解説

電子透かし技術の最新動向

松井 甲子雄 防衛大学校情報工学教室

はじめに

急速なディジタル化とネットワーク化によりコピーに必要な装置も経費も格段に安価となり，しかもそのディジタルコピーは原本とまったく同じ品質というメリットもある．そのため不正コピーや改ざんなどの違法利用が野放し状態となり，著作権管理は当事者の知的良心に委ねられている．そのような情報環境のもとでは優れた創作品を公開する意欲を阻害されるだけでなく正常な商取引も成立し得ないことになる．そこで，ディジタルコンテンツの知的財産権を保証し，それに見合う使用料を徴収するシステムの構築と，同時にコンテンツ自体の流通管理も可能ならしめる技術の開発が強く要請されて電子透かし（digital watermarking）という新しい技術が登場してきた[1]．

この社会的背景に基づきディジタルコンテンツの著作権保護対策のために，すでに国内でもメーカ各社の研究開発とともに情報系団体の2，3の委員会が活動を始め，また欧米においても活発な研究開発とその規格統一への検討がなされている[2),3)]．本稿ではこの電子透かしの目的や原理，用途などの解説とともに，電子透かしに対する攻撃とその耐性などにも触れて，この分野の最新の技術とその動向を紹介したい．

著作権保護のための新技術

画家は自分の描いた絵に必ずサインを入れる．そのサインが絵の価格を左右することになる．同じようにホームページに掲げた画像や音楽にも独創性に優れたコンテンツにはその価値が認められている．そこで，電子的にコンテンツの上にサインを入れたとする．油絵の上の物理的なサインとは異なってメモリ上のディジタルサインを削除するのはいとも簡単である．しかも原画を傷めることもない．それでは記入したサインも何の役にも立たない．またサインが画面上にいつも表示されているとユーザには見苦しくスマートでない．そこでサインをコンテンツの内部に埋め込んでおくことを考えてみよう．密かに画像の中に作者の名前や記号をビットに分解して潜ませておくのである．このように仕組むことができるならば，一見しただけではメディアのどの部分にどのような形でサインが埋め込まれているのか第3者には判別できない．しかし，ユーザがそのコンテンツを著作者に断りなく悪用していると認められるときには，著作権者は法的手続きをとるとともに，その証拠としてこの電子透かしを違法コピーから抽出して見せることができる．これが著作権侵害の最も確かな決め手になるであろう．このような趣旨から電子透かしが著作権保護対策として採用されようとしている．

一方，ディジタル映像やディジタル音楽などはすべてビット情報の積み重ねから構成されている．人間の目や耳は多くの情報を瞬時のうちに収集できる反面，多量のビット情報には冗長性がありその1部を改ざんしても骨格部分を変更しない限り視聴者に判別される可能性は意外に低いものがある．そこで，電子的に画像や音楽のビット情報の1部を著作権情報で置き換えてもユーザに迷惑をかけることにはならないであろう．この人間の特性を上手に利用して快適なマルチメディア環境を提供するために電子透かしをコンテンツに埋め込んで利用しようというのが第2の理由である．

さらにアナログ時代のようにコンテンツのヘッダ部分に著作権情報を記入しておくと悪意を持ってその著作権情報を削除しようと試みる者もいる．またディジタル画像

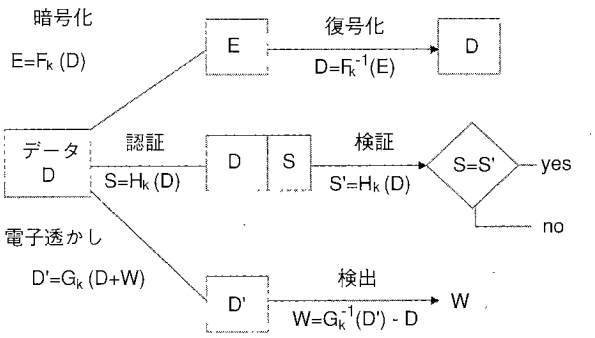

図-1　マルチメディアのセキュリティ対策

や音楽ではその1部分を切り取って他に転用する者もいる．それらの著作権を犯す行為に対しては，ヘッダ部の注意書きのみではまったく効果がない．このような悪質な行為に対しディジタル映像の各フレームごとに電子透かしを埋め込んでおくことにより，きめ細かい対策を講ずることができる．これが第3の理由である．これらの理由から著作権管理のために電子透かしを利用しようとする新しい試みがここ数年の間ににわかに注目を集めてきたものと考えられる．

どこが暗号と違うのか

一般にマルチメディアのセキュリティ対策としては，図-1に示すような方式が考えられている．その1つは暗号化関数F_k（kは鍵を示す）を使ってデータを暗号化することによりセキュリティを保ったままユーザに配布する形式である．これは復号鍵kを所有するユーザのみがそのディジタルコンテンツを観賞することができるシステムである．しかし，そのユーザが第3者に不正にコピーを譲渡した場合にはセキュリティ効果を失ってしまう．不正コピーの出所を追及する手段を持ち合わせないからである．

一方，第2の認証機能は内容Dに改ざんが行われているか否かを認証子Sで検査し，原本の正当性を保証する型式である．ハッシュ関数H_kを使って受領したデータDに添付された認証子Sと受領データDのハッシュ値S'が一致するか否かで改ざんの有無を判定する．この方式は電子文書や電子マネーなどの正当性に関するセキュリティ対策には欠かせない手段である．しかしこの2つの機能だけでは明らかにマルチメディアの不正コピー対策として不十分である．

そこで第3の案として電子透かしのアイデアが急浮上したのである．これは図-1から分かるように，データDに透かし情報Wを付加し，埋め込み関数G_kを使ってコンテンツに秘匿する．したがって，前述の認証方式とは観点を変えたセキュリティ手段であり，ユーザが手にする

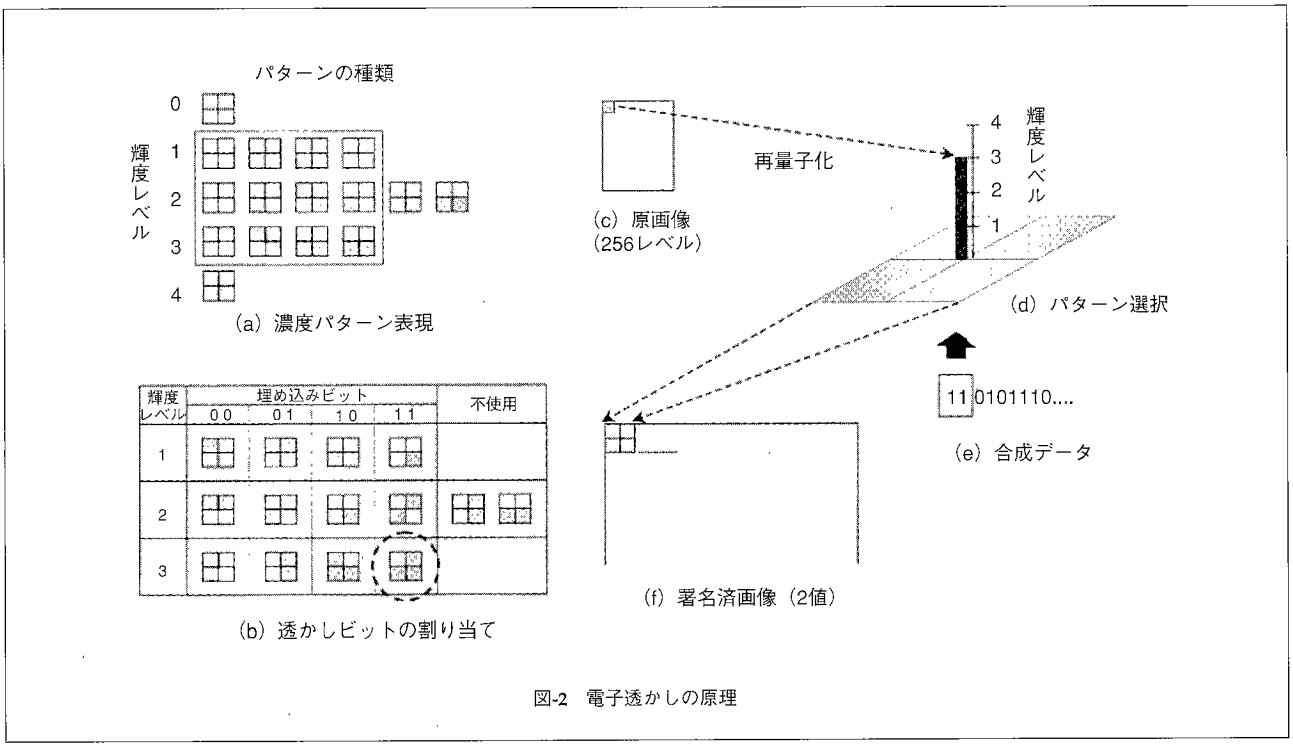

図-2　電子透かしの原理

(a) 透かしなし　　(b) 透かしあり

図-3　透かし画像の例

データD'は原本のDとは若干異なったものであることに注意しなければならない．ただし，このD'がDに近いほど優れた透かし方式であることはいうまでもない．

ところで，電子透かし技術は突然にこの世に登場してきたものであろうか．実は，その思想は暗号（cryptography）とほぼ同じく昔からこの世に存在していたと考えてよい．暗号はその暗号化と復号化のアルゴリズムを公開しても鍵によってセキュリティを保持できるシステムである．これに対し，通信していること自身を隠した秘密の手段によってセキュリティを確保しようとする試みが世界の諜報機関などでアナログ時代から密かに研究されており，それを通信秘匿（steganography）と呼んでいた．この概念からディジタル時代にふさわしい秘密伝達法として画像深層暗号やデータハイデング，サブリミナル，コバートチャネルなどの新しい用語で呼ばれるものが再登場し，その1つの応用として電子透かしが広まってきたのである[1]．それゆえ，電子透かしは透かし情報の形式とその埋め込み位置を第3者の目に直接見えないように秘匿した方法でセキュリティを確保するために，その伝達形式が見える暗号とは本質的に性格を異にするものである．この特性が，電子透かしの規格の統一問題やその攻撃耐性に対して厳しい制約をもたらすことになる．

すでに述べた電子透かしの役割からどんな特性を持つ透かしの構造を作ればよいか考察してみよう．まず，透かし情報はヘッダ部や特定の空き領域ではなく，コンテンツ自身に埋め込む必要がある．これは容易に見破られないためである．その際に透かし情報がJPEGやMPEGなどのデータ圧縮で消去されないことも考慮に入れる．また画像の編集や処理，あるいは切り抜きなどで透かし情報が散逸しないように重複して記録しておくことも大切である．

一方，透かしの改ざんや消去などの悪意を持つ攻撃に耐えることも考慮しておかねばならない．想定される攻撃形態とそれに耐える手法の研究開発が早急に解決すべき課題となっている[1]．

また電子透かしをコピー制御に使う立場からそのアルゴリズムは簡素であることが望ましい[4]．しかもコンテンツの仕様やメディアの種類に左右されない共通形式の透かしのアルゴリズムを求めているがいまだ期待したものは得られていない．最後にこれらの配慮の上で，欲を言うならば原本とほぼ変らないレベルの品質を保証できる方式が望ましい．

どんな道具を使うのか

電子透かしを埋め込むにあたって，基本となる発想は画像や音声の持つ冗長度を利用することである．その第1は，画像を構成している画素単位に透かし情報を埋め込む方法である．たとえば輝度情報を利用した濃度パターン法による電子透かしの原理を図-2に示す[1]．

濃度パターン法は濃淡画像を白黒の2値画像として印刷する際に用いられる輝度情報を密度情報に変換する方法である．理解しやすいように1つの多値画素を表現するのに2×2画素からなる2値のセルを準備する．このセルで表現できる輝度情報は，同図（a）のように各レベルが1ないし複数のセルからなっている．ここにセル選択の自由度があるのでそれを透かし情報に利用する．そこで

メディア	データ形式		透かしの方法
画像	静止画	2値	濃度パターン法，組織ディザ法，誤差拡散法，ランレングス法
		多値	ビットプレーン法，局所構造利用法，画素空間法，群構造法，パッチワーク法，列生成法，量子化誤差法，FFT法，スペクトル拡散
		カラー	DCT法，wavelet法，ADCT法，色差利用法，色覚モデル法
	動画		DCT法，wavelet法，動きベクトル
	FAX		ランレングス法，差分利用法
音声	非圧縮	音声	時間マスキング法，周波数マスキング法，ディザ信号法，適応PCM法
		音響	エコー法，スペクトラム拡散法，変形DCT法
	圧縮		ベクトル量子化法，極性符号法，音源パルス法，パリティビット法
文字	文書	和文	文字回転法，文字幅伸縮法
		英文	ラインシフト法，ワードシフト法
	ソフトウェア	ソースコード	変数名利用法，命令文利用法
		オブジェクトコード	ダミーコード利用法

表-1　埋め込みメディアによる電子透かしの分類

同図（b）に示すように（a）のリストから冗長性を持つ部分を取り出して，各セルに密かに透かしビットを割り当てておく．これが暗号表の役割を果たしている．これらの準備が整ったところで同図（c）の原画像から1画素を取り出し，これを5段階0～4レベルの明るさに再量子化する．そして輝度レベルが決まると同図（e）の合成すべき透かしビットに従い（b）から該当する○印のパターン（d）を選択し，これを2値画像（f）上に出力する．この方法を（c）のすべての画素に適用すると透かし入りの出力画像を得ることができる．その出力画像の1例を**図-3**に示す．これは最も基本的な透かしの原理を示す例である．すでに公表された透かしのアルゴリズムを考察すると，多くのものは画像（または音声）信号波 $y = A\sin(\omega t + \theta)$ の3要素である振幅A，周波数ω，位相θを透かし信号で変調する方式になっている．振幅Aを利用するものは画素の量子化値を微少に変更し，ωを利用するものは直交変換（DCTやwavelet）後に周波数係数値を作為的に修正し，さらにθを利用するものはフーリエ変換による虚数値を透かし信号で変化させている．在来の提案方式を**表-1**にまとめておく[1]．

このような信号波を透かし信号で変調するタイプのほかに，画像や音声データを確率モデルとみなして，その統計分布モデル自体を透かし信号で変形しようと試みたものも考案されている．まさに多様な道具が出揃ってきたところである．

一方，図-1で示したように透かし信号Wを検出する際に原本Dとの照合を必要とする場合と鍵のみで復号できる場合がある．後者をblind型，前者をnon-blind型と分類することもある[2]．表-1に掲げたアルゴリズムの中にはnon-blind型が多く，オフラインでの著作権侵害の立証には有効であるが，復号に原本が必要となるためオンラインのコピー制御には不適切となるものもある．このため，最近ではblind型のアルゴリズムの開発が急務となってきた．

また，透かし情報のセキュリティ確保と運用の利便性のために2種類の鍵を導入する試みもある．コンテンツの正当な権利者が透かしを書き込み復号でき，さらに書き換えもできる方式をprivate鍵と呼ぶ．一方，透かし情報を見ることはできるが書き込み変更を許さない方式をpublic鍵と呼んで，公開鍵暗号の発想を電子透かしにも導入しようと試みている[2]．しかしながら現在までのところ，この2つの鍵を使った具体的なアルゴリズムの提案は見当たらない．その理由としてpublic鍵を導入すると透かしがどんな内容か，あるいはどんなロゴマークを用いているか分かってしまうため，そのマークの逆パターンを画像上に重ねて消去したり解読不能にする攻撃の糸口を与

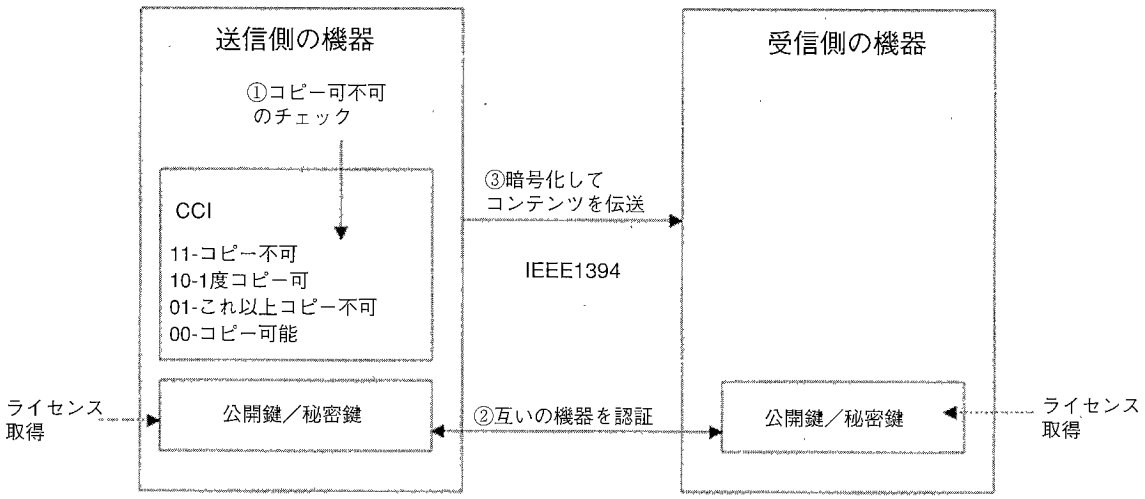

図-4　IEEE1394とコピー制御方式[7]

えてしまうからである．

次に，透かし情報として何を用いるべきかという問題も重要である．最も多く採用されている方法は文字または数値情報すなわちビット系列の埋め込みである．この方式は少ない冗長性に必要な情報（400ビット程度[3]）を保持できるが，画像処理や各種の攻撃にぜい弱である．埋め込みビットが正しく復号されないと数値情報が役に立たないので，多くの場合誤り訂正などの冗長符号を利用せざるを得ない．これに対してロゴマークを利用する方法も多く用いられている．この方法では特定パターンを反復してコンテンツ内に埋め込むので，各種攻撃に対してパターンの残存性が高く，証拠能力は十分である．しかし，コピー制御やビット情報を必要とするアプリケーションには不適である．さらに統計的な特性値，特に平均値や分布の偏りなどを用いる方法では多数データを対象とするため攻撃に比較的強い耐性を示す．ただし，その検証過程において透かし情報を表現するパラメータの検定が煩雑であることや画像の基本要素の統計的分布を強制的に変更するため画質劣化を無視できないなどの欠点もある．

このように電子透かしとしてどんな道具を用いるかにより，画質の維持や攻撃への耐性などが異なり，また応用分野への利便性も変わってくることに配慮しなければならない．

透かしは何に使えるか

マルチメディア・コンテンツの製作者や版権者が，その作品の中に電子透かしを埋め込んでおき，第3者の不正使用を防止する役目がこれまでの開発の主テーマであった．しかし，研究が進展するに従い，その役割を消極的な検証対策に限定せず，最近，次々に新しい積極的な応用分野が登場している．

その1つとして，ディジタルカメラに電子透かしの機能を付加しておき，撮影と同時に画像データに透かし信号を埋め込む方式がある．この目的は，報道記事などにおいて，撮影者が現場写真の修正や改ざんするのを防止し，写真が本物であることを保証する認証手段にしようとの目論みである．

次に，コンテンツの流通過程において，その販売者が管理上から必要なデータを透かしに記録したいという要望がある．これは購入者による不正コピーの横流しを防止する狙いである．販売者はコンテンツに識別番号と販売日時などの数値データを透かし信号として埋め込んでおく．そして，Web crawlerを使ってネットワーク上の不正利用者を監視する意向である．ただし，いまだこのWeb crawlerの検索効率が悪く，1部の開発業者も企画倒れの模様である．

さらに積極的な応用として透かしビットによるコピー制御がある[4]．CPTWG（Copy Protection Technical Working Group）ではコピー制御技術の標準化が検討されている．**図-4**に示すようなIEEE 1394の規格とともにこのコピー制御情報CCIを電子透かし方式でコンテンツに埋め込んでおくのである[7]．このCCI信号は2ビット程度で十分であり，悪意を持つ第3者の攻撃によって消去もしくは破壊されないことが必須である．ただし，コピー制御に電子透かしを利用する場合にはCCIビットが

その都度可変でなければならないのでblind型の読み出し，書き込みが可能な透かしアルゴリズムが必要になってくる．

このように電子透かし技術が成熟するに従い，ますます，その長所が多方面で利用されてゆくことであろう．

まだまだ弱い透かし技術

ディジタルコンテンツの著作権保護を可能にするため電子透かしを創作物に埋め込むと，必ず画質劣化を伴うことになる．その劣化の徴候が観賞する人に不快にならない程度であれば透かし技術として採用できる．しかし，単純な埋め込み方法では容易に攻撃を受けることになる．電子透かしへの攻撃には，透かし情報の削除，改ざん，解読，撹乱などがある．また，意図的な攻撃でなくとも簡単な画像処理によっても大きな被害を受けることが多々あることを承知しておかなければならない[6]．

もちろん，JPEGやMPEG，あるいはベクトル量子化などによるデータ圧縮の際にも本質的な影響を受けるので，電子透かしの埋め込みデータがどのような処理を通過してユーザの手元に届き，再利用されるか十分に検討しなければならない．

これらの電子透かしに対する好ましからざる諸現象を集約した評価ツールとしてKuhn[5]はStirMarkなるソフトを彼のホームページに公開している．この評価基準は大変に厳しいもので，表-1に掲げた多くのアルゴリズムはその基準に達し得ないことが検証されつつある．このため，透かし技術はいかにあるべきか多方面から再検討を迫られている現状にある．

そこで耐性の強い透かしを仕込むにはどのような着意が必要か，その問題点を最新情報から考えてみよう．まず，画像（または音声）という限定された空間上に密かに埋め込まれた透かし情報を永久に保持することはきわ困難であると思われる．このため完全なものを1つだけ求めるのではなく，次善の策をいくつか準備して攻撃に対応せざるを得ない．たとえば

(1) 透かし信号はできるだけ多くの画素に埋め込み，可能ならば全画素に同一信号を反映させる
(2) できるだけ冗長性のある透かし構造を用いる
(3) 周波数領域では可能な限り広帯域に拡散させる
(4) 復号には秘密鍵を持つblind型が必須となる

以上のような性質を組み込んだ透かしのアルゴリズムを考案して各種の攻撃により十分に評価することが大切である．

透かしは頼みの綱になり得るか

電子透かし技術はディジタルコンテンツの健全な流通のために不可欠な要素技術であるから，すでに国内外でいくつかの試供システムもしくは営業システムが稼動を始めている．しかし，それらのほとんどのシステムでは，どのようなアルゴリズムを用いて透かし情報を隠匿しているかその内容を公開していない．これは電子透かしがsteganographyから派生した技術であるからやむを得ない現象なのかもしれないが，機能をブラックボックスとして公表しただけではその信頼性をユーザに訴える力は弱い．その上，透かし技術が非公開のままでは，他のシステムとの相互運用性（interoperability）に欠ける問題が生まれてくる．

互いに異なったサービス機関が提供する透かし信号の間に本質的に共通する識別コードを埋め込んでコンパティビリティを持たせるにはどうすべきかなどの重要な課題を未解決のまま各社ともスタートしている．さらには透かしにコピーコントロール機能を付与したときの共通フォーマットの問題も積み残されたままである．ディジタルコンテンツに埋め込まれた透かし信号が各社のデコーダに共通していなければ役に立たないことは明白である．

これらの現実を直視するとき，電子透かし技術が抱えている最大の問題は，まず（1）強い耐性を持つ技術を公開することであり，(2) それを各種の攻撃にさらして安全性を確かめた後に (3) 共通仕様を設定すべきであろうと思われる．

現状の技術レベルから推量するに，単一のアルゴリズムで多様な攻撃をかわすことが可能なものは少なく，信頼性向上のためにメディアごとに複数のアルゴリズムを組み合わせたシステムが不可欠となる．

そのような耐性のある電子透かし技術の開発とシステムの構築が整えば自己の創作品を安心して委託できる著作権保護手段として頼みの綱になり得ることであろう．

参考文献

1) 松井甲子雄：電子透かしの基礎ーマルチメディアのニュープロテクト技術ー，森北出版（1998）．
2) Imprimatur : Watermarking Technology for Copyright Protection : General Requirements and Interoperability, http://www.imprimatur.alcs.co.uk/IMP_FTP/I4602/a（1998）．
3) DAVIC : Copyright Information, DAVIC1.4 Specification Baseline Document, No.84, revision4.0（1998）．
4) Cox, I.J. and Linnartz, J.M.G. : Some General Methods for Tampering with Watermarks, IEEE Journal on Selected Areas in Comm., Vol.16, No.4, pp.587-593（1998）．
5) Kuhn, M.G. : StirMark, Ver.2.2, http://www.cl.cam.uk/~fapp2/watermarking/image_watermarking/stirmark /（1998）．
6) Barnett, R. and Pearson, D. : Attack Operators Fordigitally Watermarked Image, IEE Proc.-Vis. Image Signal Prosess., Vol.145, No.4, pp.271-279（1998）．
7) 野村総合研究所：デジタル私的録音のプロテクト技術に関する動向調査，p.3（1998）．

（平成11年1月7日受付）