

## 利便性を重視した著作権保護方式

平野秀幸、小谷誠剛、小野越夫

株式会社 富士通研究所

従来の著作権保護システムは著作物(デジタルコンテンツ)管理者に重点が置かれていたので、サービス面において利用者の使い勝手が悪かった。そこで、管理者を含む全てのシステム利用者の利便性に関し以下の3点に着目して改善策を検討した。(1) 既存の利用者環境での処理機能高速化、(2) 情報の一元管理によるコンテンツ利用上のトラブル予防、(3) 柔軟性を持つアクセス制限。結果として、利用者の利便性を損なわずにデジタルコンテンツの不正利用防止を可能とする著作権保護方式を考案し、その方式に基づいた静止画の著作権保護システムのプロトタイプを開発した。

Concept and prototype system of copy management and protection method with convenience

Hideyuki Hirano, Seigo Kotani, Etsuo Ono, Fujitsu Laboratories LTD.

abstract

We have developed a new copy management and protection method with convenience for every user. A prototype of our method proved the feasibility and the efficiency. We believe the method would solve the problems that traditional copy protect system have.

- key word -

Water Mark Intellectual Property Management Protection Copy Protection Cipher

### 1. はじめに

デジタル画像入力用 CCD センサの高性能・低価格化、ストレージの大容量・低価格化にあわせ、通信コストの低価格化により、一般家庭においてもデジタルコンテンツを利用できる環境が整いつつある。又、パソコンの低価格化や高性能化に伴ないパソコンとネットワークが普及し、誰でも簡単に、高品質のデジタルコンテンツを流通できるようになった。その結果、商品価値が高く、高品質なデジタルコンテンツを低コストで複製でき

るようになった。

従来、デジタルコンテンツの著作権者の権利を守る仕組みに関し、活発な研究が行われてきており、デジタルコンテンツに著作権情報を埋め込み利用者の正当性を確認する電子透かし技術[1],[2]やカプセル技術[3],[4]等が報告されている。

しかし、従来の研究では下記の課題を解決するまでに至っていない。

### (1)高精細の画質を持つデジタルコンテンツの検索・閲覧処理性能の低下

200万画素数以上の入力性能を持つカメラやスキャナなど高性能な入力装置が普及している(下図参照)。画像入力された高精細なデジタルコンテンツ群を記録するストレージにおいて、画像検索や検索後の画像閲覧性能は、デジタルコンテンツの画素数、パソコン・表示機器の性能に依存する。したがって、従来のパソコンでは検索・閲覧処理能力が不足し、高精細画像の使い勝手が悪かった。



### (2)コンテンツ利用上のトラブル

従来の著作権保護方式では再生処理に関連する情報(以下許諾情報と呼ぶ)と配布デジタルコンテンツを分離しており、許諾情報がファイル形式の場合、利用者の操作ミスやパソコンの障害により、前記許諾情報ファイルを消失させる可能性がある。

### (3) 限定されたアクセス制限機能

不正利用防止や不正コピー防止機能は利便性を実現する機能とトレードオフの関係である。従来の著作権保護システムでは著作者(管理者)に重点を置いていたので、入手したデジタルコンテンツの使い勝手に課題を残していた。又、アクセス制限を実現するアクセス許可条件の種類が少なかったので個々のコンテンツの価値や利用環境等に応じて、コンテンツ毎に異なるアクセス制限を実現するまでに至っていなかった。したがって、単純で限定されたアクセス制限しか実現できず、

利用者(管理者)のサービスを低下させていた。

## 2. 提案する著作権保護方式

本章では、提案する著作権保護方式について説明する。

前章までに述べたように、ハードウェアの高性能化や低価格化によるデジタルコンテンツの利用環境の変化を考慮し、使い勝手が悪くならないサービスの実現を目指した。本方式ではデジタルコンテンツの利用を正当な利用者に限定し不正利用や不正コピーを防止することをポリシーとし、デジタルコンテンツを暗号鍵で暗号化し暗号鍵を管理する手法を用いる。

今回、下記3点のサービス実現を指針とし、従来技術同様に、デジタルコンテンツを不正利用されない著作権保護方式を提案する。

### (1)既存の利用者環境での処理機能高速化

既存の利用者システムで利用可能となる環境(Microsoft社などが提供するファイルマネージャ機能を備える汎用ブラウザ)において、配信されたデジタルコンテンツの概要を高速検索・閲覧できる画像フォーマットを利用する。上記画像フォーマットを利用することで、利用者は特別なファイル管理ソフトを起動することなく、入手したデジタルコンテンツの画像概要を理解できる。

又、閲覧・検索対象となる画像とデジタルコンテンツを一体化することで、高精細なデジタルコンテンツであっても、閲覧・検索の処理時間をより短縮化できる。前記閲覧・検索対象画像は、デジタルコンテンツと関連付け可能な画像であり、本方式では見本画像と呼ぶ。見本画像を備えることで、入手したデジタルコンテンツ群の中から、画像理解機能を備えた検索ロボットにより、所望のデジタルコンテンツを高速検索することが可能となる。

画像フォーマットは見本画像と暗号化デジタルコンテンツを同一ファイル化できることを特徴とする(図1参照)。

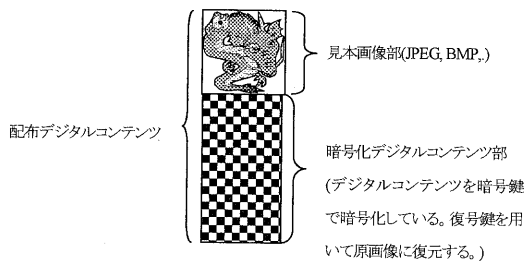


図 1. 配布デジタルコンテンツ(作品 1)画像フォーマット概念図

Windows 2000 のブラウザ(Explorer)において、ホルダー内のデータ(JPEG, BMP,PPT,XLS,...)を thumbnail 化し画像表示する新機能が追加された。

例として、配布デジタルコンテンツ(作品 1.jpg,作品 2.jpg)等を格納したホルダー(Test-Holder)を表示した(図 2 参照)。

Explorer は作品 1,作品 2 の見本画像部を対象として thumbnail 画像を作成・表示する。従って、見本画像部の画像サイズを小さくすることで、Explorer は高速処理することができる。

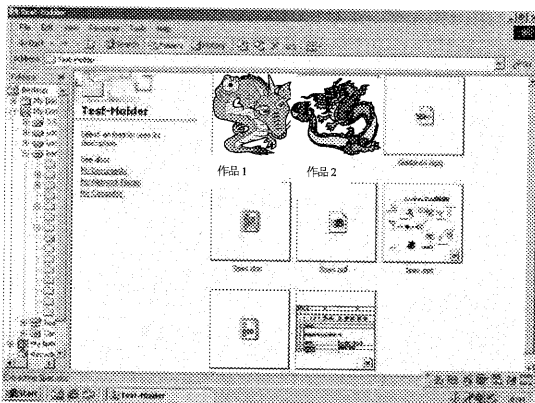


図 2. Explorer(Windows 2000)でフォルダ(Test-Holder)を表示した例

## (2)情報の一元管理によるコンテンツ利用上のトラブル予防

正当な利用者がデジタルコンテンツを閲覧利用するために、デジタルコンテンツの復号に関する情報を電子透かし化し保管する方式を開発した。

従来の著作権保護方式では復号処理に関する情報(以下許諾情報と呼ぶ)と配布デジタルコンテンツを分離しており、許諾情報がファイル形式の場合、利用者の操作ミスやパソコンの障害により、前記許諾情報ファイルを消失させる可能性がある。又、前記許諾情報ファイルが不測のフォルダパスに移動されているなど利用環境が変化した場合にも、ユーザが対応できない可能性がある。

そこで、個々の情報をコンテンツ毎に一元管理し、管理情報とコンテンツを一体化する仕組みとした。管理情報はコンテンツ ID[1] 等デジタルコンテンツを特定化するリンク情報、許諾情報などとする。又、見本画像と管理情報の一体化に不可視型の電子透かしを利用することにした(表 1 参照)。

配布デジタルコンテンツは見本画像部と暗号化デジタルコンテンツ部から構成されており、暗号化デジタルコンテンツ部を閲覧する場合、見本画像部に埋め込んだ透かし情報を用いて、暗号化デジタルコンテンツ部を復号・表示する。又、前記透かしのリンク情報を利用することで、暗号化デジタルコンテンツ部の置換えによる不正利用を検出できる(図 3 参照)。

結果として、許諾情報の消失防止と暗号化デジタルコンテンツ部の不正利用防止を期待できる。又、電子透かし第 4 番目の役割を利用することで、不可視型電子透かしの応用範囲が広がる可能性を持っている。

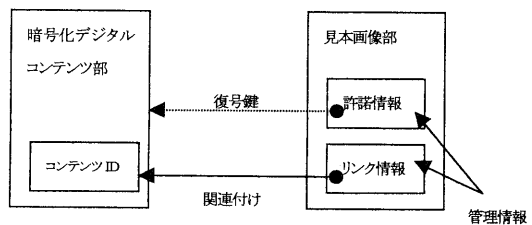


図 3. 管理情報の一元化概念図

表 1 電子透かしの役割

項番	電子透かしの役割
1	利用したいデジタルコンテンツの検出
2	疑わしいデジタルコンテンツの検出
3	再生・コピー制御
4	管理情報の保管

(3) 柔軟性を持つアクセス制限

作品価値や利用用途毎にデジタルコンテンツの利用環境を柔軟的に制限するために、数種類のハードウェア認証情報(ハード ID)やソフトウェア認証情報(ソフト ID)を扱える仕組みとした。選択した個々の認証情報(ID)によって、デジタルコンテンツ毎に異なるアクセス制限を実現することができる(図 4 参照)。

ハード ID の効果として、特定の記録媒体、特定のパソコンハード環境など、利用目的別に制限できる。ソフト ID は従来のパスワードと同様に ID 保有者を利用制限できる。上記 ID を利用することで、管理者はデジタルコンテンツの種類や品質に応じデジタルコンテンツの利用範囲を設定でき、利用者は利用環境を選択可能となる。

ID や ID 種別は許諾情報として見本画像に不可視型電子透かしとして埋め込まれる。利用時に透かし抽出、情報比較され、デジタルコンテンツをアクセス制限する。

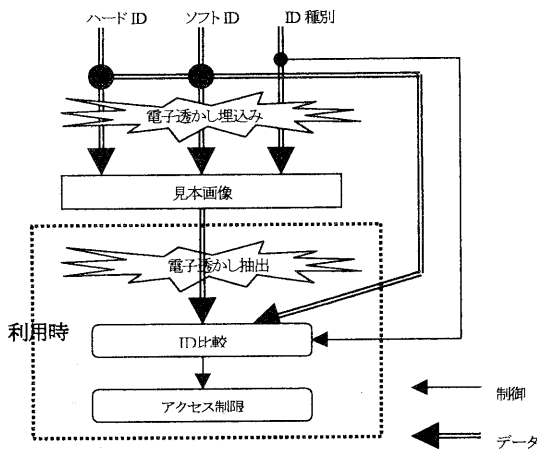


図 4. 一コンテンツに対応するアクセス制限の概念図

3. システム構成

本方式を実装したプロトタイプシステムの構成を図 5 に記す。本システムは配布デジタルコンテンツ作成部とデジタルコンテンツ利用部から構成される。上記2つの構成要素の機能概要を以下に記す。

尚、見本画像部と原画像は JPEG や BMP などの論理構造を備えた画像フォーマットであり、配布デジタルコンテンツは見本画像部と暗号化原画像の一体化画像である。又、上記画像フォーマットは汎用ブラウザ (Explorer など)において見本画像部だけが処理対象となることを特徴とする。

配布デジタルコンテンツ作成部では、デジタルコンテンツ 1 を利用者毎に異なる認証情報 A, B でアクセス制限した配布デジタルコンテンツ 1A, 1B を作成する。上記認証情報 A, B はデジタルコンテンツ利用部からそれぞれ取得される。

デジタルコンテンツ利用部では、配布デジタルコンテンツのアクセス制限情報を個々の利用者認証情報と照合する。認証情報が合致した時のみ暗号化コンテンツ部を利用できる。

上記構成要素の詳細機能を以下に記す。

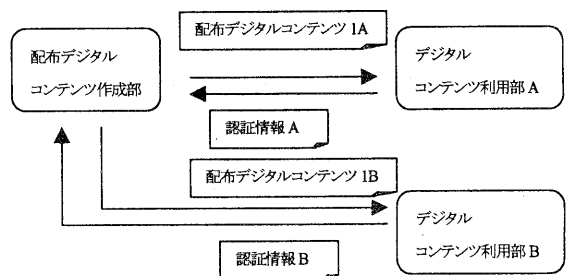


図 5. システム構成

3.1 配布デジタルコンテンツ作成部の機能

コンテンツ ID[1]関連情報を不可視型電子透かしとして原画像に埋め込み、許諾情報と暗号化原画像を一体化し、原画像の内容を理解できる配布画像を生成することを目的とする。下記の処理手順で実行される(図 6 参照)。

共通鍵暗号化方式を用い、管理者が発行しコンテン

ツ毎にユニークな共通鍵をコンテンツ鍵とする。原画像の暗号/復号化を目的とする情報をコンテンツ鍵、コンテンツ鍵を認証情報で暗号化した情報を秘匿鍵と呼ぶ。又、種々のハードIDやソフトIDの中から選択した情報を認証情報とし、認証情報の種別情報をID種別情報と呼ぶ。認証情報として以下の情報を利用する。

- ・ハードID: Media ID (媒体固有のシリアル番号付き光磁気 DISK:セキュリティ機能付き GIGAMO 装置)  
([http://www.fimworld.ne.jp/product/hard/magnetic/fmpd25ls\\_1.html](http://www.fimworld.ne.jp/product/hard/magnetic/fmpd25ls_1.html))
- ・ソフトID: パスワード

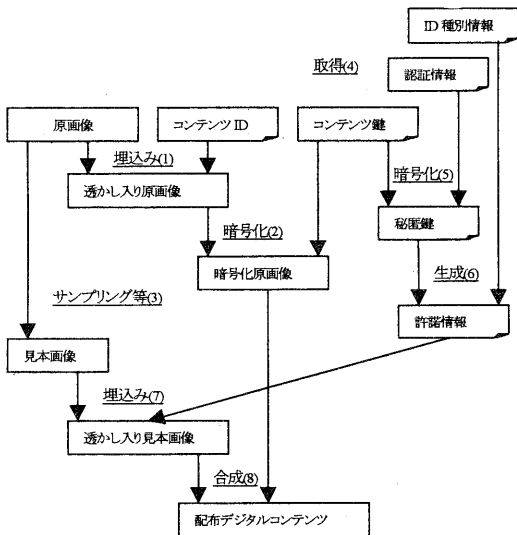


図 6. デジタルコンテンツ作成部処理手順

- (1)原画像に著作権者情報などのコンテンツ ID[1]を不可視型電子透かし(周波数変換型)として埋込む。
- (2)透かし入り原画像をコンテンツ鍵で暗号化(DES)し、暗号化原画像を生成する。
- (3)原画像からサンプリング化(線形補間)等で見本画像を生成する。
- (4)認証情報(ハードID,ソフトID)を取得する。
- (5)コンテンツ鍵と認証情報から秘匿鍵を作成する。
- (6)秘匿鍵とID種別情報から許諾情報を作成する。
- (7)見本画像に許諾情報を不可視型透かし(周波数変換型)として埋込む。
- (8)透かし入り見本画像と暗号化原画像を一体化し、配布デジタルコンテンツ(JPEG形式)を生成する。

### 3.2 デジタルコンテンツ利用部の機能

配布デジタルコンテンツの表示、原画に埋め込まれた著作権者情報などのコンテンツID[1]表示を目的とする。下記の処理手順で実行される(図7参照)。

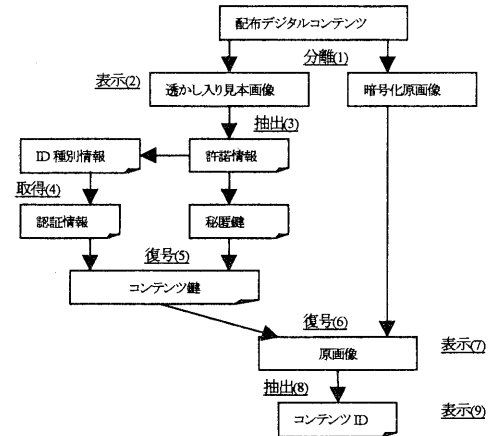


図 7. コンテンツ利用部処理手順

- (1)配布デジタルコンテンツから見本画像部と暗号化原画像部を分離する。
- (2)見本画像部を表示する。  
原画像の著作権者情報表示処理手順を以下に記す。
- (3)見本画像部から不可視型電子透かし(周波数変換型)として埋込んである許諾情報(秘匿鍵やID種別情報など)を抽出する。
- (4)ID種別情報に対応する認証情報(ハードID,ソフトID)を取得する。
- (5)秘匿鍵と認証情報でデジタルコンテンツの復号鍵(コンテンツ鍵)を生成する。
- (6)コンテンツ鍵により暗号化デジタルコンテンツを復号(DES)する。
- (7)デジタルコンテンツを表示する。
- (8)デジタルコンテンツから不可視型電子透かし(周波数変換型)として埋め込んでいる著作権者情報などを抽出する。
- (9)著作権者情報などのコンテンツID[1]を表示する。

#### 4. 考察

開発したプロトタイプの実用性の確認を目的として、下記環境で測定を実施した。尚、システムのストレージ装置としてセキュリティ機能付き GIGAMO 装置を使用し、認証情報は GIGAMO 媒体の Media ID とする。

表2 流通デジタルコンテンツ作成機能処理環境

流通デジタルコンテンツ作成機能 (Application)	FMV DESK POWER SIV237
	CPU: Pentium II 233MHz
	OS: Windows NT 4.0
	原画像画素 : 1K×1K×24bit
処理時間	見本画像画素: 256×256×24bit
	ファイルサイズ: 約 200Kbyte
処理時間	約 10 秒

表3 デジタルコンテンツ利用機能処理環境

デジタルコンテンツ利用機能 (Application)	FMV DESK POWER T20
	CPU: Pentium 200MHz
	OS: Windows NT 4.0
	原画像画素 : 1K×1K×24bit
処理時間	見本画像画素: 256×256×24bit
	ファイルサイズ: 約 200Kbyte
処理時間	約 3 秒

本著作権保護方式の処理対象をハイビジョン画素相当(1K×1K フルカラー)の画像とした。配布デジタルコンテンツ作成時間は1作品あたり約10秒(表2参照)であった。例として100枚分の作品を一括処理する場合、システム処理時間は約17分となる。処理の自動化機能を備えることにより実用化可能と考える。

配布デジタルコンテンツ(1作品)を分解し原画像部に埋め込まれている著作権情報などを抽出・表示処理する時間は、約3秒(表3参照)であった。尚、6枚の配布デジタルコンテンツの一覧表示時間は約1秒であった。

#### 5.まとめ

本稿では、静止画の著作権保護方式について述べた。まず、高精細画像の検索・閲覧処理において見本

画像を処理対象とする画像フォーマットを利用することにより既存の利用者環境で処理機能を高速化することができる。又、個々の情報を一元化管理することによりコンテンツ利用上のトラブルを予防できる。さらに利用範囲の制限を目的とする認証情報(アクセス許可条件)を複数提供することで、作品価値や利用用途毎にデジタルコンテンツを利用制限でき、管理者を含む全てのシステム利用者の意向にそったサービスを実現できる。

本システムのプロトタイプによって処理時間の測定を実施した結果、配布デジタルコンテンツ作成機能とデジタルコンテンツ利用機能の両方において、実用範囲内であることを確認できた。

今後は、パソコン画面に表示された画像データの不正コピー防止機能や万が一不正コピーされた場合のアクセス回数制限機能などについて、検討を進める予定である。

#### —参考文献—

- [1]安田,青木,長田,コンテンツIDと電子透かしへの要求条件,1999年電子情報通信学会基礎・境界ソサイティ大会
- [2]井上彰,“マルチメディア時代の暗号システム 電子透かし”丸山学芸図書,1997.
- [3]Marc A Kaplan, IBM cryptolopes, Super Distribution and Digital Rights management,  
<http://www.research.ibm.com/people/k/kaplan/cryptolope-docs/crypap.html>
- [4]宇田,砂田,井上,重野,松下,安全なデジタル音楽コンテンツ統合システム,コンピュータセキュリティシンポジウム'98