの情報を送ることができるが，個別のID情報が入った画像データには，同様の流通方式が適用できない．CD-ROMは雑誌の付録や展示会での配布，カタログショッピング，写真集，と広範囲に渡って利用されており，この流通に簡易な手法によって個別IDの埋め込む方式を確立することは非常に有意義であるといえる．ま

た，インターネット上でブロードキャスト型の配信を行う際にも同様の方式が適用可能である．

3. 画像データの保護方式及び流通モデルの検討

本研究では，前章で示した問題点を解決した画像データの流通方式として，同一のスクランブル画像ファイルを様々な流通手段 (CD-ROM 流通など) で配布し，利用者が画像を購入する段階において利用者毎の ID を埋め込む画像流通形態を提案し，そこで必要になる要素技術の考案を行なう．スクランブルと情報埋め込みを共に行う場合，単純な組み合せでは，一方の操作がもう一方の働きを阻害してしまうことがある．そこでまず，スクランブル状態で情報を埋め込んでも復元してから読み取り可能で，情報埋め込み後にスクランブルをかけてもその状態で情報を読み取れる埋め込み方式を示すことにする．その後，スクランブル技術・情報埋め込みの技術を活用した画像データの流通方式を提案する．

3.1 画像スクランブルに対応する情報埋め込み方式

画像データは通常符号圧縮されて扱われるが，動画では MPEG，静止画では JPEG が標準として用いられることが多い．本研究では JPEG 形式の画像データを対象に研究を進めこととする．

JPEG では画像を 8×8 画素のブロックに分割し，各ブロックごとに離散コサイン変換 (DCT)，量子化，エントロピー符号化を経て符号圧縮化が行なわれる．（図 2）

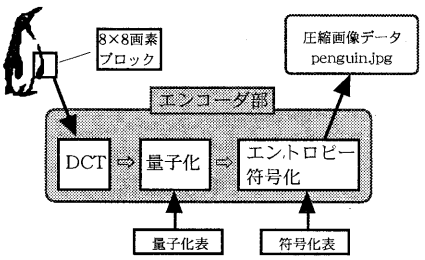

図 2 JPEG 画像符合化

画素データは 1 個の DC 係数と 63 個の AC 係数へと DCT 変換された後，JPEG データ内に用意された量子化テーブルを用いて量子化される．量子化された値は図 3に示す順序で並べ変えられる．つまり DCT 系数列は画素ブロックでの空間周波数が低周波側から高周波側へと順番に並ぶことになる（この並びを 0 ～ 63 のインデックス値とする）．その後 DCT 系数列はハフマン符号語と付加ビットで符号化される．

本稿において特に断りがない場合，「量子化」，「符号化」は JPEG 符号化過程での操作を指し，「係数」は DCT 変換の後に量子化・符号化された DCT 係数を指すこととする．

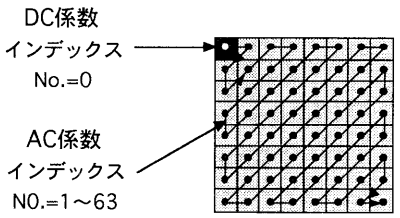

図 3 DCT 系数列

3.1.1 JPEG 画像データへの情報埋め込み方式

JPEG 画像への情報埋め込みは，量子化・符号化プロセスを経た最終的な圧縮画像データの DCT 係数列を対象とする．これは後に示す画像スクランブルによって，情報が破壊されない埋め込み方式を実現するためと，情報埋め込みによるデータの変換を効率的に行うためである．係数列のうちハフマン符号語の変更は JPEG フォーマット規則に反する恐れがあり，仮に規則を満たした場合でも，カテゴリの変更によって復号後の画素値が大きく変わり，画像へ大きな乱れが生じる可能性がある．したがって情報の埋め込みは，付加ビット部分に対してのみ行なう．

情報の埋め込みは，付加ビットの値に一定のしきい値を設けて，それらしきい値間に 0 と 1 のビットをそれぞれ割り当てた正規化値を設定しておき，埋め込みたいデータの値によっていずれかの正規化値へと係数値を変更することで完了する．図 4に正規化の例を示す．この図の例ではしきい値が 4, 6, 8 に設定されており，埋め込み情報が 0 のときは値を 5 （4 ～ 6 の中点）へ，1 のときは 7 へ（6 ～ 8 の中点）へと正規化される．負の値についても同様に正規化を行なうが，しきい値の設定は正負で対称にしておく．この理由については次節で述べることにする．また，対象とする係数の付加ビット数が足りず正規化する値に変更できない場合は，その係数をスキップして次の係数への埋め込みを試みる．

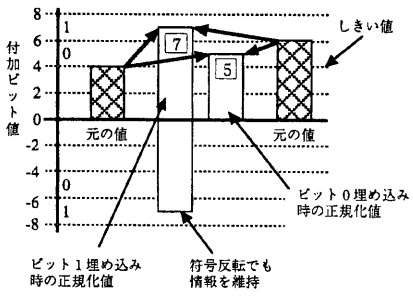

図 4 付加ビット値の正規化

以下に具体的な埋め込み手順を示す．埋め込む情報は

0, 1のbit列として用意し，JPEGデータの付加ビット値に埋め込んでいくことにする．

(1) 情報を埋め込むインデックス値の範囲Zを決定．
(2) 付加ビットのしきい値幅dを決定．
(3) JPEGデータより符号化されたデータを読み，インデックス値がZの範囲なら付加ビット部分を抽出．
(4) 付加ビットがdの中間の値に正規化可能なら情報を埋め込む．

本方式では，情報を付加ビットに直接情報を書き込んでいるので，量子化されたDCT係数を操作していることになる．つまり実際のDCT係数に対する変更量は，量子化テーブルの値との積に近い値となる．従ってその値より十分小さな画像の変形には影響なく情報が読み取れることになる．

画像にノイズが入ったり，情報を改竄しようと画像に操作が加えられた場合，しきい値幅dが大きいほど，しきい値の中間点に正規化した画像データの値はしきい値を超えて変化する確立が下がり，埋め込み情報を保持する可能性が高くなる．しかしdを大きくすると，埋め込み時のデータ変更幅も大きくなり，元画像に対する影響も大きくなる．また，情報を埋め込むDCT係数(インデックス値)の選択範囲Zも，しきい値のステップと同様，情報埋め込み時の重要なパラメータとなる．低周波側の係数を変更すると画像に与える影響は大きいが，画像の変形に対して埋め込み情報が残りやすくなり，高周波側の係数変更はその逆になる．これら情報埋め込み時のパラメータは，画像の同一性保持と埋め込みデータの改竄防止効果との関係を考慮し，用途に合わせて設定する必要がある．

3.1.2 画像スクランブル方式

画像スクランブルは付加ビットの値を直接変更し，JPEGの画素ブロック単位で画像撹乱を行う．付加ビットは規定されたビット数の任意の値が許されることから，JPEGのフォーマットを守ったままでデータの変換が行なえる．また，DCT係数の大まかな値はハフマン符号語で規定されるカテゴリ値によって決められているので，付加ビットの変更によっても同一カテゴリ内での値変動にとどまり，画像の概要をある程度残すことができるのである．

実際のスクランブルは，暗号鍵から作成した乱数列を用いて，ある付加ビットに対して全ビットの反転を行うことで実現することにする．付加ビットは全ビットを反転すると値の正負が逆転するという特性を持っているため，上記スクランブル手法によって，前節で示したしきい値を正負対称に設定して埋め込んだ情報に対して，埋め込まれた情報を破壊することなくスクランブルの設定・解除を行うことができる．

3.2 個別情報(ID)の埋め込み方式

これまでに電子透かしの技術を用いて，個別のIDを埋め込んだ画像を流通させる方式がいくつか提案されている[5]．しかし，画像にID情報を入れられるのは情報の提供者側のみで，2.3に示した「CD-ROM等を用いた同一画像ファイルの大量流通には適用できない」という問題点は残されたままである．画像が流通した後で情報の埋め込みが行われるのが望ましいが，悪質な利用者に情報の埋め込み装置を送りつけて，不正防止のためのIDを埋め込むよう単に委託するのは，盗人に金庫の鍵をかけるよう言い渡すようなもので実用的でない．そこで，画像の一時的な保護機能を有するスクランブル方式を，利用者側での画像への情報埋め込みに応用する．スクランブルをかけられた画像を利用するには，必ずその画像データを読み込み，スクランブル解除の処理を行なってから出力するというプロセスが生じる．このプロセスにおいて利用者の個別ID情報を付加することで，同一画像ファイルの配布と個別IDの埋め込みという双方の目的を達成することできる．以下に提案する流通方式を示す．

3.3 画像データの流通モデル

3.3.1 流通方式の設計

以下に提案する画像取り引きの方式を示す．

表記方法：

I： オリジナル画像
I_{sc}： スクランブル画像
I_{ID}： 埋め込み済みディスクランブル画像
U_{ID}： ユーザーの固有情報（ユーザーID等）
P： 画像固有の情報（著作権情報等）
k_s： スクランブル鍵
k_U： 利用者Uに対する共有システム鍵
κ： ディスクランブル情報鍵
$SC_k(I)$： 画像Iを鍵kを用いてスクランブルした画像
$w(I, D_1, D_2 \ldots D_n)$： 画像$I$に情報$D_1, D_2 \ldots D_n$を埋め込んだ画像
$E_k(D_1, D_2 \ldots D_n)$： データ$D_1, D_2 \ldots D_n$を鍵kを用いて暗号化したデータ
$DW_{k_s}(I_{sc}, u, p)$： I_{sc}をk_sでディスクランブル及びu, pの情報を埋め込んだ画像(u: 利用者個別ID，p: 画像固有の情報)
$RD(I_{ID})$： 読み出した画像I_{ID}の埋め込み情報

画像提供者(PROV)と利用者(USER)との取り引きフロー

(1) PROV: スクランブル鍵k_sで画像Iをスクランブルしスクランブル画像$I_{sc} = SC_{k_s}(I)$を作成．
(2) PROV:I_{sc}を公開，配布．
(3) USER: スクランブル画像I_{sc}を入手，評価．
(4) USER: スクランブル画像I_{sc}の注文．
(5) PROV: 著作情報PとユーザーID U_{ID}とk_sをユーザーとの共有鍵k_Uで暗号化して合成し，ディ

スクランブル情報鍵 $\kappa_{puk} = E_{k_U}(P, U_{ID}, k_s)$ を作成.

(6) PROV:κ_{puk} を送付.

(7) USER: ディスクランブル及び情報埋め込み装置によって情報入りディスクランブル画像 $I_{ID} = DW_{k_s}(I_{sc}, P, U_{ID})$ を生成.

k_s, P, U_{ID} は USER が入手した κ_{puk} と k_u から，以下の行程によって生成され，I_{ID} を得る.

(i) システム共通鍵 k_U を用いて κ_{puk} から著作情報 P とユーザー ID U_{ID} と k_s を分離.
$\{P, U_{ID}, k_s\} = E^{-1}k_U(\kappa_{puk})$

(ii) k_s を用いてディスクランブル．かつ情報埋め込み.
$I_{ID} = w(SC_{k_s}^{-1}(I_{sc}), P, U_{ID})$

提供者による不正画像のチェックフロー

不正に利用されている画像や不信な画像を発見した場合，画像の提供者は以下の方法で画像情報を読みだしチェックできる．表記法は上記 3.3.1 節と同じである.

(1) PROV: 不正使用画像 $I_{ID'}$ を入手

(2) PROV: 情報読み出し装置によって $I_{ID'}$ より情報読み出し.
$\{U_{ID}, P\} = RD(I_{ID'})$

(3) U_{ID} 登録者を調査.

3.3.2 提案方式の考察

前節で提案した流通方式では，スクランブル解除鍵の中に個別 ID 等の埋め込み情報が含まれていることになり，CD-ROM 等によって利用者がすでにスクランブル画像を入手している場合は，画像の購入によるデータの送受信が提供者側からの 1 回のみになる．提供者側ではユーザー ID 等を暗号化 (E_k) する処理のみで非常に負担が軽く，送られるデータ量も画像情報に比べ非常に少ない．ただし利用者 U は予め共有システム鍵 k_U を持っている必要がある．k_U はスクランブル解除のための鍵 k_s や埋め込む情報 P, U_{ID} など重要な情報を $E_k(P, U_{ID}, k_s)$ から抽出するときに必要となるが，もしこの k_U によって $E_k(P, U_{ID}, k_s)$ がディスクランブル装置外で復号されることになれば，スクランブルの解除のみが行われたり，埋め込まれる情報が改竄されてしまうなどの不正が行われてしまう．したがって実際のディスクランブル時に，装置内で k_U から秘密のアルゴリズムによって真の鍵情報 k'_U を生成し，k'_U で暗号を解く仕組みにする必要がある.

ここで問題になるのはディスクランブル装置内のアルゴリズム解析に対する耐久性である．k'_U を生成する部分だけでなく，情報を埋め込む部分やスクランブルを解除する部分等も，解析されると画像を保護することはできなくなる．この部分を保護に耐タンパー装置を用いることが考えられるが，その場合は費用対効果の問題となる.

画像固有の情報 (P) を予め配布する画像に埋め込んでおき，後から追加する情報は個別の情報 ID(U_{ID}) のみとすることもできる．しかしその場合，後から追加する情報が極端に少ないと，情報が埋め込まれた複数の画像の差分から，追加部分が正確に推定される危険性が高くなる．U_{ID} と共に後から P を埋め込む本方式では，利用者ごとに異なるビット数だけシフトするなど，P の書式を変化することで，そのような攻撃に対する耐性を高めることができる.

4. 実験システム

本研究の提案する流通モデルに基づく画像取り引きの実験システムを作成し，システムの実現性と問題点について考察を行なった．データの暗号化部分には FEAL-8 アルゴリズムを用いた.

4.1 評　　価

本方式に基づく画像取り引きの方式を端末上で実際に行なって，提供者側から同一の画像ファイルを送信した後に，利用者側で画像に個別の情報 (利用者別 ID 等) を埋め込ませるという，目標とした画像の流通形態が機能することを確認した．また今回作成した情報埋め込みアルゴリズムによって，スクランブル状態に関わらず，情報の書き込み／読みが可能であることを確認した.

情報埋め込みの性能として，550 × 370 ピクセル (約 30KB 程度) の JPEG 画像 (quality 75%) に対し，しきい値幅 d を 4，インデックス値の範囲 Z を $\{1...5\}$ と設定した場合，500 ～ 1500 ビットの情報埋め込みが可能であった (図 5，6)．改竄に対する強度を高めるためには，画像データの値を正規化する際のしきい値幅 d を大きく取る必要がある．しかし平坦な画像等に多くみられる付加ビット値の小さな係数は，目的の値へ変更することができず情報が埋め込めないことがある．画像が平坦な部分は情報の埋め込みによる画像への影響が大きく現れやすく，実際に可能な場合でも情報を埋め込むことは得策ではない．付加ビット数に応じた埋め込みの判定は，画像の品質を維持することにもなり，ビット数を拡張してまでデータの変更を行う必要はないと考えた.

先の条件で埋め込みを行った画像に対する変形では，quality40% の JPEG 圧縮の後で 95% 以上の情報を読み出すことができた．また，JPEG → GIF → JPEG のようなフォーマットの変換でも 95% 以上の情報が読み出せた．画面の切り取りを行った場合，残った部分の情報は完全に読み出せることを確認した．したがって 1 画像に同じ情報を繰り返し埋め込む手法をとることで，残された画像から埋め込み情報を読み出すことは可能である．画像のコントラスト変化には弱く，コントラスト -10% で読み取り率は 70% 程度に下がってしまった.

図5 オリジナル画像

図6 情報を埋め込んだ画像

4.2 課　　題

今回の情報埋め込み手法では，平坦な画像に対して大きなしきい値を設けた場合などには，実際に情報を埋め込める係数が限られてしまい，情報の改竄が行われやすくなる．一画像内で複数のしきい値を用いたり，特定の係数には別の埋め込みアルゴリズムを適用するなどの対策も必要である．

3.3.2節でも示したが，ID情報などの個別情報を画像に埋め込んだときは，それらの画像を多数集めて差分をとると，元の画像が推測できる可能性がある．様々な種類のサンプル画像に対して，どの程度の情報を埋め込んだ画像を何枚集めたら，どれくらい元画像を推測できるのかといった検討を十分に行い，差分による推測に強い情報の埋め込み手法を考案する必要がある．

5. ま と め

今回，CD-ROMによる画像データの大量販売等においても，利用者ごとに固有のIDを埋め込ませ，画像データの強力な個別管理を行なえる流通方式について提案した．また画像スクランブルとの組み合わせに適した情報の埋め込み方式を考案し，提案する流通方式の実験システムに実装してその有効性を確認した．今後は，実験システムの完成度を高め，提案方式の有効性についてさらに検討を行なっていく予定である．また，画像に個別情報を埋め込んだときに，情報の改竄や消去等の攻撃に対しどれほどの耐久力があるかといった評価を行なうことと，その場合に適した情報埋め込み手法についても検討して行きたいと考えている．

参 考 文 献

1) 藤井，谷口，山中："スクランブル映像を用いたネットワークにおける映像情報流通方式"．第51回情処全大，2-85,1995.
2) I.J.Cox et al.: "Secure Spread Spectrum Watermarking for Multimedia", NEC Research Institute,Technical Report 95-10.
3) W.Bender et al.: "Techniques for Data Hiding", Proceedings of the SPIE,2420:40,1995.
4) 久保田英明，"著作権ビジネス最前線"，中央経済社，1992.
5) NIKKEI ELECTRONICS 1996.4.22(No.660).