

## 調査対象技術の技術概要 「電子透かし」

- ( 1 ) テーマ名：電子透かし
- ( 2 ) 標準技術収集技術内容

### 1．技術の動向と調査対象の概観

電子透かし技術とは、人間の知覚（視覚、聴覚）特性を利用し、静止画、動画、オーディオ等のデジタルコンテンツに対して、コンテンツとは別の情報を、人間に知覚できないように埋め込む技術をいう。

「密かに情報を埋め込む技術」ということでは、以前より、「紙幣の透かし」やステガノグラフィ（深層暗号ともいう）という暗号技術が使われていたが、この「情報を埋め込む技術」自体が注目を浴びるようになってきたのは、インターネットが広く普及するようになった極く最近のことである。

20 世紀末から 21 世紀初頭にかけて、社会基盤としてインターネットが普及するようになって、デジタル化電子情報通信技術を活用する新しいビジネスが立ちあがってきた。コンテンツビジネスもその一つである。電子化された図書、静止画、動画、オーディオなどのマルチメディアコンテンツを、ネットワーク上で直接販売するビジネスである。インターネットを利用した消費者向けビジネス（Business-to-Consumer）なかでも、最も成長が期待されているビジネスでもある。現実には、デジタル化された音楽の配信など、さまざまなコンテンツ配信ビジネスが開始されている。

しかし、競合者あるいは消費者による「不正コピー」、あるいは、その危惧があることが、コンテンツビジネスの本格的拡大の障害となっている。コンテンツビジネスの健全な成長のためには、著作権の保護、主張、正当な課金、不正コピー防止などが必須要件と考えられるようになってきている。新しい技術を駆使した「情報セキュリティ強度」の高い著作権処理システムの実現が必要になってきている。

このような環境のなかで、注目されるようになってきたのが「電子透かし」の技術である。1997 年頃より、この分野の技術開発が急激に活発化しており、関連する報告文献の件数を急増している。これらの報告を概観すると、電子透かしにおける技術開発の内容は下記の分野に分類できるようである。

- 「透かしの埋め込み技術」に関するもの
- 「透かしの応用技術」に関するもの

以下、「埋め込み技術」と「応用技術」という視点から、電子透かしに関する技術動向を調査することとし、これらについてその動向を俯瞰することとする。

## 2. 透かし埋め込み技術

画像であれ音声であれ、すべてのデジタルコンテンツは「周波数領域での表現」が可能である。具体的にいうと、画像も音声も周波数の異なるコサイン(Cos)の和として表現できる信号として扱うことができる。

$$x = A_1 \cos(\omega_1 + \theta_1) + A_2 \cos(\omega_2 + \theta_2) + \dots + A_n \cos(\omega_n + \theta_n)$$

$A_1, A_2, \dots, A_n$  : 振幅  
 $\omega_1, \omega_2, \dots, \omega_n$  : 角周波数  
 $\theta_1, \theta_2, \dots, \theta_n$  : 位相

( 1 )

「電子透かしを埋め込む」と云う事は、(1)式において、視覚的にも聴覚的にもあまり影響を与えないような項の  $A$  ,  $\omega$  ,  $\theta$  のいずれかに、「電子透かし情報」に基づいてわずかな変更量を付加することである。

冗長な部分の振幅を変更する方式が「画素置換型の電子透かし技術」であり、コンテンツに対し影響度の低い高域周波数項を削除したり、周波数に僅かな変更を加えたりするのが「周波数特性を利用した電子透かし技術」で、具体的にはフーリエ変換あるいはウェレット変換型電子透かし技術と呼ばれる方式である。この方式は圧縮技術に深く関った透かし技術である。また、位相 を操作するのが「位相操作型の電子透かし技術」で音楽関係ではポピュラーな方法である。

「電子透かし埋め込み技術」を原理的に説明したが、新しい方式が誕生した場合でも、基本的には(1)式のなんらかのパラメータを操作しているものと考えることができる。

しかしながら、メディアが多様になり、ブロードバンド伝送が普及するに伴って、メディアや圧縮方式と深くリンクした「透かし埋め込み技術」が提案されるようになってきている。このような動向に注目して、樹系図に示すような静止画像、動画、音、ドキュメント類のメディア毎に「透かし埋め込み技術」を調査することにする。

また、質的には異なるのだが、最近、注目を浴びている「透かしを利用した電子署名」および「攻撃に対する電子透かしの耐性評価」なども、樹系図上、各メディアと同レベルの階層に配置し、これを調査対象とする。

### (1) 静止画像

静止画像には2値画像、濃淡画像、カラー画像など多彩なメディア形態が含まれる。また様々な「透かし埋め込み技術や手法」が開発されており、静止画に適用される技術や手法は、電子透かし全般のなかでの基本的あるいは標準的な技術となっている。

ここでは、「技術や手法」からの視点、「メディア形態」からの視点、二つの視点から電子透かしについて述べてみる。

## 1) 「技術や手法」からの視点

### ・画素置換法

画像データの各画素は8ビットで構成され、画像の明るさを表す輝度情報が含まれている。白黒画像はそれぞれ異なる輝度情報を持った8枚のビットプレーンを重ね合わせたものと考えられることも可能である。最下位のビットは画像の特徴にあまり影響することのない冗長なビットプレーンである。画素置換法とは冗長な下位のビットプレーンに情報を埋め込む方式である。攻撃に対する耐性を高めるため、ビットプレーン拡散法、画素空間利用法などの改善方式が提案されている。

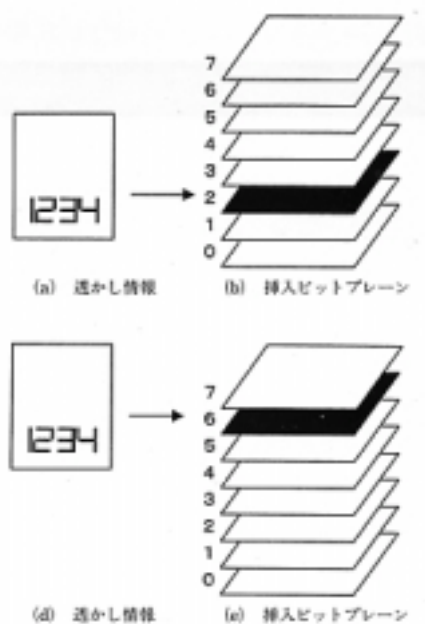


図1 . 画素置換法でのビットプレーンの考え方

(出典：電子透かしの基礎/松井甲子雄)

### ・周波数領域利用法

画像情報を(1)式のような周波数領域に変換し、冗長な周波数項を微小変更して「透かし情報」を書き込む方法である。図2に示すプロセスで情報が埋め込まれていく。このプロセスの中では、画像を周波数領域に変換するために「変換関数」が必要である。離散コサイン変換(DCT)など直交変換が利用されることが多い。

このこの変換の中で重要となるのは、「画像の適用する関数との関係」及び MPEG、JPEG といった圧縮に対する耐性である。

圧縮に対する耐性を高める方法として、直交変換を用いる方法がある。直交変換して周波数領域の係数が得られるが、この値を埋め込む情報に従って変換する方法である。変更後、逆変換によって元に戻せば、画像全体に変更の影響が散らばり、人間に知覚されにくくなる。MPEG、JPEG といった圧縮方法も、この直交変換である DCT を利用しているので、圧縮

しても残る周波数領域の係数値を変更することで、圧縮耐性が得られるわけである。  
また、直交変換としては、DCT だけでなく、高速フーリエ変換やウェーブレット変換なども用いられることが多くなってきている。

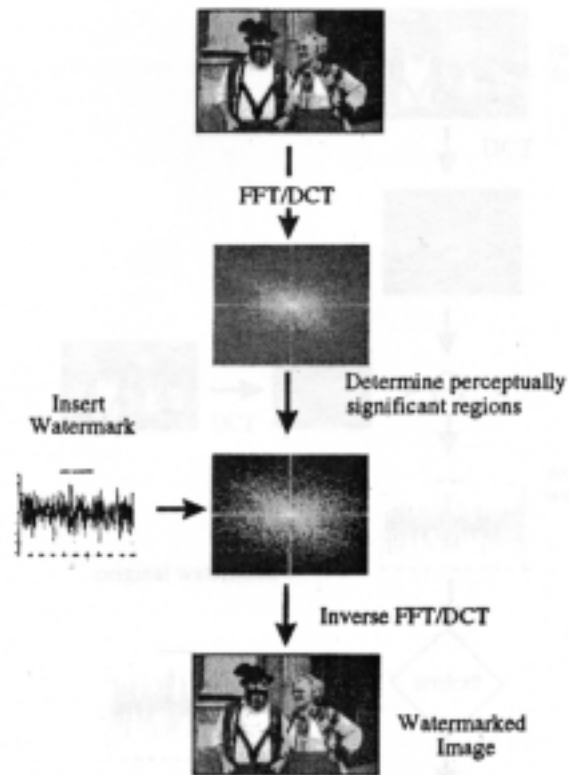


図 2 . I.J.Cox らの電子透かし挿入法

・濃度パターン法

プリンタなどで利用されている方法で、1 画素をいくつかのマイクロドット（マス）に分けておくことで、本来は、白黒 2 値情報しか持たない画素に階調情報を持たせるのが濃度パターン法である。1 画素をマイクロドットに分割することで冗長度が高くなる。ここに透かし情報を埋め込むのが「濃度パターン法」による透かし埋め込み技術である。これを図 3 に示す。また類似の方法に図 4 に示す「ディザ法」がある。

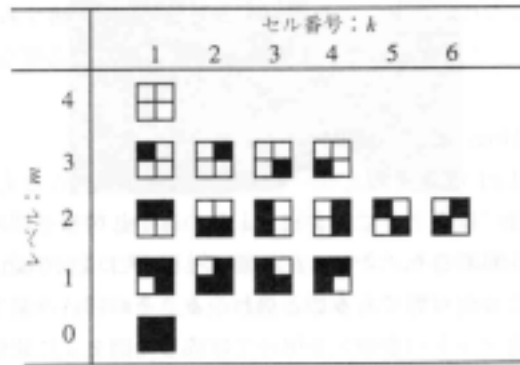


図3 濃度パターン法の埋め込みの原理  
(出典：電子透かしの基礎/松井甲子雄)

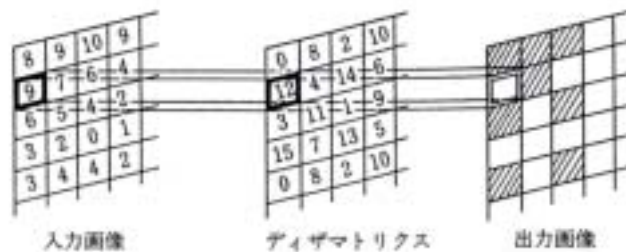


図4 組織的ディザ法の原理  
(出典：電子透かしの基礎/松井甲子雄)

## 2) 「メディア形態」からの視点

### ・カラー画像への電子透かし

カラーの自然画像といえば、通常、多値中間調カラー画像を意味しており、RGBの画素情報を持つ。R、G、B3色からなる画像信号はそのまま使われるだけでなく、さまざまな表現形式がある。それらの主たる目的は輝度（明るさ）と色の信号に分離することにより送信効率等を上げることにある。代表的なものに、カラーテレビで使われるYIQ表色系、JPEGやMPEGなどで用いられているYCbCr表色系がある。

基本的には電子透かしでカラー信号を扱う時、いかなる表色系であっても輝度成分(Y)に対しては多値画像への透かし法がそのまま適用できる。また、色(色差)成分(I,Q,Cb,Cr)を用いたカラー特有の透かし法もある。

### ・圧縮画像(JPEG)への電子透かし

先にも述べたが、JPEG圧縮にはDCT(離散コサイン変換)が使われることが多い。DCT方式の基本ブロックを図に示す。この処理過程において、透かし情報を埋め込むことができる場所を考えると、最も基本的な方法として、DCT変換時の量子化誤差を利用することである。あるいは、DCT係数の中の指定周波数成分に透かしビットを直接埋め込む方法もあ

る。また DCT のための量子化ステップサイズの最適値は入力画像および画像表示装置に依存してユーザーが決めることになっているので、このパラメータを透かしビット楯で制御することができる。

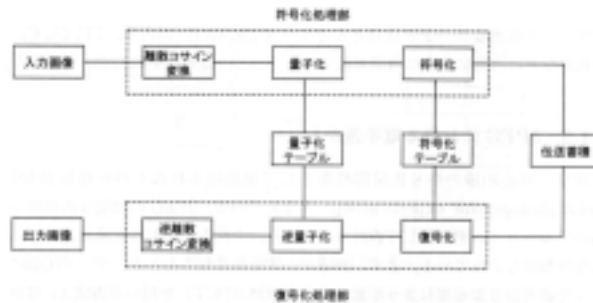


図5 . DCT方式の基本処理過程  
(出典：電子透かしの基礎/松井甲子雄)

・ 3次元画像への電子透かし

静止画像の応用として、コンピュータグラフィックス(CG)画像やバーチャルリアリティ(VR)画像がある。これらは一般に三次元(3D)画像としてモデル化されている。

3次元モデルの形状は、点、線、面、ソリッド(中身の詰まった立体)などの形状プリミティブの組み合わせで定義される。形状プリミティブには、Non-Uniform Rational B-Spline(NURBS)曲線や曲面、ポリゴン(多角形)、ポリヘドロン(多面体)、ボクセル等がある。また形状には頂点に付随する法線ベクトル、色、テクスチャ座標等の属性が付けられていることが多い。

3次元画像への電子透かしとしては、3次元形状を表現するために最も広く利用されるポリゴン(多角形)メッシュへとその属性への透かしの埋め込む方法や、自動車などの形状設計CADで多用されるパラメトリック曲線・曲面に対する透かし埋め込み方法等が考えられる。このうちポリゴンメッシュへの透かしの埋め込み方法には3つが考えられる。

- A. 座標値の変換による埋め込み：ポリゴンメッシュによって定義された形状の座標値を埋め込みの対象とする。座標値そのままでは、たとえば平行移動や回転で消えてしまう。あるクラスの幾何変換、たとえば相似変換やアフィン変換に対する不変量を利用して透かしの埋め込む手法などがある。
- B. 頂点座標への変換領域での埋め込み：3角形メッシュをウェーブレット変換し、その変換領域の係数を操作して情報を埋め込む。
- C. 位相の変更による埋め込み：3Dモデルのトポロジ、つまり頂点の結合関係を変更して埋め込む透かしもある。

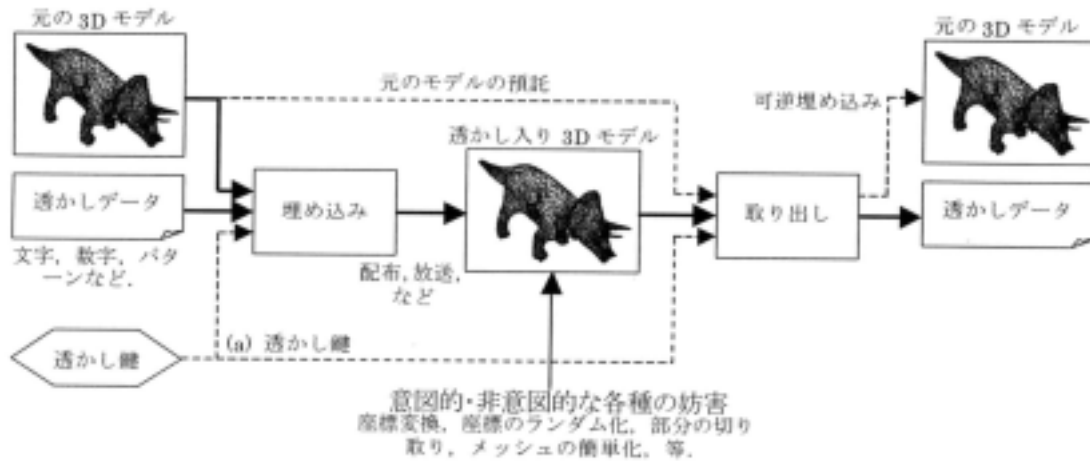


図6 三次元画像への電子透かしの埋め込み方法

(出典：メディアデータ型としての3次元モデルとその電子透かし技術 / 大淵竜太郎)

・ファクシミリ画像への電子透かし

世界中で広く利用されているファクシミリは国際電信電話諮問委員会(CCITT)が定めた G3規格に基づいている。G3規格では、必須機能として Modified Huffman(MH)法とよばれるランレングス符号化方式と、オプション機能として Modified READ(MR)法とよばれる二次元符号化法の二つの符号化方式を提示している。従って、ファクシミリ画像への電子透かしの埋め込み方法としては、多値画像の輝度成分に相当するランレングスへの透かしの埋め込み方法と、位相成分に相当する上下ラン間のズレ幅への透かしの埋め込み方法が考えられる。

G3 端末の上位機種として G4 規格が CCITT から発表され、後身の国際電気通信連合 (ITU) においても引き継がれている。G4 機の符号化方式は modified-modified READ (MMR)法とよばれるが、MMR 法は基本的に MR 法と同じであり、透かし情報の埋め込みには全く支障を及ぼさない。

ディザ画像は、白画素と黒画素が交互に繰り返し出現することが多く、ディザ画像を MH 符号化しても効率よく伝送することができない。ビットインターリーブ法は、分断されたランを結合して効率よく符号化する方式である。従って、このビットインターリーブ法による透かしの埋め込み方法も考えられる。

## (2) 動画像

インターネットの高速化にともない、動画像は最も期待されるデジタルコンテンツである。動画像は静止画像が連続的に表示されていると考えることができるから、基本的には静止画像の応用ということもできる。しかし、動画像は静止画像と比較してファイル容量が大きくなるため圧縮技術が必須であること、コンテンツの内容が時間経過とともに変化し、その前後の画像の差が小さい場合が多いなどの特徴がある。

動画像には MPEG という国際標準規格が適用されるのが一般的である。MPEG は動画のフレーム間の構成、フレーム内のデータの階層構造、圧縮方式などを規定する。MPEG ではフレーム間圧縮という圧縮原理が導入されており、フレーム間の差分が動きベクトルや予測符号というデータに変換される。これらのデータは、幾つかのレイヤからなる階層構造をもつデータ形式に表現される。また、MPEG は普及段階にある MPEG1、MPEG2 形式と、モバイル通信にも応用可能な MPEG4 に大別できる。

動画像では MPEG に深く関る「透かし埋め込み技術」が特徴であり、下記の3つの技術が中心となっている。

- ・ 時間軸埋め込み法（フレーム間の構成を利用）
- ・ 空間軸埋め込み法（画像の圧縮を利用）
- ・ レイヤ構造埋め込み法（MPEG のデータ構造を利用）

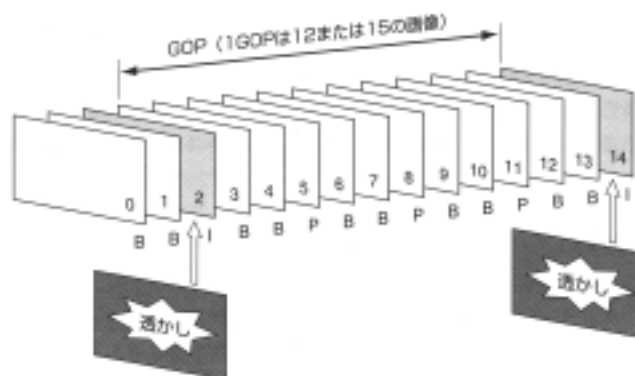


図7 MPEG の特定フレームに電子透かしを入れる方式の考え方  
(出典：電子透かしとコンテンツ保護/小野東)

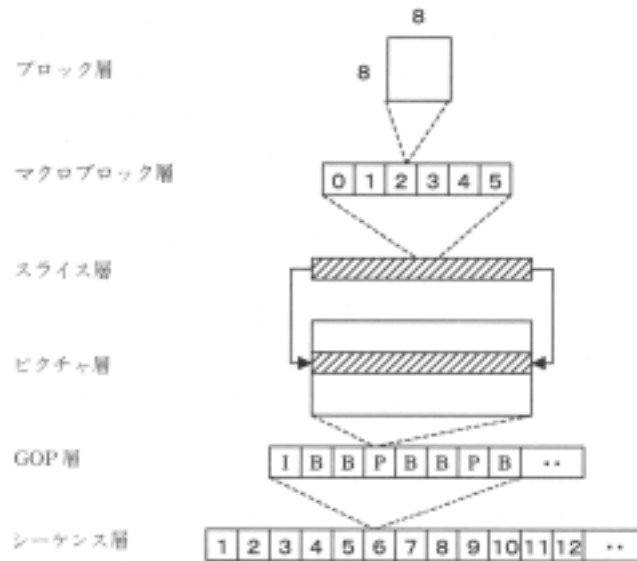


図8 MPEGにおけるデータ階層構造  
(出典：電子透かしの基礎/松井甲子雄)

### (3) 音

音や音楽への電子透かしは、静止画像の二次元データに対し、一次元のデータとして捉えることができる。また、大きな音の前後の小さな音は聞き分けられない、位相の変化に鈍感、高音や低音に鈍感など、耳の生理的特性を積極的に活用した埋め込み技術を採用していることが多く見られる。

アナログの音はサンプリングされてデジタルデータとなる。このデジタルデータを非圧縮で利用する場合もあるが、MP3に代表されるような形式に圧縮されて利用するのが一般的なので、圧縮方式に特化した透かし方法もある。また、音声のように内容が伝われば音質が悪くても問題にならないものと、音楽の様に音質の劣化が問題になるものとに大別して扱った。

音データは、周波数領域に変換しない埋め込み方式(量子化前)と周波数領域へ変換してから埋め込む方式(量子化後)とに分類できる。量子化前の埋め込みとしては生理的特長を利用した「マスキング法」などがあり、量子化後の埋め込みとしては、係数に変更を加える「係数操作型」、位相を操作する「位相操作型」などがある。

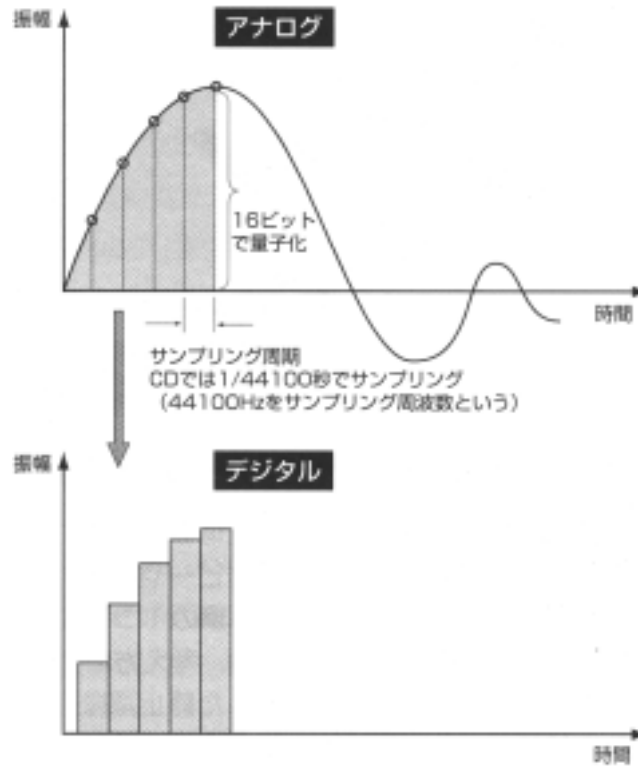


図9 PCM方式とは  
 (出典：電子透かしとコンテンツ保護/小野東)

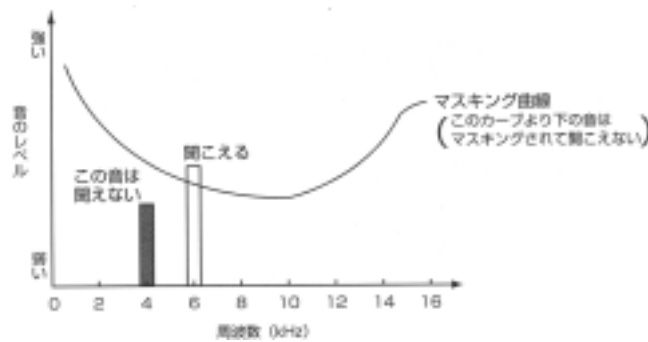


図10 聴覚のマスキング特性  
 (出典：電子透かしとコンテンツ保護/小野東)

#### (4) ドキュメント

ドキュメントへの電子透かしとして、文書、ソフトウェア、電子地図に対する電子透かしを取り上げた。

文書への電子透かしは、単語の集合からなる欧文と、基本的に字間のスペースがない和文とに大別できる。欧文を対象とした電子透かしでは、単語間のスペースを制御する「ワード

シフト法」がある。和文を対象とした電子透かしでは、文字の回転を制御する「文字回転法」、文字の大きさを制御する「文字伸縮法」などがある。

ソフトウェアへの電子透かしは、ソースコードに新たな代入文を挿入する「変数利用法」があり、規格化されたオブジェクトコードの冗長性を利用した「ダミーコード利用法」がある。

電子地図は、地図データをベクトルデータとして扱うことが多く見られる。電子地図への透かしは、このベクトルデータに対して、地図やベクトルの特性を利用した方法がある。



図 文字の回転と縮小  
(出典：電子透かしの基礎/松井甲子雄)

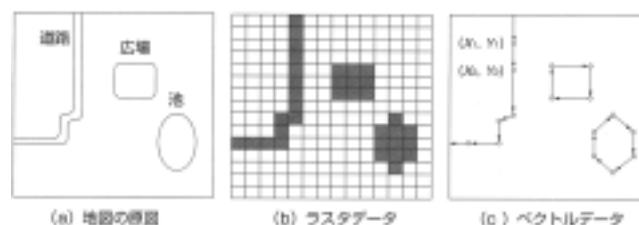


図 1 2 地図データの表現形式による違い  
(出典：電子透かしとコンテンツ保護/小野束)

### 3. 透かしの応用技術

「透かし技術の応用」とはまさにコンテンツビジネスにおける「商用システム」と考えて差し支えない。電子透かしの利用形態は用いられるコンテンツの種別、サービスの仕組みなどにより様々であるが、埋め込まれた情報の利用方法を中心に分類すると以下のような応用モデルに整理できる。

これらの応用モデルの多くは「高度な情報セキュリティ機能」を装備したコンテンツビジネスに関するものである。電子透かしの技術を単独で利用しているのではなく、電子署名、認証局、公開鍵暗号方式など他のセキュリティ対策を組み込んだ複合システムとして構築されているものが多い。

「商用システム」とはいえないが、電子透かしを利用して暗号のやり取りを行う利用も、一部で、考えられている。デジタルメディアを利用した「現代版ステガノグラフィー」である。

- ・ 著作権主張モデル
- ・ 原本性確認モデル
- ・ 附属情報付加モデル
- ・ 機器制御モデル
- ・ 現代版ステガノグラフィー

#### (1) 著作権主張モデル

コンテンツの著作権者を示す情報やコンテンツの購入者、利用者に関する情報を電子透かしで埋めこみ、著作権者がコンテンツの著作権を主張するために、その透かし情報を用いる応用例を「著作権主張モデル」という。このモデルは以下のようなケースに適用されている。

- ・ 不正利用の心理的抑圧
- ・ 不正利用の監視
- ・ コンテンツ配信
- ・ 超流通

- ・ 不正利用の心理的抑圧

図13は不正利用抑止システムを示したものである。

コンテンツを販売、流通させるとき、コンテンツに著作者、購入者など著作権に関する情報を透かし込むことで、不正利用の心理的な抑制を狙う手法である。また、購入者情報を付加しておくことで、不正利用者の特定と権利主張が可能となっている。

さらに、不正利用の心理的抑圧というケースにおいても、画像に透かしデータを入れるだけでなく、

- A. 会員のみ配布する専用ビューワで複製のみ画像を利用できる場合において、この専用ビューワでも見えない透かしの埋め込む、

B. 会員のみで透かしの解除キーを渡し、このキーを用いて画像を利用できる場合において、キーを使用した際に自動的に新たなる会員情報が電子透かしとして埋め込まれる。など、二重に透かしを入れることで、心理的抑圧だけでなく、実質的に不正利用者の発見に効果する方法も検討されている。

埋め込まれるデータとしては、コンテンツ ID と呼ばれるコードが用いられる場合がある。コンテンツ ID とは、著作者、購入者その他コンテンツ管理データと紐付けされる画像ごとにユニークな識別子のことであり、コンテンツ ID を透かしとして埋め込めば、少ない情報量の埋め込みで済ますことが可能になり、その結果としてメディアの品質の劣化を防ぐことも可能である。このコンテンツ ID そのものを暗号化しておけば、解読が困難となり、不正利用の発見に対して効果のある電子透かしとなる。

#### ・不正利用の監視

不正の監視方法は以下のような方法が提案されている。

- A. 透かし読み取り機能を持つ監視ロボットにより、Web サイトのページに含まれているコンテンツをトップダウン的に探索する監視ロボット型、
- B. 特定ノードのゲートウェイや、サーバーに透かし読み取りフィルターを入れて通過するコンテンツをすべてチェックする特定ネットワーク監視型、
- C. 利用者のブラウザのダウンロードモジュールに透かし読み取りツールをあらかじめプラグインしておき、ダウンロードしたコンテンツ ID とアクセスサイトの URL をコンテンツ ID 管理センターに通知し、チェックするボトムアップ的な利用者協力型

に分類される。

また、上記分類のうち監視ロボット型についてはこうした不正利用監視をサービスとして提供するという技術も提案されている。このサービスにおける中核的な機能は、(1)不正利用探索機能、(2)不正利用判定機能、(3)不正利用報告機能、である。そして、不正利用が発覚した場合には、掲載削除通告が法律事務所や第三者機関からなされる。

#### ・コンテンツ配信

2次配布者、および電子透かしの埋め込むサーバーが不正利用する場合の防御策が提案されている。これは、著作者の著作権を守ると同時に、購入者が不正コピーを購入させられるというリスクを防止するためのものである。この技術のポイントは、

- A. 著作者、配布者および購入者など関係者全員が電子署名をする
- B. サーバーの管理者が埋め込む方法や場所を決定するのではなく、サーバーにバンドルされた電子透かし埋め込み用プログラムが自動的に起動し、署名内容に依存して埋め込み方法や場所を決定する

などの方法を通じて不正を防止するというものである。関係者全員の署名がそろわないと正式な複製ができないために、単独もしくは関係者のうちの複数者での不正は不可能になる。また、サーバーは、透かしの埋め込む方法や、埋め込み場所についての情報がないために不正が不可能となる。

#### ・超流通

不正利用を防御するという考え方とは逆の発想が超流通である。この超流通の考え方は、コピーを防御するという考え方ではなく、逆に不正をすることなく自由にコピーができるようなシステムを構築するというものである。コンテンツ識別子や課金情報、権利者情報などが記載された超流通ラベルという電子的な情報が電子透かしとして付加される。利用者は、画像をコピーした場合に自動的に課金されるシステムである。コンテンツがあふれ、また、データのコピーが自由に行える時代に適合した新しい流通システムの考え方である。

## (2) 原本性確認モデル

デジタルデータの編集はフォトタッチツールや電子ファイル編集ツール等の使用で極めて容易になった。そのためデジタルデータの原本性は従来の銀塩写真や紙の書類に比較して低く、証拠としての能力に乏しいという問題が生じている。

デジタルコンテンツの原本性を確認するために、電子透かしを用いる下記のような応用例が提案されている。これらの応用例では、コンテンツの原本性を示す情報や特殊なパターンが埋め込まれ、改ざんや編集が行われて場合には、容易に埋め込まれた電子透かしが破壊されてしまう方式が取られているものが多い。また、他の情報セキュリティー方式と電子透かしと連携させることで原本性を保証する仕組みを構築しているものも多い。

- ・ 電子署名を使った写真画像改ざん検知
- ・ デジタル画像の改ざん位置検出
- ・ 暗号化、復号鍵を使った改ざん部分情報の復元
- ・ 認定マークを使ったホームページ真正性確認

図14は、ホームページ公開での「なりすましを防止」するためのシステムを示したものである。認定局より授与された、ホームページ公開者の URL とその電子署名が透かし込まれた認定マークをホームページに貼付することで、真正性を閲覧者に通知できる仕組みになっている。

- ・ 電子署名を使った写真画像改ざん検知

本技術に対応して、いくつかの技術が提案されている。

- A. 二次加工に耐性のある電子透かし技術を用いて情報量が少なく済むコンテンツID(著作権情報とリンクさせている識別子)を電子透かしとして埋め込む方法
- B. 電子透かしを埋め込むだけでなく、画像の下部の目立たないところに署名を添付してこの署名を誰でも簡単に検証可能する方法
- C. 画像にサインをする際に、そのサインにペンの筆圧やペンの傾きデータを電子透かしとして埋め込んで真贋性を判定する方法、

とくに、BやCは、著作権を可視的と非可視的との二重の方法により埋め込むことにより、改ざん検知を確実なものにするという提案である。

- ・ デジタル画像の改ざん位置検出

この例として、(A)デジタル画像の部分をオブジェクト化し購入者ごとにすこしずつ位置を変

える操作を施して画像を作る、(B)カラー情報などのビットデータを画像全体にわたって少しずつ変更する、などの方法によりデータを個体化する方法があげられる。この場合、オリジナル画像と改ざん後の画像を比較すれば、誰が、どの部位を改ざんしたかの情報が得られる。この方法は、切り取り耐性に優れる方法である。

### (3) 附属情報付加モデル

著作権主張モデルや原本性確認モデルはデジタルコンテンツ保護のための電子透かしの応用例である。それに対して、デジタルコンテンツの関連情報または附属情報を電子透かしとしてそのコンテンツに埋め込み、コンテンツの利用時に透かし情報を読み出して、参照・利用するという形態がある。これが附属情報付加モデルである。付加される情報は、下記に示すようにコンテンツに関係する内容が多いが、一般的には、コンテンツとは全く無関係の情報が付加されている。透かし複合のソフトウェアの秘匿性が保たれるならば、まさに暗号の世界である。

- ・ 撮影情報付加
- ・ 説明付加
- ・ 字幕付加
- ・ 吹き替え音声付加
- ・ CM 付加

#### ・ 撮影情報付加

医療の現場では、カルテや診断画像などのデジタル化が進んでいる。しかしながら、このようなデータはそれぞれ単独にて保存すると管理が複雑になる。もし、単一のファイルとして管理されるとデータ管理が容易になる。これを実現する方法として、電子透かし技術を応用し、カルテに診断画像データを埋め込むという方法が提案されている。この方法は、さまざまなデータ管理に応用展開できる方法であり、電子透かしの新しい利用法と考えられる。

#### ・ 説明付加

音楽情報に歌手名、曲名、作詞や作曲家のその他録音に関するさまざまなデータを埋め込むという必要性から、量子化ノイズを消すためのディザ信号の代わりに文字情報を JIS コードで 2 進符号に変換したものをを用いる方法が提案されている。周波数成分に及ぼす影響は小さく、また音質におよぼす影響はほとんどないことが実証されており、このような技術を用いれば音楽情報に文字情報を付加することが可能になる。音楽情報に埋め込むデータは何でもよく、またこの埋め込まれたデータに暗号化が施されていれば、新しい暗号化の技術としても用いることができる。

### (4) 機器制御モデル

電子透かしが埋め込まれているマルチメディアコンテンツに関係する機器、例えば、DVD プレーヤなどを制御するために電子透かしを用いる応用例を機器制御モデルという。下記に

示すようにいくつかの方式が提案されている。

- ・コピープロテクション
- ・有害コンテンツのフィルタリング
- ・メタ電子透かし

図15はコピープロテクションシステムの概要を示したものである。コンテンツにプレーヤなど機器への制御コードを透かし込んでおくことで、2回目以降のコピーを禁止するという形で、不正コピーを物理的に禁止する方式である。この方式は、電子透かしとコンテンツを制御するOS、再生ソフトウェア、ハードウェアなどが一体となった対策があって始めて機能するものであり、各業界代表による標準規格化の推進が非常に重要である。特に、DVDでの規格標準化は活発で、電子透かし、RPC(Regional Playback Control)、CSS(Contents Scrambling System)などを取り込んだ使用が論議されている。

・コピープロテクション

DVDなどの動画のコピープロテクションに対して、デジタルカメラなどで撮影した静止画に撮影時に著作権情報を自動的に電子透かしとして埋め込む、という考え方が提案されている。これは、デジタルカメラで撮影された撮影データがそのままホームページに載せられることが多いことを配慮して撮影時に埋め込みを行うというものである。電子透かしとして埋め込むデータは、カメラ内部のROMに保存されているカメラの識別子や日付、画像の著作権に属するデータなどである。新しい機器制御モデルとして位置づけられる。

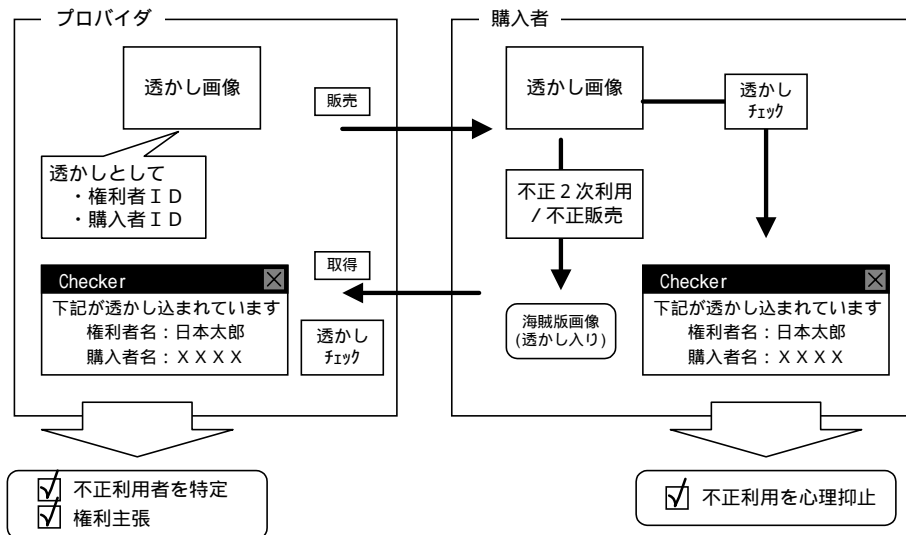


図13．不正利用抑止システム

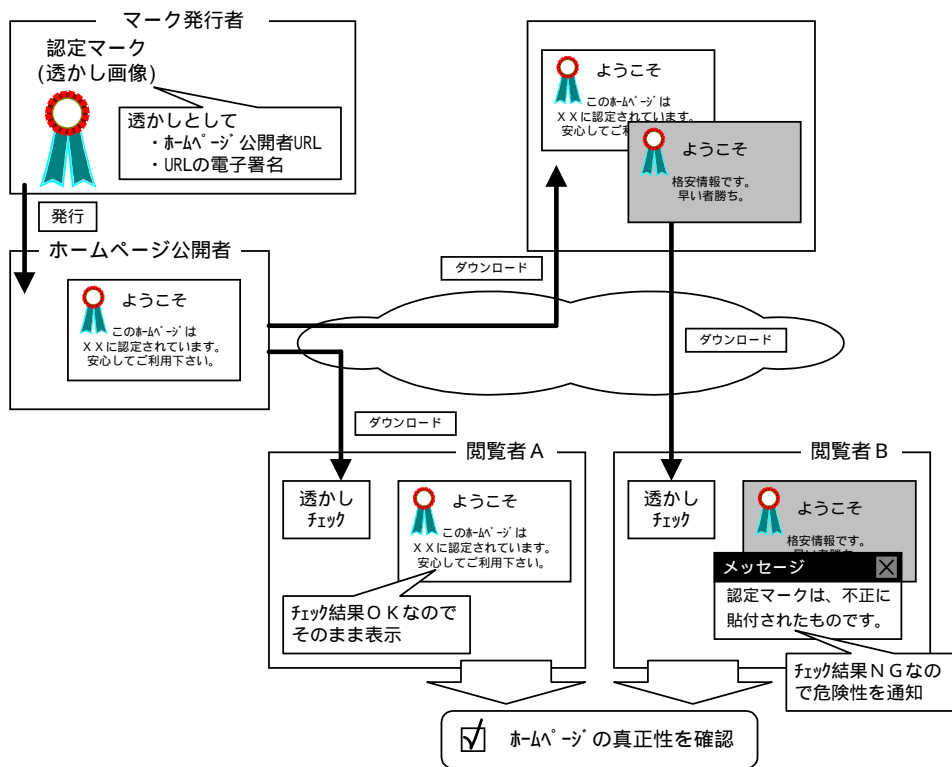


図 1 4 . 認定マークを使ったホームページ真正性確認システム

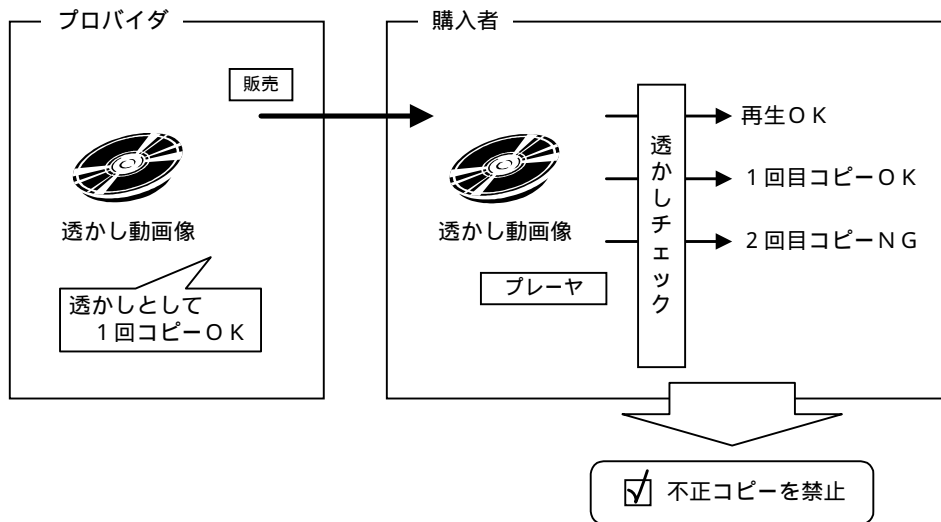


図 1 5 . コピープロテクション

## (5)現代版ステガノグラフィ

ステガノグラフィ (steganography) は、古くは西暦前のギリシャ時代に起源を求めることができる。その意味は、こっそり書き込むことである。ステガノグラフィの有名な例として、「奴隷の頭髪を剃り込んで、秘密のメッセージを頭皮に入れ墨し、頭髪が伸びた後でその奴隷を敵陣に放ち、味方と交信させた」という逸話が残っている。その後、時代を追って透明インク、マイクロドットなどの秘匿技術が発明され、20世紀初頭には紙を媒体とするアナログ・ステガノグラフィが盛んであった。今日のデジタル化時代においては、情報通信網と暗号化技術の発展と相俟ってほとんどがデジタル・ステガノグラフィである。

ステガノグラフィの定義は、「秘密情報を何気なく別のメディア (情報媒体) に埋め込み第三者にその存在すらも気づかせない」というものである。秘密情報を秘匿する方法、即ち埋め込み方法を技術分類的に見ると、デジタル・ステガノグラフィも電子透かしも何ら変わることはない。デジタル・ステガノグラフィを埋め込み方法によって概略分類すると、

- ・ 代入法 (substitution techniques)
- ・ 変換法 (transform domain techniques)
- ・ 構成法 (constructive techniques)

の三つに分けられる。

代入法は、置換法とも呼ばれ、メディア (画像、テキスト、音声など) の冗長部分あるいはノイズ性部分に秘密情報を埋め込むというもので、画像で例をとれば、LSB (Least Significant Bit; 最下位ビット) からなるビットプレーンにこの代入法を適用することができる。ただ、画像や音声の量子化データは圧縮されることが多く、代入法によるとノイズ成分に相当する下位ビット情報は圧縮操作の対象となり、埋め込み情報はそのまま消去されるという欠点を有する。

変換法はこの問題を解消するのに利用され、代表的なものが周波数領域変換法である。したがって、カラー画像や音声などへの情報埋め込みには変換法が用いられる。構成法は、メディアの量子化ノイズに注目し、メディアの特徴を捉えた擬似ノイズモデルを利用して情報を埋め込む方法がある。

現在、インターネット空間の中で膨大なコンテンツが飛び交っている。このなかに現代版ステガノグラフィを駆使した暗号 (cryptography) がこっそりと書き込まれているかもしれない。