マルチメディア通信と分散処理 80－9
グループウェア 21－9
（1997. 1. 30）

ディジタル画像情報保護のためのスクランブル方式

藤井 寛[†] 串間和彦[†]

ディジタル画像流通においては品質を保持したコピーおよびネットワークによる転送の容易さに起因する，違法コピー氾濫の防止が重要な課題である．我々は暗号を用いてJPEG画像データを変換し，品質を劣化させたスクランブル画像を生成する方式を開発した．本方式は高速な変換に基づくリアルタイム・スクランブル解除によって違法コピーを防止できる．また，本方式はブロック内パラメータ，密度，領域の三つのパラメータでスクランブル程度を制御する．さらに，画像データは複数の鍵によって多重にスクランブルすることも可能である．多重スクランブルは鍵の個数による画像品質制御および複数の著作権の存在する画像の保護に利用できる．

Digital Image Scrambling Method for Copyright Protection

HIROSHI FUJII[†] and KAZUHIKO KUSHIMA[†]

During the distribution of digital images, protection against piracy is important because it is easy to duplicate digital data without deterioration and to spread pirated versions through networks. This paper presents a method for scrambling image data encoded in JPEG. Our method uses a cipher algorithm for data transformation. Its high-speed transformation enables real time descrambling, thereby preventing illegal copying. Using our method, scrambling can be controlled by the intra-block parameters, density and area. The method also allows a single image to be scrambled a number of times using different scrambling keys. Multiple scrambling can be used to determine the image quality based on the level of payment. It can also be used to protect image data composed of several parts, the copyright for each part being owned by different authors.

1. はじめに

高性能CPUおよびJPEG[1]，MPEG[2),3)]等の高能率画像圧縮符号化方式の出現によって計算機上での静止画や動画の処理が容易になり，これに伴ってCD-ROMやネットワークを用いたディジタル画像流通が盛んになりつつある．ディジタルデータは品質を保持したコピーおよびネットワークによる転送が簡単で違法コピーが容易に氾濫しうるため，流通においては著作権保護，特に違法コピー防止が非常に重要である[4)]．

一方，画像情報取引の円滑化のためには情報提供者は商品を宣伝し，利用者は事前に画像を評価できることが望ましい[6)]．それには保護された画像情報の内容が確認できる必要がある．我々は暗号を用いて概要が認識できる程度に品質を劣化させたスクランブル画像を用いて流通における画像データを保護する方式を開発した．

画像スクランブルによる著作権管理では違法コピー防止のためにユーザによる元画像データのコピーを禁止する機能が必要である．これにはスクランブル解除が画像再生時にリアルタイムで行われ，スクランブル解除後のデータがユーザ端末に格納されないようにすべきである．リアルタイムのスクランブル解除には変換の高速性が要求され，特に動画における高速変換は必須である．また画像流通においては様々な特性の画像が提供されるため，その特性や意図する宣伝効果に応じたスクランブル程度の設定と制御が可能でなければならない．

我々の開発したディジタル画像スクランブル方式はJPEGデータに対する高速な変換と，パラメータによるスクランブル程度の制御機能によって上の条件を満足する．画像変換には暗号を用いており，元画像の復元には復号鍵を用いる．本方式ではさらに単一画像の複数鍵による多重スクランブルが可能で，利用者の支払いに応じたスクランブル解除の度合の制御および編集画像の著作権管理も可能にする．

2. 画像符号化方式

JPEGのベースラインプロセスでは画像データは2次元離散コサイン変換（DCT），量子化，可変長符号（VLC）化を経て圧縮符号化される（図1）．

画像はまず8×8画素のブロックに分割され，各ブ

† NTT 情報通信研究所
NTT information and communication systems laboratories

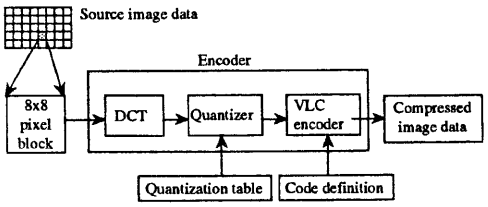

図1 画像エンコーダのダイアグラム

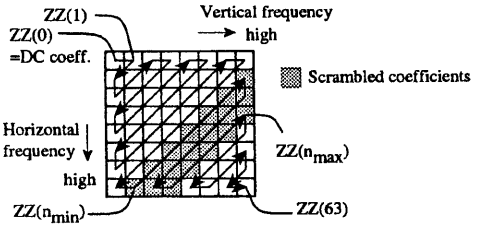

図2 DCT係数行列のジグザグスキャン

ロックは2次元DCTによってDCT係数の8×8行列に変換される．行列中の各係数は量子化表に基づいて量子化され，図2のようにジグザグスキャンによって一次元化された64個の量子化DCT係数が系列における先頭からの位置によって$ZZ(0)$から$ZZ(63)$まで順に番号付けされる．

次にDCT係数系列中の非零係数と，それに先行する零係数の系列長の組が可変長符号化される．非零のDCT係数は絶対値によって2^nの幅（$n=0,1,2,\cdots$）でカテゴリ化され，各カテゴリは番号S（$S=0,1,2,\cdots$）で参照される．ここでカテゴリ番号と零係数系列長の組がハフマン符号化され，さらに非零の係数値がハフマン符号語の直後に付加されたS桁のビットで表される．S桁の付加ビットは係数値を2進数で表現する．例えば$ZZ(1)\sim ZZ(4)$が4,0,0,3のとき，$2^1 < ZZ(4) \leq 2^2$であるから$ZZ(4)$に対して$S=2$．Sと$ZZ(4)$の直前の零係数系列長の組(2/2)を表わすハフマン符号語を'11111001'とすると，系列$ZZ(2),ZZ(3),ZZ(4)$は'1111100111'で表わされる．最下位2ビット'11'は付加ビットで，$ZZ(4)$の値3を表わす．

3. スクランブルパラメータ

3.1 付加ビット変換

本方式は付加ビット値の変換によって画像スクランブルを行う．S桁の付加ビットはカテゴリSに属するDCT係数値に2進数として一対一対応しており，付加ビット長を保存する任意の変換でJPEGデータ形式は保存され，非零のDCT係数値のみがカテゴリ内で変化する．例えば2章の$ZZ(2),ZZ(3),ZZ(4)$を符号化した'1111100111'の最下位2ビットは任意の値に変換可能である．変換後の符号語'1111100100'，'1111100101'，'1111100110'によって$ZZ(4)$の値はそれぞれ同一カテゴリ内の-3，-2，2となり，変化後の値が符号化する画像は元画像からわずかに変形したものとなる．

画像スクランブルの程度は変換する付加ビットの数と位置で制御できる．スクランブル程度の制御のために本方式ではスクランブルパラメータとしてブロック内パラメータ，密度，領域を用いる．

3.2 ブロック内パラメータ

画像上のブロックはDCT係数の系列で表現されており，スクランブル程度は変換対象となる周波数および変換によるDCT係数値の変位によって決定される．ブロック内パラメータはこれを制御する．

DCT係数のうちAC係数に対して，$ZZ(n)$のインデクスnに対するパラメータn_{min}，n_{max}によって値を変換する係数を指定する．AC係数$ZZ(n)$の値は図2のように$n_{min} \leq n \leq n_{max}$のとき変換する．$n$が大きいほど$ZZ(n)$の符号化する周波数は高くなるため，$n_{min}$が小さいほどブロック内の大きな構造がスクランブルされ，n_{max}が大きいほどブロック内の細かな構造がスクランブルされる[9]．

付加ビットは係数値の2進数表現であるから，付加ビット変換による係数値の変化量は変換対象の桁で制御できる．付加ビットの下位第mビットを変換すると係数値の最大変化量は2^m-1である．本方式では上記mをDC係数に対してm_{DC}，AC係数に対してm_{AC}として制御パラメータとする．

以上の述べたように，ブロック内パラメータは4字組

$$b=(m_{DC},m_{AC},n_{min},n_{max}) \qquad (1)$$

である．

図6(1)，(2B)，(3B)にJPEG画像に対するブロック内パラメータ(10,10,1,63)，(0,10,1,63)，(0,10,1,2)によるスクランブル効果を示す．

3.3 領　域

画像は8×8画素のブロックに分割されて各々符号化されるから，ブロック内パラメータはブロック毎に独立に指定できる．領域パラメータは，その内部に存在するブロックがスクランブル対象となる領域を指定する．これによって図6(1)，(2A)，(3A)のように，画像中の特定部分のみのスクランブルが可能となる．

3.4 密　度

AC係数の変換はブロック内のパタンをスクランブルするため，ブロック面積が非常に小さい高解像度画像にはスクランブル効果が現れにくい．逆にDC係数はブロックの全画素の平均値であり，解像度に関わらずスクランブル効果が得られるが，スクランブル程度の制御が柔軟性に欠ける．

そこでDC係数のスクランブル効果の制御のために密

度パラメータを導入する．これは式(2)のようにブロックのスクランブルのon/offを表わす二値の$n \times m$行列で，$n \times m$個のブロックからなる局所領域に対応し，画像上の水平第Nブロック，垂直第Mブロックのブロックは行列の$(N \bmod n+1, M \bmod m+1)$要素に従ってスクランブルされる．式(2)は$2 \times 2$ブロックからなる局所領域のスクランブルパタンを指定しており，画像を市松模様にスクランブルする．

$$d = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \qquad (2)$$

3.5 パラメータによるスクランブル程度制御

スクランブルパラメータによって画像の性質，意図する宣伝効果等に応じたスクランブル程度の制御が可能になる．$T_p(I)$を画像Iのスクランブルパラメータpによる変換対象となる付加ビットの集合とすると，

$$T_{p_1}(I) \subset T_{p_2}(I) \qquad (3)$$

のときp_2によるスクランブルはp_1によるものより強い．

異なる画像I_1, I_2に対しては，付加ビットの数や位置，画像の解像度，量子化係数等が異なるため，同一パラメータであってもスクランブル効果は同一とはならない．望ましいスクランブルを行うパラメータの決定は，実際に画像に適用して効果を確認する，もしくは画像の付加ビットの分布や符号化パラメータの値に基づいて決定する必要がある．我々の試作したシステムでは設定したパラメータによるスクランブル効果のプレビュー機能をもたせてパラメータ決定を可能にしている．

4. スクランブル・データ変換法

本方式は圧縮符号化データから画素値を計算せずに符号内のビット変換のみで画像スクランブルを行うため変換が高速である．付加ビット変換には乱数ビット系列rとの排他的論理和を用いる．変換対象付加ビットの連接を$a = a_1\ a_2\ r_3\ \cdots$，乱数ビット系列を$r = r_1\ r_2\ r_3\ \cdots$とするとき，$a_k$は$r$の第$k$ビット$r_k$との排他的論理和によって

$$a'_k = a_k \oplus r_k \qquad (4)$$

に変換される．スクランブル解除は逆変換

$$a_k = a'_k \oplus r_k \qquad (5)$$

によって行う．

図3に本方式の画像スクランブルモジュールの構成図を示す．VLCデコーダDには画像データが1ビットづつ入力される．Dは付加ビットを検出して桁，$ZZ(n)$のインデクスおよび画像上のブロック位置をフォーマット情報としてビット選択器Sへ出力し，同時に画像データをEへ1ビットづつ出力する．SはDからのフォーマット情報とスクランブルパラメータを比較し，Dに入力しているビットが変換対象であるとき乱数系列発生器Rにシグナルを送る．RはSからシグナルがあるとき1ビットをランダムな値で出力し，それ以外のとき'0'を出力する．Dの出力する画像データはEにおいてRの出力との排他的論理和に変換され，スクランブル変換された圧縮符号化画像データとして出力される．画像スクランブルとその解除は同一演算であるから，同一モジュールによってスクランブルおよびスクランブル解除が行える．

Rにおける乱数系列発生に，本方式は暗号アルゴリズムFEAL[5]のOFBモードを用いている．乱数はスクランブルパラメータによって指定されるFEALの鍵kよって制御される．

スクランブルモジュールは単独でJPEGデータからスクランブルJPEGデータへの変換および逆変換を行う．加えて**図4**のようにJPEGデコーダ内のVLCデコーダと置換することで画像デコーダへ組み込むことも可能である．点線の部分が組み込みによる追加コンポーネントである．このデコーダは画像スクランブルを解除しながら復号し，画像を直接表示する．

JPEGデコーダ内のVLCデコーダDは可変長符号語と付加ビットを分離する．次にQ^{-1}で両者の値に基づいてDCT係数行列が生成される．次に逆方向DCT（DCT^{-1}）で画素が復元され，モニタに画像が表示される．ここでVLCデコーダの出力する付加ビットがEでスクランブルモジュールによって変換されてスクランブル解除される．同様にエンコーダにスクランブルモジュールを組み込むこともできる．

スクランブルモジュールを単独でスクランブル解除装置として用いる場合，スクランブル解除された画像データはファイルとして保存される．この場合，課金形態はpay per copyとなる．pay per copyでは購入した画像を何度でも使用でき，コピーも可能である．この形態は実現が容易で従来のソフトウェア販売や画像データ販売と同様の形態であるが違法コピーの行われる可能性も高い．

これに対してpay per viewは画像の利用毎に課金する形態で，元画像データを利用者が保存するのを許さない．この形態は違法コピーの危険性が低いが，画像データのコピー防止技術が必要となる．図4の装置はスクランブル解除と表示を同時に行い，元画像データをデコーダ外部に生成しないためpay per viewを実現できる．

pay per viewでは特に動画の再生において時間の制約が厳しく，高速な変換が要求される．図4の装置ではS, Rにおける乱数発生とDにおける可変長符号の復号は並列処理可能であるから，乱数発生を高速化することでスクランブル解除による処理時間の増加をEにおける排他的論理和演算のみに抑えることができる．よってmotion JPEGデコーダにスクランブルモジュールを組み込めばリアルタイムのスクランブル解除による動画のpay per viewも可能である．

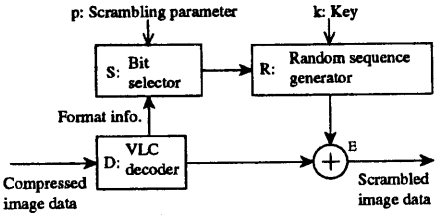

図3 スクランブルモジュール

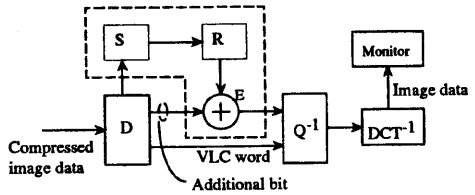

図4 リアルタイムデコーダ

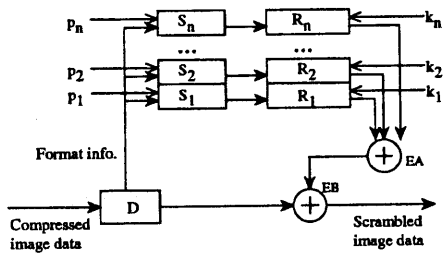

図5 多重スクランブルモジュール

5. 多重スクランブル

5.1 変換モジュール

本方式は画像データフォーマットを変化させないから，スクランブル画像をさらに繰り返しスクランブル可能で，これを利用して一つの画像に複数の鍵が設定できる．図5がn個のパラメータ$p_1, p_2, \cdots, p_n$による多重スクランブルを行うモジュールの構成である．S_i，R_iがパラメータp_iに基づいて乱数系列を発生し，EAでは$R_1, R_2, \cdots, R_n$の出力の排他的論理和として合成乱数ビットが生成される．EBでは合成乱数ビットと画像データの排他的論理和によって多重スクランブル画像データが生成される．

排他的論理和の性質から，多重スクランブルはパラメータの組み合わせにのみ依存し，適用順序や同時に適用するパラメータの組み合わせに依存しない．スクランブル解除はスクランブルで用いたパラメータによる再度の変換で行うが，解除時のパラメータの適用順序はスクランブル時の順序から独立である．

5.2 情報流通支援への利用

多重スクランブルは鍵による画像品質制御に用いる．第一の応用は支払いに応じた品質制御である．パラメータ集合$P_n = \{p_1, p_2, \cdots, p_n\}$に基づいてスクランブルされた画像$I_s = S(P_n, I_o)$を仮定する．利用者は支払い額に応じて$i$個のパラメータ$P_i' = \{p_n, p_{n-1}, \cdots, p_{n-i+1}\}$の鍵$k_n, k_{n-1}, \cdots, k_{n-i+1} (i \leq n)$を入手し，部分的にスクランブル解除された画像

$$S(P_n - P_i', I_o) = S(P_{n-i}, I_o) \qquad (6)$$

を得る．$S(P_{n-i}, I_o)$はiが大きくなるほど，つまり利用者の支払いが増加するほど元画像に近くなる．

例えばすべてのiについてP_iがP_{i-1}より広い領域をスクランブルするとき，支払いの増加によってスクランブル面積が減少する．同様に密度およびブロック内のスクランブル強度の支払いに応じた制御も可能である（図6）．多重スクランブルの性質から，部分的にスクランブル解除した画像に鍵を追加して画質を順次向上させることもできる．

多重スクランブルの第二の応用は著作権管理である．別々の著者$A_1, A_2, \cdots, A_n$の提供する複数の素材$I_1, I_2, \cdots, I_n$が編集された画像Iにおいて，I_iに由来する部分にはA_iの著作権が存在する．よってIの各部分の利用は対応する著者によって個別に管理されるべきである．本方式はI中のI_i部分を著作権保護のためにA_iがスクランブルすることを可能にする．各ブロックのスクランブル解除には設定されたすべての鍵が必要である．著者は自分の提供した画像素材を鍵によって保護し，I_iの使用に対する課金を直接管理できる．図7は3つの素材からなる図鑑のページである．編集者A_1の鍵はテキスト部分のみスクランブル解除する．各写真のスクランブル解除には対応する鍵を著者A_2，A_3から購入しなければならない．

6. 試作システム

我々は本稿で述べた方式に基づいてスクランブル画像作成支援系およびスクランブル画像ビューアを試作した．

スクランブル画像作成支援系はAdobe Photoshopのプラグインとして実現している．画像スクランブルには，まずGUIを用いてスクランブル領域を指定し，次に指定領域に対してパラメータ指定ダイアログから密度，ブロック内パラメータを設定する．作成支援系は出力としてパラメータに基づいたスクランブル画像および対応するスクランブル解除鍵を生成する．多重スクランブルは上記操作の繰り返しによる．スクランブル画像に

は画像IDが，鍵には画像IDおよび鍵IDが付与されており，生成された画像および鍵は次に述べるスクランブル画像ビューアでの表示に用いられる．

スクランブル画像ビューアはNetscape Navigatorのプラグインとして実現され，HTML文書内のスクランブルJPEG画像を表示する（図8）．スクランブル解除鍵はユーザ端末上の鍵フォルダに格納されており，ビューアはスクランブルJPEG画像のIDと鍵IDを検査し，鍵フォルダ内に対応するIDの鍵が存在しないとき，スクランブルJPEG画像はそのままWWWブラウザ画面に表示される．鍵フォルダ内に対応する鍵が存在するとき，スクランブル解除されたオリジナル画像がブラウザ上に表示される．このときスクランブル解除されたオリジナルJPEGデータは生成されず，直接画像が表示されるためユーザによるコピーは行えない．またスクランブル画像ビューアは多重鍵をサポートしており，設定された鍵の一部分のみが鍵フォルダ内に存在するとき，存在する鍵についてのみスクランブル解除された画像が表示される．

7. おわりに

本稿ではディジタル画像流通支援のためのスクランブル方式について述べた．画像流通において著作権保護は最も重要であるが，本方式はスクランブル変換が高速で，簡単な構成のモジュールを画像デコーダに追加することでリアルタイムのスクランブル解除が可能になり，元画像のユーザ端末上への格納を防止して違法コピーに対処できる．またスクランブル程度の制御が可能で，流通における見本として最適なスクランブル画像が生成可能である．さらに多重スクランブルによって支払に応じた画像品質制御や編集された画像の著作権管理も可能となる．また，本方式は単純な変更でMPEGにも適用可能となる．

Pay per copyの形態ではスクランブル解除後のデータのコピーが可能であり，またpay per viewであってもVRAM等からスクランブル解除画像がコピーされる危険があるため，その保護が必要である．我々はこのためにスクランブル解除時に利用者IDを電子透かし[7),8)]として画像に埋め込むことで違法コピーを抑止する方式を研究中である[10)]．

参考文献

1) Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines, ISO/IEC 10918-1 (1994).
2) Information technology – Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s, ISO/IEC 11172 (1993).
3) Information technology – Generic of moving pictures and associated audio information, ISO/IEC DIS 13818 (1994).
4) Spector, P.L.: The internet goes international: intellectual property considerations for industry, Proc. PTC '96, pp. 560–566, Honolulu (1996).
5) Miyaguchi, S.: The FEAL cipher family, Advances in Cryptology - Crypto '90, LNCS537, pp. 627-638, Springer-Verlag (1991).
6) Inuma, K.: Two-way interactive advertising in the information society, Proc. PTC '96, pp. 837–844, Honolulu (1996).
7) Cox, I. J., Kilian, J., Leighton, T. and Shamon, T.: Secure spread spertrum watermarking for multimedia, NEC Research Institute, Technical Report 95-10 (1995).
8) Bender, W., Gruhl, D. and Morimoto, N.: Techniques for data hiding, Proc. of SPIE, vol. 2420, pp. 40– (1995).
9) 阿部剛仁，藤井寛，山中康史，谷口展郎:JPEG半開示映像作成における開示度パラメータ，第52回情処全大，2-209 (1996).
10) 阿部剛仁，藤井寛，串間和彦:個別情報埋め込みによる画像データの保護方式，第80回マルチメディア通信と分散処理研究会 / 第21回グループウェア研究会 (1996).

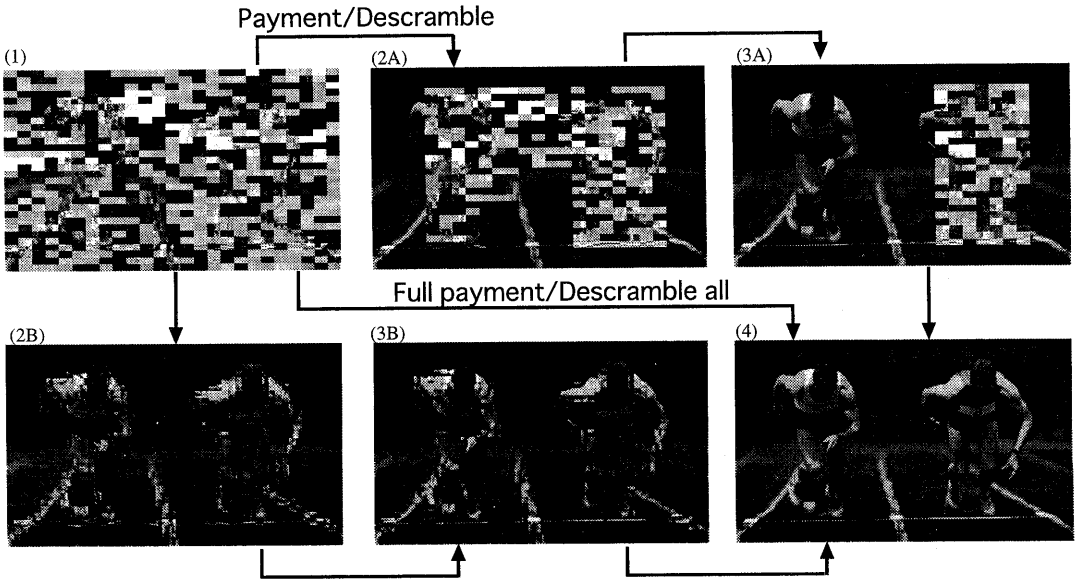

図6 支払による品質制御

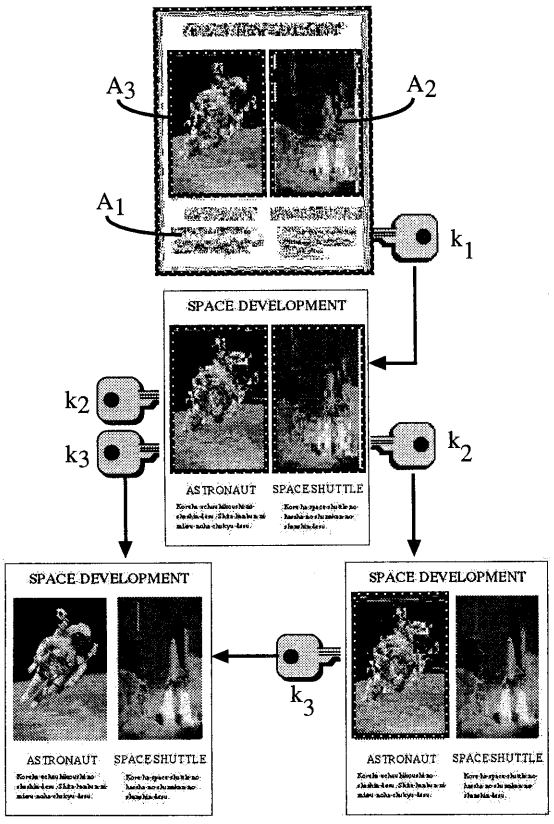

図7 多重スクランブルによる著作権管理

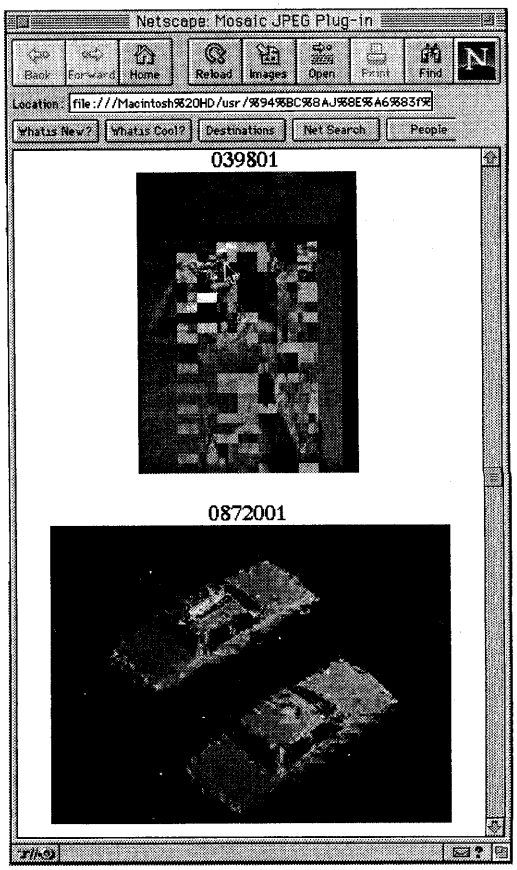

図8 スクランブル画像ビューア