ディジタル画像情報流通支援のためのスクランブル方式

藤井 寛† 山中康史†

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．違法コピーの危険性から提供者には見本画像の公開に抵抗があり，そのため利用者は事前の内容確認が困難である．我々は画像情報流通を阻害する本問題を解決する，JPEGおよびMPEG1画像データのスクランブル方式を開発した．本方式は暗号を用いて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．スクランブル解除は暗号鍵によって制御され，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．効果的宣伝と違法コピー防止のためにはスクランブルの程度が制御可能であることが望ましい．本方式はブロック内パラメータ，密度，領域の3つのパラメータでこれを制御する．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 Information Distribution

HIROSHI FUJII† and YASUSHI YAMANAKA†

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. Providers of image data cannot disclose the original data for fear of piracy, yet still need to advertise their products and to allow customers to evaluate a product prior to paying for it. This paper presents a method for scrambling image data encoded in JPEG or MPEG1 in order to solve this problem. Our method uses a cipher algorithm for data transformation to generate a deteriorated version of the image data. Its high-speed transformation enables real time descrambling, thereby preventing illegal copying. For effective advertisements and copyright protection, the degree to which image data is scrambled should be controllable. 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，これにともなってCD-ROMやネットワークを用いたディジタル画像流通がさかんになりつつある．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)]．

通常，情報の不正利用防止と保護には暗号が用いられている[5),6)]．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[7)]．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が，完全に隠蔽された暗号化データでは不適当である．

ディジタル画像の著作権保護方式の1つに電子透かし（Watermark）[8)~10)]がある．これは表示品質に影響を与えずに画像に著者情報等を埋め込むもので，埋込み情報によって画像の著作権主張と流通の監視を可能にする．従来，画像の編集による埋込み情報の消去という欠点があったが，変形等にある程度の耐性を持つ方式も考案され，アナログコピーの検出も可能になりつつある[11)]．しかし電子透かしは画像の利用は自由で不正利用や違法コピー自体を直接防止はできないという問題が残る．また埋込み情報の消去も完全には防

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

げない．

これに対して我々は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．スクランブル画像[12)~14)]は宣伝や内容確認には利用可能であるが，低品質であるため違法コピーの問題は少ない．

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．理想的にはスクランブル解除はハードウェア的に保護された領域で行うことが望ましい[15)]．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，宣伝の観点から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 およびMPEG1 データをデータ形式を保存したまま元画像とスクランブル画像の間で直接変換し，変換の計算量は非常に小さい．スクランブル程度はパラメータによって制御可能である．また画像変換には暗号を用いており，流通時に通常の暗号化情報と同様に扱え，鍵を用いて元画像が復元できる．流通管理は鍵によって行い，利用者はまずスクランブル画像を入手して評価し，次にスクランブル解除鍵を購入して元画像を復元する．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ができる．多重スクランブルは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．DCT 係数はブロック内の水平および垂直方向の各空間周波数成分の強度を表し，DCT 係数行列中に左から右へ水平方向周波数の低いものから順に，また上から下へ垂直方向周波数の低いものから順に並んでいる．行列の (1,1) 要素はDC 係数と呼ばれ，それ以外はAC 係数と呼ばれる．行列中の64個のDCT 係数は量子化後**図2** のようにジグザグスキャンによって一次元系列化され，さらに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．

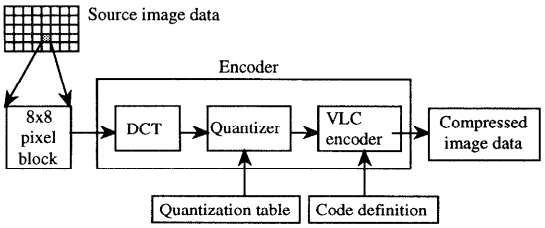


図1 画像エンコーダのダイアグラム
Fig. 1 Encoder diagram.

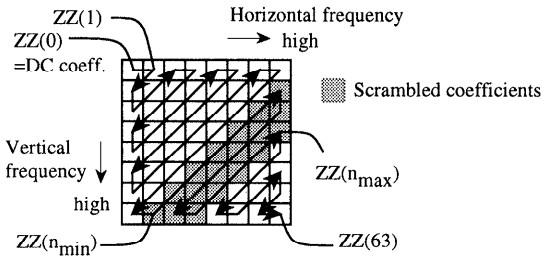


図2 DCT 係数行列のジグザグスキャン
Fig. 2 Zig-zag scanning of the DCT coefficient matrix.

次にDCT 係数系列中の非零係数と，先行する零係数の系列長 R の組が可変長符号化される．まず非零係数が絶対値によって 2^S の幅（$S=0,1,2,\cdots$）でカテゴリ化され，番号 S で参照される．次に S と R の組が可変長符号化され，さらに非零係数値を特定するために後ろに S 桁のビットが付加される．付加ビットは係数値を2進数で表現する．たとえば $ZZ(1)$～$ZZ(4)$ が4，0，0，3のとき，$ZZ(4)$ に対して，$2^1 < 3 \leq 2^2$ から $S=2$．$R/S=2/2$ が‘11111001’で符号化されるとすると，系列 $ZZ(2)$，$ZZ(3)$，$ZZ(4)$ は‘1111100111’で表される．最下位2ビット‘11’は付加ビットで，$ZZ(4)$ の値3を表す．最終的にはすべてのDCT 係数が可変長符号と付加ビットの組の系列で表現される．

MPEG1 も動画中の各静止画にブロック分割，DCT，量子化，可変長符号化を行う．ただしブロックのうちintra block はJPEG と同様に画素値自体を符号化するが，non-intra block には時間軸方向の予測符号化が用いられる．DC 係数はJPEG と同様のカテゴリ化によって S 桁の付加ビットとともに符号化される．一方，AC 係数は通常絶対値に基づきカテゴリ化され，正負を一桁の付加ビットで表す．たとえば $ZZ(1)$～$ZZ(4)$ が4，0，0，3のとき，$ZZ(4)$ の絶対値3と零

系列長2の組を表す符号語を '0000001011' とすると，系列 $ZZ(2)$，$ZZ(3)$，$ZZ(4)$ は '00000010110' で表される．最下位ビット '0' は符号ビットである．

3. スクランブル方式

3.1 変換対象付加ビット

本論文の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．JPEG では S 桁の付加ビットがカテゴリ 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．よって任意の付加ビットが JPEG データ形式を保存したまま値を変換できる．たとえば2章の $ZZ(2)$，$ZZ(3)$，$ZZ(4)$ を符号化した '1111100111' の最下位2ビットは付加ビットであるから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．

MPEG1 では DC 係数は JPEG と同様の付加ビット変換によってスクランブルする．AC 係数は可変長符号の直後に存在する，符号ビットである一桁の付加ビットが変換対象になり，付加ビット値の変換によって非零の DCT 係数の符号が反転する．

3.2 スクランブルパラメータ

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を4字組

$$p = (b, d, a, k) \tag{1}$$

として定義する．ここで b はブロック内パラメータ，d は密度，a は領域，k は鍵で，それぞれ独立に値を設定可能である（図3）．

3.2.1 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．この制御ためにブロック内パラメータを導入する．

DCT 係数のうち DC 係数はブロックの画素値の平均を決定し，AC 係数はブロック内のパターンを決定する．ここで AC 係数に対して，値を変換する係数を指定するために $ZZ(n)$ のインデクス n に対するパラメータ $n_{\min}$，$n_{\max}$ を導入する．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相対的に高くなるため，$n_{\min}$ が小さいほど画像の低周波成分つまりブロック内の大きな構造がスクランブルされ，$n_{\max}$ が大きいほど高周波成分つまりブロック内の細かな構造がスクランブルされる[16]．

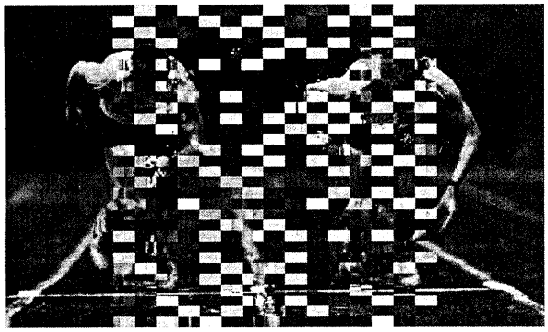


図3 JPEG スクランブル画像（ブロック内パラメータ：(1,10,1,63)，領域：中央部分，密度：2 × 2 単位行列）
Fig. 3 Scrambled JPEG image (Intra-block parameter: (1,10,1,63). Area: Center. Density: 2 × 2 unit matrix.).

JPEG の DCT 係数および MPEG1 の DC 係数の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 ビットの重みは最上位の $3 \cdot 2^{m-1} - 1$ を除いて 2^{m-1} であり，下位第 m ビット以下の i 桁の付加ビットを変換すると係数値の最大変化量は $2^m - 2^{m-i}$ である．ここで m が1増加すると最大変化量は約2倍になる．i が大きいほど変換される付加ビットが少なく，変換が高速になるが攻撃に対して弱くなる．本方式ではこの 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し，DC 係数および AC 係数の付加ビットの下位それぞれ第 m_{DC} 桁，m_{AC} 桁以下 i ビットがスクランブル変換対象となる．$m_{DC} = 0$，$m_{AC} = 0$ のとき DC 係数，AC 係数の変換がそれぞれ停止される．

以上の述べたように，ブロック内パラメータは4字組

$$b = (m_{DC}, m_{AC}, n_{\min}, n_{\max}) \tag{2}$$

で，ブロックのスクランブル程度を制御する．MPEG1 では通常 AC 係数に対する付加ビットは符号ビットのみであるから m_{AC} は二値となる．

図 4(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．

3.2.2 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ごと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

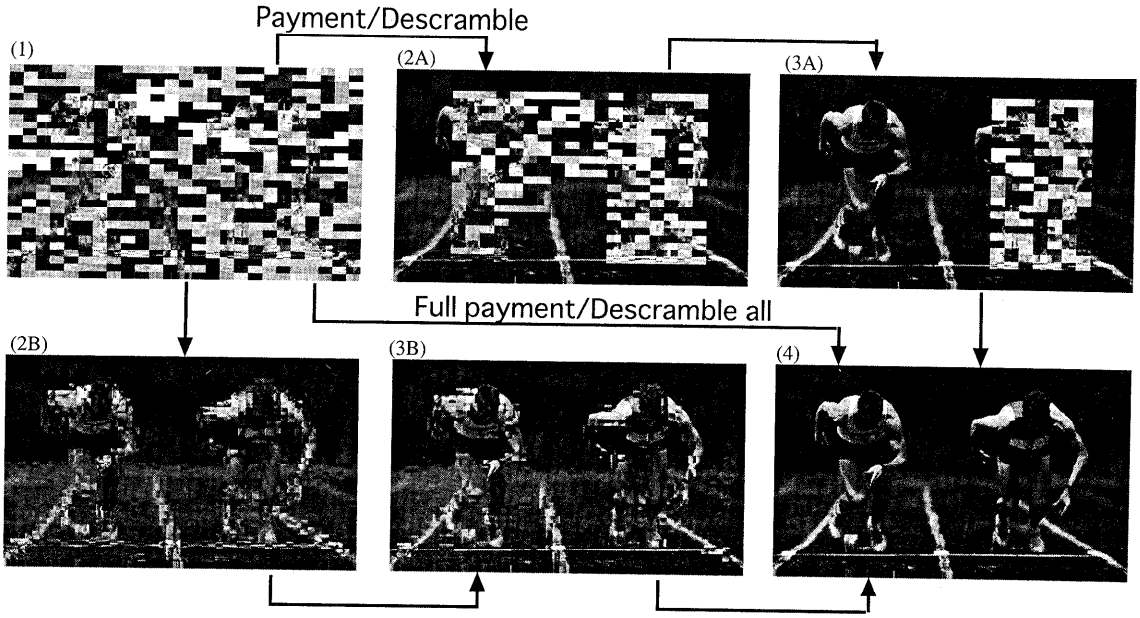


図4 支払による品質制御（ブロック内パラメータ：画像(1)，(2A)，(3A)に対して(10,10,1,63)，(2B)に対して(0,10,1,63)，(3B)に対して(0,10,1,2)）
Fig. 4 Quality control based on payment (Intra-block parameters are (10,10,1,63) for images (1), (2A), (3A); (0,10,1,63) for (2B); and (0,10,1,2) for (3B)).

定する．これによって図4(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．

本方式では $M \times N$ 画素の画像に対して，$M/8s_1 \times N/8s_2$ ビットのビットマップデータによってスクランブル領域を指定する．s_1，s_2 はスケーリング係数である．

DC係数は通常，予測符号化によって直前ブロックの係数値との差が符号化されるため，先行するDC係数値が後続するブロックのDC係数値に影響を与える．本方式では領域指定におけるDC係数スクランブルの他のブロックへの波及を防止するために，DC係数スクランブルを行う場合は予測符号化を用いないでJPEG符号化する．

3.2.3 密　　度

AC係数の変換はブロック内のパター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や，非零のAC係数が少なくその絶対値が小さい平坦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，解像度にかかわらず，また平坦画像に対しても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．密度パラメータは局所領域中のブロックに対するブロック内パラメータの設定パターンを定義する．具体的には式(3)のようにブロックのスクランブルのon/offを表す二値の $n \times m$ 行列である．これは $n \times m$ 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．

局所領域中のスクランブルするブロックの割合によって大域的なスクランブル強度が制御される．たとえば式(3)は 2×2 ブロックからなる局所領域のスクランブルパターンを指定しており，画像を図3のように市松模様にスクランブルし，全ブロックのスクランブルに比べて大域的な強度が約1/2になる．

$$d = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{3}$$

3.3 パラメータによるスクランブル程度制御

画像 I の，ブロック内パラメータ b による変換対象ビットの集合を $T_b(I)$，密度パラメータ d による変換対象ブロックの全付加ビットの集合を $T_d(I)$，領域 a 内のブロックの全付加ビットの集合を $T_a(I)$ とするとき，スクランブルパラメータ $p=(b,d,a,k)$ による画像 I の変換対象付加ビット集合 $T_p(I)$ は

$$T_p(I) = T_b(I) \cap T_d(I) \cap T_a(I) \tag{4}$$

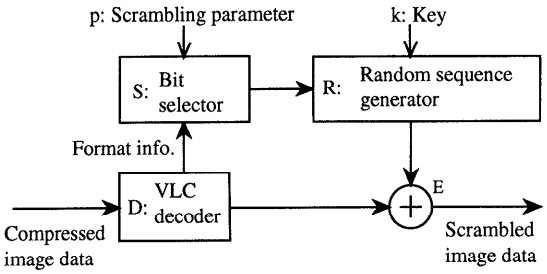


図5 スクランブルモジュール
Fig. 5 Data scrambling module.

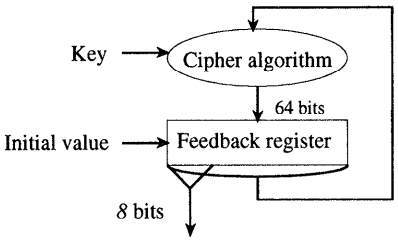


図6 乱数系列発生器
Fig. 6 The random sequence generator.

となる．p の要素 b, d, a すべてに対して変換対象となる付加ビットが実際に p によってスクランブルされる．

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．任意の2つのスクランブルパラメータ $p_1=(b_1,d_1,a_1,k_1)$, $p_2=(b_2,d_2,a_2,k_2)$ について

$$T_{p_1}(I)\subset T_{p_2}(I) \tag{5}$$

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．ここで式(4)から，$T_{b_1}(I)\subseteq T_{b_2}(I)\wedge T_{d_1}(I)\subseteq T_{d_2}(I)\wedge T_{a_1}(I)\subseteq T_{a_2}(I)$ のとき $T_{p_1}(I)\subseteq T_{p_2}(I)$ となり，同一画像に対してパラメータ b, d, a のうち2つを固定し，残り1つを変化させることで独立にスクランブル程度の設定が行える．また特に

$$b_i=(m_{DCi},m_{ACi},n_{\min i},n_{\max i})$$

において，$m_{DC1}\leq m_{DC2}\wedge m_{AC1}\leq m_{AC2}\wedge n_{\min 1}\geq n_{\min 2}\wedge n_{\max 1}\leq n_{\max 2}$ のとき $T_{b_1}(I)\subseteq T_{b_2}(I)$ となる．

3.4 データ変換方式

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．付加ビット変換にはビット長を保存する任意の方法が適用できるが，本方式では乱数ビット系列との排他的論理和を用いる．画像 I の乱数系列 r による変換は次のように行う．変換対象付加ビット集合 $T_p(I)$ 中の I における出現順序が k 番目のビットを a_k，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

$$a'_k=a_k\oplus r_k \tag{6}$$

に変換される．スクランブル解除は逆変換

$$a_k=a'_k\oplus r_k \tag{7}$$

によって行う．

図5 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ビットずつ入力される．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ビットずつ出力する．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方法は任意である．乱数発生速度と構成の容易さ重視する場合，フィードバックシフトレジスタ等の簡単な回路で構成し，安全性のためには暗号アルゴリズムによる乱数発生器を用いる．我々の試作したシステムは暗号アルゴリズム FEAL[6] の OFB モードを用いている．暗号アルゴリズムの出力 64 ビットは入力に帰還され再び 64 ビットのデータを出力する．また出力の上位 8 ビットが乱数ビットとして使用される．以上を繰り返して任意長の乱数系列が発生する（**図6**）．乱数はスクランブルパラメータによって指定される暗号鍵 k よって制御される．

図5のスクランブルモジュールは単独で JPEG または MPEG1 データからスクランブル JPEG，MPEG1 データへの変換および逆変換を行う．加えて JPEG および MPEG1 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．**図7** はスクランブルモジュールを組み込んだ JPEG デコーダの構成図で，点線で囲んだ部分が組込みによる追加コンポーネントである．

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量子化 DCT 係数が計算され，さらに逆量子化されて DCT 係数行列が生成される．次に逆方向

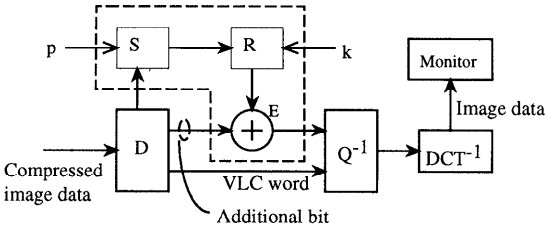


図7 リアルタイムデコーダ
Fig. 7 Realtime descrambler.

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．

3.5 多重スクランブル

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1つの画像に複数の鍵が設定できる．画像 I をパラメータ $p_1, p_2, \cdots, p_n$ の順に繰り返しスクランブルするとする．I における出現順序が k 番目の付加ビットが a_k，また a_k を変換対象とするパラメータが $p_{k_1}, p_{k_2}, \cdots, p_{k_{n_k}}$ $(n_k \leq n, k_{i-1} < k_i)$ であるとき a_k は

$$a_k \oplus r_{k_1,k} \oplus r_{k_2,k} \oplus \cdots \oplus r_{k_{n_k},k} \tag{8}$$

に変換される．ただし $r_{k_i,k}$ は p_{k_i} が発生する乱数ビットのうち a_k を変換するビットを表す．ここですべての整数 k について

$$r_k = r_{k_1,k} \oplus r_{k_2,k} \oplus \cdots \oplus r_{k_{n_k},k} \tag{9}$$

となる合成乱数系列 $r = r_1\ r_2\ r_3\ \cdots$ があれば，r による I の変換は $p_1, p_2, \cdots, p_n$ による繰返しスクランブルと等しくなる．これを多重スクランブルと呼ぶ．

p_k による変換対象付加ビットの集合を $T_{p_k}(I)$ とするとパラメータ集合 $P = \{p_1, p_2, \cdots, p_n\}$ 中の全パラメータによる多重スクランブルにおける変換対象付加ビット集合は

$$\bigcup_{p \in P} T_p(I) = \bigcup_{i=1}^{n} T_{p_i}(I) \tag{10}$$

である．

図8 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．合成乱数系列 r は図中の S_i, R_i, EA からなるコンポーネントによって発生される．ビット選択器 S_i はパラメータ p_i とVLCデコーダ D からのフォーマット情報に基づいて変換対象の付加ビットを検出し，乱数系列発生器 R_i にシグナルを送る．R_i は鍵 k_i に基づいて乱数系列を発生させ，3.4節と同様に1ビットずつ出力する．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 r_k が生成され，EB で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．

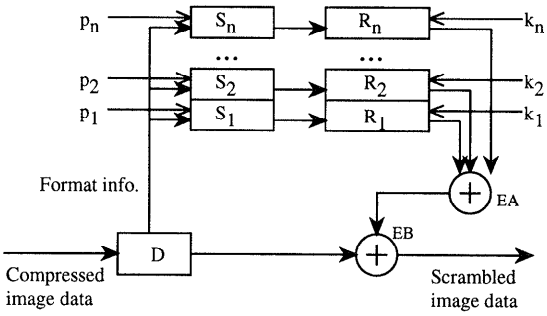


図8 多重スクランブルモジュール
Fig. 8 Multiple-scrambling module.

P をスクランブルパラメータの集合，I を画像データ，$S(P, I)$ を P に属するすべてのパラメータに基づく I の多重スクランブルで得られた画像とする．このとき任意の P_1，P_2 に対して

$$S(P_2, S(P_1, I)) = S((P_1 \cup P_2) - P_1 \cap P_2, I) \tag{11}$$

$$S(\phi, I) = I \tag{12}$$

が成立する．パラメータ集合 P_1 による多重スクランブル画像 I_1 をさらにパラメータ集合 P_2 で多重スクランブルするとき，新たに P_2 で追加されるパラメータによるスクランブルが I_1 に重畳され，P_1，P_2 両方に含まれるパラメータについてはスクランブルが解除される．また，式(11)，(12)から，

$P_1 = P_2$ のとき

$$S(P_2, S(P_1, I)) = S(\phi, I) = I \tag{13}$$

$P_1 \cap P_2 = \phi$ のとき

$$S(P_2, S(P_1, I)) = S(P_1 \cup P_2, I), \tag{14}$$

$P_1 \supset P_2$ のとき

$$S(P_2, S(P_1, I)) = S(P_1 - P_2, I), \tag{15}$$

である．式(13)から，スクランブル解除はスクランブル時に用いたパラメータ集合と同一集合による再度のスクランブルで実現される．さらに，式(14)，(15)から，多段階のスクランブルによる多重スクランブルの生成および解除が可能であるが，スクランブル時のパラメータ適用順序と解除時の適用順序は独立に決定できる．

4. スクランブル画像の利用例

4.1 課金への利用

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，鍵を入手した利用者はスクランブル解除された画像データをファイルとして保存して利用する．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一方，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 は画像の利用ごとに課金する形態で，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 7 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．ただし，スクランブル解除鍵 k の不正コピーによって元画像の違法コピーが生成されうるから，実際は k をさらにユーザごとの鍵 k_u で暗号化して $E_{k_u}(k)$ とし，スクランブル解除時に $E_{k_u}(k)$ の復号を行う必要がある．

4.2 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

$$S(P_i', S(P_n, I_o)) = S(P_n - P_i', I_o) \quad (16)$$

$$= S(P_{n-i}, I_o) \quad (17)$$

を得る．式 (10) から，$S(P_{n-i}, I_o)$ 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り，$i = n$ のとき $S(P_{n-i}, I_o) = I_o$ となって元画像が復元する．

たとえばすべての 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 4 参照）．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．データがハイパテキスト等複数の独立したデータから構成される場合は素材ごとにスクランブルすればよいが，単一データに複数の著作権が存在する場合は単一画像の複数著者による管理が必要となる．

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．対応するパラメータ p_i は I_i から生成された画素を含むブロックを被覆するように設定する．同一ブロックに複数の著作権が存在する場合，そのブロックは複数の著者によって多重スクランブルされる．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 9** 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 k_1 はテキスト部分 I_1 のみスクランブル解除する．各写真 I_2，I_3 のスクランブル解除には対応する鍵 k_2，k_3 を著者 A_2，A_3 から購入しなければならない．

5. 評　　価

5.1 変換速度

本方式は圧縮画像から画素値を算出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．我々は 640 × 480 画素の 24 ビット・フルカラー JPEG 画像 60 枚を用いて，本スクランブル方式の変換効率の評価を行った．

評価画像のデータ量，圧縮率，付加ビットおよび付加ビット系列の総数とブロックあたりの数を**表 1** に示す．画像全面を最も強くスクランブルする場合の変換対象付加ビット数の最大値および最小値が，それぞれ付加ビット総数および付加ビット系列の総数に等しく，3.2.1 項において $i = m$ および $i = 1$ とした場合に相当する．

変換対象ビットは同ビット数の乱数によって変換される．FEAL の OFB モードはハードウェアで 15 Mbps，ソフトウェアで 2.4 Mbps の乱数発生が可能である[17]．**表 2** に両者に対して，全面を最も強くスクランブルする場合の乱数発生時間を $i = m$ および $i = 1$ について示す．乱数発生時間はソフトウェアで 1 画像あたり平均 50～100 (msec)，ハードウェアで 8～16 (msec) であり，ビット選択器の条件判断および排他的論理和演算が乱数発生に比べて十分速いと仮定すると，図 5 によるスクランブル変換を逐次処理で行う場

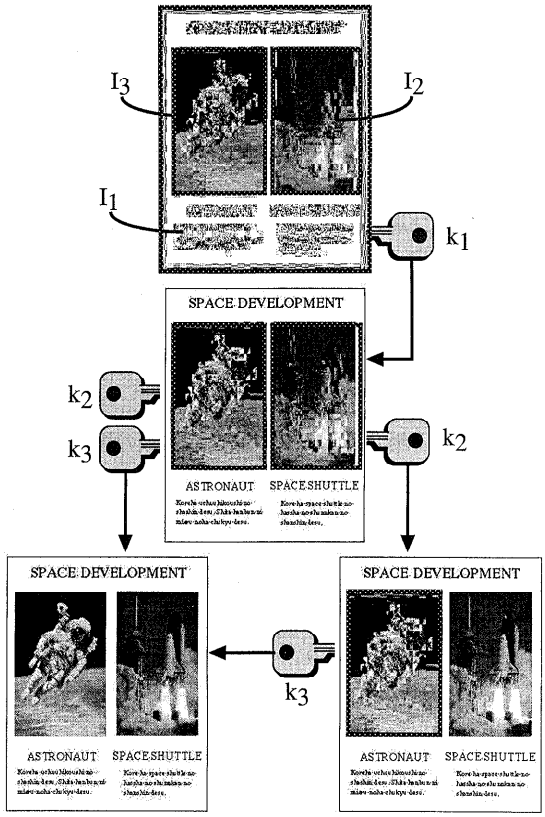


図9 多重スクランブルを用いた著作権保護
Fig. 9 Copyright protection using multiple scrambling.

合であっても，変換時間は JPEG 構文解析時間より数～100（msec）程度増加するにすぎない．

pay per view では画像表示時にスクランブル解除を行う．本方式は画素値に対する演算が不要であるから，図 7 の装置による画像表示時のスクランブル解除でも処理時間の増加は表 2 の場合と等しく，非常に少ない．動画の再生は特に時間の制約が厳しく，再生時のリアルタイム・スクランブル解除のために高速な変換が要求される．図 7 の装置は S，R における乱数発生と D における可変長符号の復号が並列処理可能で，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．motion JPEG や MPEG1 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・スクランブル解除による動画の pay per view も可能となる．具体的には図 7 の装置はソフトウェアによる乱数発生で毎秒平均 10～20 枚，乱数発生ハードウェアを用いれば毎秒平均 60 枚以上のフルカラー・フルスクリーン JPEG 画像が処理可能である．

表1 評価画像
Table 1 Test images.

	平均	最小	最大
データ量（byte）	88537	7468	319229
圧縮率	1/10	1/120	1/2.9
付加ビット総数	242181	4714	1050990
付加ビット系列総数	117548	3945	382935
付加ビット数/ブロック	50.5	1.00	219
付加ビット系列数/ブロック	24.5	0.82	79.8

表2 乱数発生時間（msec）
Table 2 Time for generating random sequences (msec).

		平均	最小	最大
ハードウェア	$i=1$	7.5	0.25	24.3
	$i=m$	15.4	0.30	66.8
ソフトウェア	$i=1$	47.2	1.58	153
	$i=m$	97.3	1.89	422

5.2 安全性

本方式は乱数を用いてスクランブルしているが，乱数発生に任意のアルゴリズムを使用可能であることから，ここでは乱数自体は十分安全であると仮定する．

画像スクランブルでは画像の性質を利用した解読に対する強さが重要である．スクランブル解除に利用可能な画像の重要な特徴量に空間周波数分布がある．たとえば 5.3 節で述べる走査線の移動によるスクランブルでは，垂直方向の空間高周波成分の値に基づいて元画像の走査線位置を推測できる．本論文の方式はブロックを符号化する周波数係数値の変更によってスクランブルを行うが，係数値の変換はカテゴリ内に閉じており，スクランブル画像は周波数分布において元画像と同様の性質を保持する．よって，周波数分布から元画像もしくは乱数系列を推定することは困難である．またスクランブルの解読において元画像が復元されたか否かの判定に，人間による判断が必要になるなど，1 パターンあたりの試行時間が大きくなる．

他方，画像フィルタでスクランブルを弱める方法が存在する．高周波成分を低減する方法は多用されるものの 1 つである．本方式のスクランブル画像にこれを適用すると，元画像からの周波数分布のずれがスクランブル画像以上に大きくなる．

付加ビットに対する全数探索については，1 ブロックあたり，付加ビット数および系列数が平均で 50.5 および 24.5 であるから，平均 $2^{24.5}$～$2^{50.5}$ 回の探索となる（表 1）．局所領域のスクランブル解除は暗号鍵の全数探索に比べて計算量は少なくなりうる．しかし 1 回の試行時間が大きく，また本方式の目的が画像の完全な隠蔽でないことから，十分な強さといえる．

5.3 スクランブル方式の比較

ここでは本方式との比較のために代表的スクランブル方式について考察する．

走査線レベルの変換は有料テレビ放送で利用されるなど最も普及したスクランブル方式である．この方式にはJPEG等の圧縮符号化を用いる場合に次のような問題点が存在する．

- スクランブルによって画像の空間高周波成分が増加するためデータ圧縮率が低下する．
- 圧縮符号化時の量子化誤差によって上記高周波成分に雑音が発生するため，スクランブル解除による元画像の完全な復元が不可能である．
- データ変換のために圧縮符号化データから画素値を算出する必要があり，計算量が増加する．

代表的方式は走査線の移動によるスクランブルである．この方式の圧縮率および雑音についての評価を**表3**に示す．評価には640×480画素フルカラー画像10枚を用いた．画像は各走査線を$0\sim2^6$の幅でランダムに左右に移動してスクランブルし，さらにJPEG圧縮した．またこれをスクランブル解除して復元画像を生成した．

このスクランブルによってJPEGデータ量はスクランブル前の1.18～2.46倍，平均で1.59倍に増加する．元画像に対する復元画像のSN比は平均19.5 dBで，元画像を単にJPEG圧縮したときの平均SN比31.9 dBに比べて非常に低い．JPEG圧縮による雑音を除いた平均SN比は19.6 dBであり，復元画像の雑音の大部分をスクランブルに起因する雑音が占める．

これに対し，ブロックの回転および反転によるスクランブルは雑音発生，圧縮率の低下を防止できるが，解読が容易であるという問題がある．ブロックの置換を併用して変換パタンを増加させられるが，少数のブロックからなる領域に対しては適用不可能である．

表3 スクランブル方式の比較
Table 3 Comparative results of scrambling methods.

	平均	最小	最大
圧縮率（スクランブル前）	1/14.8	1/8.6	1/32.6
圧縮率（スクランブル後）	1/9.3	1/6.6	1/14.2
スクランブル前後の圧縮率の比	1.59	1.18	2.46
JPEG画像のSN比（dB）	31.9	29.6	35.6
復元画像のSN比（dB）	19.5	17.1	21.2
SN比3（dB）	19.6	17.1	21.5

SN比3：走査線シフトのみによる影響

SN比：$20\log_{10}(p_{\max}/\sqrt{\sum \Delta p_{x,y}{}^2/N})$

$p_{\max}$：画素の最大値，Δp_{xy}：画素p_{xy}の誤差，N：画素数

6. スクランブルを用いた画像情報流通

本章ではスクランブル画像を利用した画像情報流通について述べる．ここでは画像提供者，編集者，利用者からなる流通形態を仮定する．提供者は画像情報を販売する．編集者は提供者から購入した画像素材を編集して画像作品を作成し，販売する．利用者は画像情報を提供者または編集者から購入して利用する．スクランブル画像はネットワークやCD-ROM等を通して見本として低価格または無料で公開され，購入前の評価に用いられる．画像の購入は鍵の購入で代替され，あらかじめ入手したスクランブル画像に鍵を作用させて元画像を復元する．

図10～図12に3つの取引形態を示す．図10は基本形態であり，画像提供者と利用者の間で直接取引が

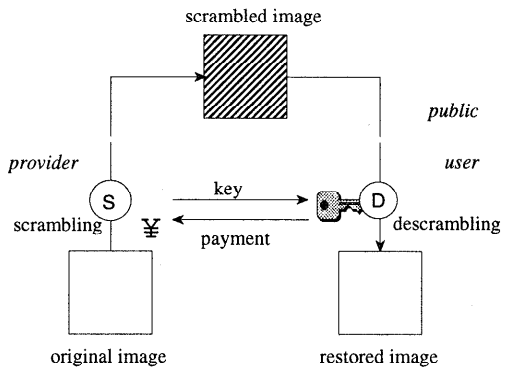


図10 スクランブルを用いた画像情報流通（1）
Fig. 10 Distribution of image data using scrambling (1).

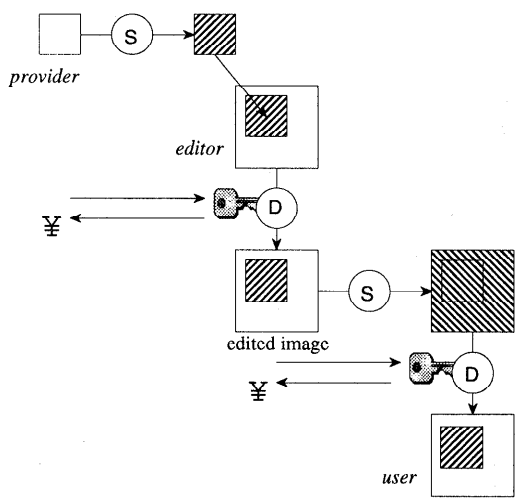


図11 スクランブルを用いた画像情報流通（2）
Fig. 11 Distribution of image data using scrambling (2).

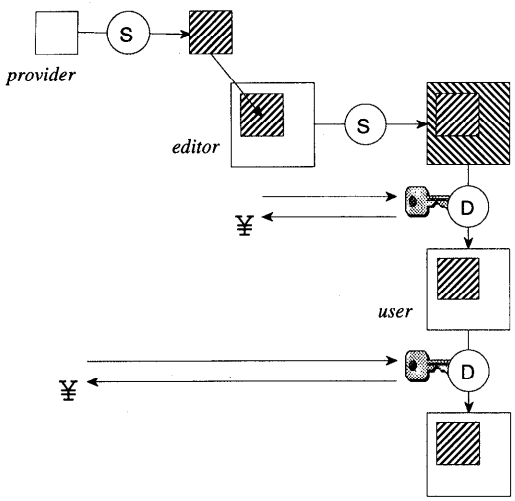


図12 スクランブルを用いた画像情報流通（3）
Fig. 12 Distribution of image data using scrambling (3).

行われる．利用者は購入に先立って公開スクランブル画像を入手して評価し，提供者から必要な画像の鍵を購入して元画像を復元する．

図11，図12は編集者を介した形態である．編集者はスクランブル画像素材を用いて試作編集し，評価を行う．図11では，試作編集の後，鍵を購入し，復元された画像素材を用いて作品を完成させる．作品は編集者によって再びスクランブルされ，図10と同様に流通する．素材提供者に対する支払いはすべて編集者によって行われる．

図12は多重スクランブルによる著作権管理を利用した流通である．試作品完成後，作品上の素材部分が各提供者の鍵でスクランブルされた状態で，さらに編集者自身のスクランブルを重畳する．編集作品の利用者は，作品全体の鍵を編集者から購入する一方，作品中の各素材部分のスクランブルを解除するために，素材提供者からも鍵を直接購入する．この形態は素材の利用に対する提供者の直接課金が可能である．

7. おわりに

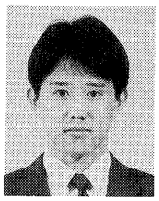
本論文ではディジタル画像流通支援のためのスクランブル方式について述べた．画像流通において著作権保護は最も重要であるが，本方式はスクランブル変換が高速で，簡単な構成のモジュールを画像デコーダに追加することでリアルタイムのスクランブル解除が可能になり，元画像のユーザ端末上への格納を防止して違法コピーに対処できる．またスクランブル程度の制御が可能で，流通における見本として最適なスクランブル画像が生成可能である．さらに多重スクランブルによって支払に応じた画像品質制御や編集された画像の著作権管理も可能となる．

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*, Honolulu, pp.560–566 (1996).
5) Data Encryption Standard, Federal Information Publication Service (FIPS) Publication 46, 15 (1977).
6) Miyaguchi, S.: The FEAL Cipher Family, *Advances in Cryptology-Crypto '90*, LNCS, Vol.537, pp.627-638, Springer-Verlag (1991).
7) Inuma, K.: Two-way Interactive Advertising in the Information Society, *Proc. PTC '96*, Honolulu, pp.837–844 (1996).
8) 松井甲子雄：画像深層暗号—手法と応用，森北出版 (1993).
9) Cox, I.J., Kilian, J., Leighton, T. and Shamon, T.: Secure Spread Spertrum Watermarking for Multimedia, NEC Research Institute, Technical Report, 95-10 (1995).
10) Bender, W., Gruhl, D. and Morimoto, N.: Techniques for Data Hiding, *Proc. SPIE*, Vol.2420, p.40 (1995).
11) 日経マルチメディア，No.17, pp.84–89 (1996.11).
12) 勝田 昇，中村誠司，村上弘規，田中初一：映像信号のディジタルスクランブルの一方式，信学技報，ISEC90-33, pp.1–7 (1990).
13) 浜崎孝幸：衛星放送有料方式と鍵管理システム，信学技報，ISEC91-28, pp.49–56 (1991).
14) 木下宏揚，塩入律雄，酒井善則：DCT符号化に適した画像暗号化方式の提案，信学論（D-I），Vol.J75-D-1, No.5, pp.314–321 (1992).
15) Mori, R. and Kawahara, M.: Superdistribution: The Concept and the architecture, *IEICE Trans.*, Vol.E73, No.7, pp.1133–1146 (1990).
16) 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回情報処理学会全国大会論文集，2-209

(1996).
17) エレクトロニクス，Vol.41，No.5，pp.64–65 (1996).

(平成8年12月9日受付)
(平成9年 7 月1日採録)



藤井　寛（正会員）

平成元年京都大学工学部情報工学科卒業．平成3年同大学院工学研究科情報工学専攻修士課程修了．同年日本電信電話（株）入社．動画像多重アクセスサーバの研究，マルチメディア情報流通方式の研究に従事．電子情報通信学会会員．

山中　康史

昭和56年九州大学工学部情報工学科卒業．昭和58年同大学院工学研究科情報工学コース修士課程修了．同年日本電信電話公社（現NTT）入社．通信網管理システム，サービス管理システム，マルチメディア情報取引方式の研究実用化に従事．NTT情報通信研究所主幹研究員．電子情報通信学会会員．